RCB
Rządowe Centrum Bezpieczeństwa

BIURO
ANALIZ I REAGOWANIA

BIULETYN

KWARTALNY

KORONAWIRUS – WIRUS SARS-COV-2 3

MECHANIZM REAGOWANIA KRYZYSOWEGO UE – IPCR PODCZAS PANDEMII COVID-19 5

SYTUACJA NA BIAŁORUSI – OBRAZ PO DWÓCH MIESIĄCACH PROTESTÓW SPOŁECZNYCH 8

NA RATUNEK LIBANOWI 11

TERRORYZM NADAL POWAŻNYM ZAGROŻENIEM DLA ŚWIATOWEGO BEZPIECZEŃSTWA 14

RANSOMWARE W NOWEJ ODSŁONIE 16

SFERA CYWILNA I WOJSKOWA WSPÓLNIE W ĆWICZENIACH 20

SUSZA ROLNICZA W 2020 ROKU ORAZ WDROŻENIE NOWEGO SYSTEMU ZBIERANIA DANYCH O STRATACH W ROLNICTWIE 22

NUMER 30 LIPIEC – WRZESIEŃ 2020

Zespół redakcyjny

Biuletynu kwartalnego Rządowego Centrum Bezpieczeństwa:

Grzegorz Świszcz – Zastępca Dyrektora RCB

Martyna Olejnik-Kołodziej

Anna Zasadzińska-Baraniewska

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

Koronawirus – wirus SARS-CoV-2

Izabela Kucharska
Główny Inspektorat Sanitarny

Znaczenie drobnoustrojów, jako realnych czynników mogących spowodować istotne niebezpieczeństwo dla zdrowia lub życia ludzi, było sygnalizowane i podkreślane przez Państwową Inspekcję Sanitarną na każdym szczeblu funkcjonowania, podczas przygotowywania lub aktualizowania planów działania na wypadek wystąpienia zagrożeń dla bezpieczeństwa państwa. Wskazywano przy tym, że wykaz chorób zakaźnych i drobnoustrojów, stanowiących potencjalne zagrożenie zdrowotne, nie może być traktowany jako katalog zamknięty, z uwagi na możliwość pojawienia się nowych, dotąd nieznanych, niezidentyfikowanych czynników chorobotwórczych.

W ramach działalności ustawowej Państwowej Inspekcji Sanitarnej, w związku z istnieniem potencjalnego zagrożenia rozprzestrzeniania się niebezpiecznych patogenów, na bieżąco prowadzony jest nadzór epidemiologiczny, mający na celu wczesne wykrywanie i zwalczanie czynników biologicznych wywołujących choroby zakaźne u ludzi. Stąd, już na początku stycznia, kiedy Światowa Organizacji Zdrowia (WHO) poinformowała o szerzeniu się w Chinach nowego koronawirusa, Główny Inspektor Sanitarny rozpoczął działania we współpracy z Urzędem Lotnictwa Cywilnego, Graniczną Stacją Sanitarno-Epidemiologiczną w Warszawie i służbami medycznymi Portu Lotniczego Chopina w Warszawie, mające na celu wzmożony monitoring osób przylatujących z kierunku Azji Wschodniej i Południowo-Wschodniej. Choć wstępna informacja służb medycznych w Chinach głosiła, że nowy wirus nie przenosi się z człowieka na człowieka, zaktualizowane zostały m.in. karty lokalizacji pasażera, przygotowane ulotki w kilku wersjach językowych dla podróżnych powracających z rejonów objętych wówczas epidemią, z informacją dotyczącą postępowania w przypadku zaobserwowania niepokojących objawów chorobowych.

W połowie stycznia Główny Inspektor Sanitarny, na swojej stronie internetowej, rozpoczął codzienną publikację komunikatów dla podróżujących, na temat aktualnej sytuacji epidemiologicznej związanej z nowym koronawirusem na świecie. Prowadzono działania informacyjne skierowane do społeczeństwa – aktualne komunikaty ECDC, WHO, CDC umieszczane były na stronie www.gis.gov.pl oraz na profilach w mediach społecznościowych.

Następnie rozpoczęto intensywne prace nad wytycznymi, które początkowo dedykowane były służbom medycznym, farmaceutycznym i lotniczym, a kolejno opracowane zostały dla szeregu innych branż i sektorów; łącznie ponad 250.

30 stycznia 2020 r. Światowa Organizacja Zdrowia ogłosiła epidemię SARS-CoV-2 zagrożeniem dla zdrowia publicznego o znaczeniu międzynarodowym, dlatego kluczowa stała się intensyfikacja działań zmierzających do zapewnienia bezpieczeństwa kraju i obywateli. Mając na uwadze niedawne (2003 r.) zagrożenie wirusem SARS (Severe Acute Respiratory Syndrome), opracowany został m.in. Krajowy plan działania na wypadek wystąpienia w Polsce przypadków podejrzenia lub zakażenia SARS-CoV-2.

Dynamiczny rozwój epidemii w Chinach, a następnie krajach azjatyckich, łatwość szerzenia się koronawirusa, duża mobilność populacji ludzi spowodowały szybkie rozprzestrzenienie się SARS-CoV-2. WHO 11 marca ogłosiła pandemię nowego koronawirusa, alarmując o rosnącej liczbie zakażeń na świecie. Pierwszy zdiagnozowany przypadek zakażenia w Polsce, przy 548 wykonanych już wówczas testach molekularnych, odnotowano 4 marca 2020 r. u pacjenta hospitalizowanego w szpitalu w Zielonej Górze, woj. lubuskie. Od tego czasu także Polska podjęła intensywne działania zmierzające do lepszego poznania epidemiologii nowego koronawirusa.

Koronawirusy, znane od 60 lat, to gatunki wirusów należących do podrodziny Coronavirinae, w zależności od rodzaju, specyficzne dla ssaków i ptaków. Są to wirusy osłonkowe posiadające jedną nić RNA. Najbardziej znane koronawirusy ludzkie to wspomniany SARS, którego rezerwuarem są ludzie, szerzy się drogą kropelkową, także powietrzną i kontaktową, a jego śmiertelność oceniana jest na 10% oraz MERS-CoV, z rezerwuarem ludzkim

i zwierzęcym (wielbłądy), ze śmiertelnością sięgającą 50% chorych.

SARS-CoV-2 jest wirusem wywołującym chorobę zwaną COVID-19. Jest to choroba zakaźna, której najczęstsze objawy to: gorączka, suchy kaszel i zmęczenie, duszność, utrata smaku lub węchu. Objawy te są zwykle łagodne i zaczynają się stopniowo. Niektórzy zakażeni ludzie chorują bardzo łagodnie, albo przechodzą zakażenie bezobjawowo. Większość ludzi (około 80%) przechodzi zakażenie bez konieczności leczenia szpitalnego.

Około 1 na 5 osób zakażonych choruje poważnie (m.in. istotne trudności z oddychaniem). Osoby starsze i osoby z innymi problemami zdrowotnymi, takimi jak: nadciśnienie, choroby układu krążenia, oddechowego, cukrzyca, nowotwory, immunosupresja, są bardziej narażone na ciężki przebieg choroby. Jednak każdy może zostać zakażony SARS-CoV-2 i poważnie zachorować, co zależy od właściwości osobniczych.

Osobom, które mają lekkie objawy, takie jak lekki kaszel lub stan podgorączkowy, zaleca się skorzystanie z teleporady medycznej, pozostanie w domu, czasowe odizolowanie się, codzienne monitorowanie stanu zdrowia i temperatury ciała, przez 10-14 dni. Osoby z ciężkimi lub nasilającymi się objawami kaszlu, duszności, gorączką powinny niezwłocznie udać się do najbliższego oddziału zakaźnego lub szpitala. Ważne jest przy tym, aby unikać narażenia innych osób na zakażenie – udać się do szpitala transportem indywidualnym, a jeśli to niemożliwe wezwać transport medyczny.

Człowiek może zarazić się SARS-CoV-2 od innych osób, które są nim zakażone. Wirus przenosi się z człowieka na człowieka przez małe kropelki z wydzieliną oddechową, które są wydalane, gdy osoba z COVID-19 kaszle, kicha lub mówi. Kropelki wydzieliny są dość ciężkie i szybko opadają na ziemię. Do zakażenia człowieka może dojść wówczas, kiedy znajduje się blisko osoby zakażonej (mniej niż 1,5 m) i jest narażony na wdychanie wirusów przez nią wydalanych. Kropelki zawierające wirusa opadają także na przedmioty i powierzchnie wokół osoby zakażonej (blaty, uchwyty, klamki, poręcze). Do zakażenia może więc dojść drogą pośrednią, poprzez dotykanie skażonych przedmiotów lub powierzchni, a następnie dotykając oczu, nosa lub ust.

Dlatego istotne jest, aby ściśle przestrzegać kilku ważnych, ale prostych zasad, pozwalających zminimalizować ryzyko zakażenia:

- Regularnie i często myć ręce wodą z mydłem. Wirus osłonięty jest cienką warstwą lipidową, która rozpuszcza się pod wpływem powszechnie dostępnych detergentów. W sytuacjach kiedy nie ma możliwości umycia rąk (w środkach transportu, sklepie, podróży) należy dezynfekować je preparatami na bazie alkoholu (min. 60%).
- Podczas powitania unikać podawania dłoni i uścisków ponieważ sprzyja to zakażeniu ze względu na kontakt bezpośredni (uściski) i pośredni (dotykanie zanieczyszczonych dłoni).
- Zachować bezpieczną odległość od rozmówcy. Należy zachować co najmniej 1,5 metra odległości od osób, z którymi rozmawiamy twarzą w twarz, które kaszlą, kichają, krzyczą lub mają widoczne objawy gorączki.
- Osłaniać usta i nos w sytuacjach, kiedy zachowanie dystansu od innych osób nie jest możliwe. Maseczka, przyłbica, czy osłona wykonana własnoręcznie z fragmentu materiału pozwoli ograniczyć rozprzestrzenianie się wirusa wraz z wydzieliną oddechową.
- Przestrzegać zasad higieny podczas kichania i kaszlu. Kiedy kaszlemy lub kichamy wydzielina oddechowa wydostaje się z naszych płuc pod ciśnieniem i może pokonać dużo większą odległość niż podczas mówienia. Wówczas należy zakryć usta i nos chusteczką lub w razie jej braku zgiętym łokciem. Chusteczkę jak najszybciej wyrzuć do kosza, umyć ręce używając mydła i wody lub zdezynfekować je.
- Unikać dotykania oczu, nosa i ust. Dotknięcie oczu, nosa lub ust zanieczyszczonymi rękami, może spowodować przeniesienie wirusa z ich powierzchni do naszego organizmu.
- Regularnie myć wodą z detergentem lub dezynfekować powierzchnie dotykowe w swoim otoczeniu. Zasada ta dotyczy zarówno takich elementów jak biurko, stół, klamki, włączniki światła, poręcze, ale pamiętać należy też o przecieraniu telefonu komórkowego, pilota do telewizora, czy uchwytów torebki.

Nie bez znaczenia dla naszego zdrowia jest dbałość o odporność. Zdrowe odżywianie się i zrównoważona dieta, spożywanie min 2 l wody dziennie, odpowiednia

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

do wieku liczba godzin snu, umiarkowana aktywność fizyczna to kilka podstawowych elementów pozytywnie wpływających na stan naszego zdrowia.

Koronasceptycy podważają istnienie zagrożenia związanego z SARS-CoV-2, a niektórzy nawet jego istnienie. Dlatego też na koniec kilka liczb od początku epidemii wg stanu na 4 października 2020 r.:

Świat:

- 34 986 502 zakażenia SARS-CoV-2,
- 1 034 240 zgonów w przebiegu COVID-19.

Unia Europejska i kraje EEA:

- 3 517 651 zakażeń SARS-CoV-2,
- 191 576 zgonów z powodu COVID-19.

Polska:

- 100 074 zakażeń SARS-CoV-2,
- 2 630 osób zmarło,
- 1 934 nowe przypadki (dzienna liczba zakażeń),
- 150 565 osób jest objętych kwarantanną.

Podejrzewając u siebie zakażenie koronawirusem należy zachować spokój i korzystać wyłącznie ze sprawdzonych źródeł informacji, aby dowiedzieć się jakie dalsze kroki poczynić. Polecane źródła polskojęzyczne to przede wszystkim strona internetowa dedykowana informacjom dotyczącym koronawirusa pod adresem: https://www.gov.pl/web/koronawirus, a także strony: Głównego Inspektoratu Sanitarnego, Ministerstwa Zdrowia, Rządowego Centrum Bezpieczeństwa, Rzecznika Praw Pacjenta, Narodowego Funduszu Zdrowia oraz poszczególnych resortów, które zamieszczają bieżące informacje przydatne w obszarze ich działania.

Wdrażanie strategii walki z pandemią koronawirusa w nadchodzącym sezonie infekcji układu oddechowego, ogłoszonej przez Ministra Zdrowia, konsekwentne działania planowane i realizowane w sektorze ochrony zdrowia, starania krajowych służb biorących udział w postępowaniu przeciwepidemicznym, w tym Państwowej Inspekcji Sanitarnej, powszechne działania edukacyjno-informacyjne oraz odpowiedzialne podejście społeczeństwa do zasad minimalizujących ryzyko zakażenia – to obecnie kluczowe elementy walki z zagrożeniem wywołanym przez nowego wirusa SARS-CoV-2. Świat bowiem nadal oczekuje na skuteczną szczepionkę i leki umożliwiające zmniejszenie do minimum liczby zgonów w wyniku COVID-19.

Piśmiennictwo – materiały ze stron:
1. www.ecdc.europa.eu
2. www.who.int
3. www.gis.gov.pl
4. www.mz.gov.pl.

Mechanizm reagowania kryzysowego UE – IPCR podczas pandemii COVID-19

Kamil Stobnicki, Sławomir Łazarek
Rządowe Centrum Bezpieczeństwa

Wydarzenia ostatnich lat (zajęcie Krymu, powstanie „państwa islamskiego", kryzys migracyjny, zamachy terrorystyczne) uświadomiły, że Unia Europejska jako globalny gracz stanęła przed nowymi wyzwaniami i zagrożeniami. Wymagały one adaptacji do zmieniającego się środowiska bezpieczeństwa. W praktyce oznaczało to konieczność nie tylko zdefiniowania na nowo priorytetów działania, lecz także wypracowania bardziej efektywnych zasad podejmowania decyzji. W następstwie tych zmian udoskonalano narzędzia wspomagające gremia i osoby decyzyjne (na różnych poziomach kierowania Unią Europejską oraz w państwach członkowskich) w wypracowaniu i podejmowaniu decyzji. Jednym z takich narzędzi jest ustanowiony decyzją Rady Unii Europejskiej unijny mechanizm reagowania kryzysowego IPCR (EU Integrated Political Crisis Response Arrangements)[1]. Rządowe Centrum Bezpieczeństwa jest krajowym punktem kontaktowym w mechanizmie IPCR, który okazuje się wyjątkowo przydatny w czasie pandemii koronawirusa.

[1] Zob. finalizacja procesu weryfikacji CCA: zintegrowane uzgodnienia UE dotyczące reagowania na szczeblu politycznym w sytuacjach kryzysowych (IPCR), 10708/13, 2013.

Pierwszym poważnym sprawdzianem dla skuteczności IPCR był kryzys migracyjny. Decyzję o aktywacji mechanizmu po raz pierwszy podjęła prezydencja luksemburska w 2015 r. w odpowiedzi na niespotykaną wcześniej skalę migracji na obszar UE. Kolejnym kryzysem uzasadniającym uruchomienie w praktyce procedur zapisanych w dokumencie ustanawiającym mechanizm IPCR stał się właśnie wybuch pandemii koronawirusa COVID-19.

W teorii IPCR powinien umożliwić efektywną koordynację, a także reagowanie na szczeblu politycznym UE na różnego rodzaju sytuacje kryzysowe. Kluczowy zatem wydaje się elastyczny charakter mechanizmu, pozwalający na reakcję niezależnie od rodzaju i zasięgu kryzysu, a także od jego źródła (wewnętrznego lub zewnętrznego). Zaletami IPCR są więc jego wszechstronność, kompleksowość i uniwersalność.

Wieloaspektowy przekrojowy charakter współczesnych zagrożeń z jednej strony, a charakter mechanizmu IPCR (jego funkcjonalność, struktura, zakres merytoryczny) z drugiej strony, wymagają dobrze skoordynowanej współpracy w ramach każdego państwa, czyli pomiędzy różnymi podmiotami zarządzania kryzysowego (właściwymi w zależności od zaistniałego kryzysu). Fakt ten stał się głównym powodem decyzji o przejęciu przez Rządowe Centrum Bezpieczeństwa funkcji koordynatora współdziałania Polski z mechanizmem IPCR. W praktyce odpowiedzialny jest za to Wydział Współpracy Międzynarodowej RCB. Nowe zadanie Centrum oznacza pełnienie wiodącej roli w opisywanych poniżej narzędziach wykorzystywanych na potrzeby IPCR. Centrum może wywiązywać się z tej roli jedynie pod warunkiem terminowej i efektywnej współpracy z kompetentnymi resortami i służbami.

W kontekście unijnej reakcji na zagrożenie koronawirusem, decyzja o uruchomieniu mechanizmu IPCR została podjęta 28 stycznia br. Wtedy to chorwacka prezydencja w Radzie w obliczu coraz bardziej niepokojących doniesień o skali epidemii oraz w celu zapewnienia państwom członkowskim jak najbardziej terminowej wymiany bieżących informacji aktywowała IPCR w trybie tzw. *information sharing mode*[2]. Pociągnęło to za sobą zwoływane ad hoc spotkania Grupy Przyjaciół Prezydencji (*Friends of Presidency, FoP IPCR*). Głównym zadaniem było wypracowanie skoordynowanych działań na początkowym etapie rozwoju epidemii. Dotyczyły one wzajemnego informowania się przez państwa członkowskie i struktury unijne o wyzwaniach, z jakimi się spotykają, a ponadto o konkretnych potrzebach związanych z rozwijającą się sytuacją kryzysową. Jednym z wiodących wtedy tematów była ewakuacja obywateli UE z Chin, które były pierwszym ogniskiem pandemii[3]. Spotkania tego gremium stworzyły również możliwość uczestniczenia w nich, oprócz krajów członkowskich, także wyspecjalizowanych unijnych agencji np. Europejskiego Centrum ds. Zapobiegania I Kontroli Chorób (*European Centre for Disease Prevention and Control, ECDC*) czy unijnych dyrekcji: DG SANTE, DG ECHO, DG HOME[4]. Zapewniało to możliwie szeroką ocenę bieżącej sytuacji i pomagało wypracować wszechstronne i w miarę możliwości skoordynowane podejście państw członkowskich oraz UE do zagrożeń i wyzwań, jakie niosła ze sobą pandemia.

Od początku aktywacji mechanizmu na internetowej platformie IPCR (z limitowanym dostępem), w specjalnie dedykowanej zakładce, ukazywały się różnego rodzaju materiały np.: dokumenty opracowywane przez DG ECHO pt: *Analytical Brief* lub publikowane pod egida Europejskiej Służby Działań Zewnętrznych (ESDZ) pt. *Corona Virus Special Monitoring.* Zawierały one najnowsze doniesienia o działaniach podejmowanych przez UE, a także prezentowały bieżący obraz sytuacji. Ponadto, kraje członkowskie zachęcane były do publikowania na tym portalu wprowadzanych u siebie regulacji dotyczących zwalczania skutków pandemii względnie przeciwdziałania im.

Statutowym narzędziem IPCR (obok spotkań nieformalnych) wykorzystywanym od początku aktywowania mechanizmu były tzw. raporty sytuacyjne ISAA (*Integrated Situational Awareness and Analysis*). Są one opracowywane w ścisłej współpracy przez KE oraz ESDZ na podstawie wkładów przekazywanych przez państwa członkowskie i agencje unijne[5]. Pytania

[2] IPCR obejmuje trzy możliwe tryby funkcjonowania: tryb monitorowania (*monitoring mode*) – bez konieczności aktywowania mechanizmu, tryb wymiany informacji (*information sharing mode*) i tryb pełnej aktywacji (*full activation mode*).

[3] W związku z ewakuacją obywateli UE aktywowany został na wniosek Francji unijny Mechanizm Ochrony Ludności.

[4] Generalne Dyrekcje ds: Zdrowia i Ochrony Konsumentów, Pomocy Humanitarnej i Ochrony Ludności, ds. Migracji i Spraw Wewnętrznych.

[5] Przekazywanie wkładów odbywa się również poprzez platformę IPCR. Do ich umieszczania upoważnione są wcześniej wskazane osoby/instytucje z odpowiednim poziomem uprawnień – tzw. *Managing Authority* i *Validating Authority*.

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

zawarte w kwestionariuszach są sformułowane w ten sposób, aby dać jak najszerszy pogląd na konsekwencje kryzysu pandemicznego, tj. oprócz pytań o aspekty medyczne i zdrowotne (np. o ewentualne niedobory w zasobach, strategię testowania, itd.) zadawane są pytania dotyczące na przykład ograniczeń w ruchu granicznym, usług turystycznych czy transportowych, a także kwestii związanych z dezinformacją czy zagrożeniami cyber. Tak opracowane raporty przedstawiają kompleksowy obraz sytuacji, służący zarówno Prezydencji kierującej pracami Rady, jak i państwom członkowskim UE. Raporty ISAA publikowane są cotygodniowo, dzięki czemu widoczny jest trend zmian zachodzących w związku z sytuacją.

Ze względu na pogarszającą się sytuację epidemiologiczną, 2 marca br. prezydencja podjęła decyzję o aktywowaniu mechanizmu IPCR w pełnym trybie. Na portalu w dedykowanej podstronie kolejne kraje dzieliły się informacjami o środkach wprowadzanych w celu ograniczenia rozprzestrzeniania się wirusa. Zaczęto zwoływać cykliczne posiedzenia tzw. grupy wysokiego szczebla (*IPCR high level roundtable, HLRT*) z udziałem ambasadorów, a także przedstawicieli KE, ESDZ, ECDC[6]. Chodziło o identyfikację luk w podejmowanych działaniach z walce z kryzysem oraz poszukiwanie obszarów, w których państwa członkowskie mogłyby działać w skoordynowany sposób na poziomie politycznym[7]. Z czasem, spotkania w formacie ambasadorów zostały uzupełnione o spotkania na poziomie eksperckim (*WLR IPCR working level roundtable*). Każde spotkanie grupy IPCR kończy się opracowaniem konkluzji operacyjnych, czyli swojego rodzaju podsumowaniem oraz wyznaczeniem kolejnych działań dla unijnych instytucji i państw członkowskich.

To właśnie na forum IPCR koordynowane były prace związane ze stopniowym znoszeniem obostrzeń wprowadzonych po „zamrożeniu życia społeczno-gospodarczego w państwach członkowskich" (*lockdown*). Służyło temu m.in. powołanie w państwach członkowskich sieci punktów kontaktowych w celu gromadzenia informacji dotyczących kolejnych środków deeskalacyjnych wprowadzanych przez poszczególne kraje. Informacje te są przez prezydencję aktualizowane co tydzień, na podstawie wkładu wszystkich państw członkowskich w formie zbiorczej tabeli tzw. *COVID-19 Transition Monitoring Table (TMT)*[8].

Kolejnym narzędziem opracowywanym przez KE na potrzeby zwiększenia świadomości społeczeństw o kryzysie jest strona internetowa *Re-open EU*[9]. Rozwiązanie to umożliwia przeglądanie wiadomości dotyczących poszczególnych państw członkowskich UE za pomocą interaktywnej mapy, zawierającej aktualne informacje na temat obowiązujących krajowych środków, a także inne praktyczne porady dla osób odwiedzających dany kraj.

W ramach IPCR działa również nieformalna grupa ekspertów z państw członkowskich UE z zakresu komunikacji kryzysowej – *Crisis Communicators' Network (CCN)*. W skład grupy wchodzą także eksperci z instytucji unijnych. W normalnych okolicznościach grupa spotyka się przynajmniej raz w okresie jednej prezydencji. Wobec pełnej aktywacji mechanizmu z powodu pandemii, spotkania (w formie wideokonferencji) odbywają się częściej. Poświęcone są omówieniu sytuacji kryzysowej związanej z pandemią koronawirusa czy np. strategii komunikacyjnej w sprawie wychodzenia z kryzysu [10].

Ważnym tematem spotkań IPCR (*HLR, WLRT*) była dyskusja nad tzw. instrumentem finansowym na rzecz wsparcia w sytuacjach nadzwyczajnych (*The Emergency Support Instrument, ESI)*.[11] Instrument ten ukierunkowany jest w obecnej sytuacji w szczególności na wsparcie sektora ochrony zdrowia. Grono jego beneficjentów może być jednak szersze,

[6] O zwołaniu spotkań oraz uczestnikach spotkania decyduje prezydencja (do 31.12 br. sprawuje ją RFN). Organizację spotkań wspiera Sekretariat Generalny Rady. Spotkania mają charakter nieformalny, mogą być organizowane na poziomie ekspertów, ambasadorów lub ministrów.

[7] W praktyce dyskusje koncentrowały się m.in. na: dostępnych zasobach medycznych, repatriacji obywateli UE z państw trzecich, utrzymaniu przepływu transportu towarów, komunikatach dla podróżujących czy konieczności właściwego informowania społeczeństwa.

[8] Po stronie polskiej tabelę uzupełnia RCB i przekazuje ją do Stałego Przedstawicielstwa RP przy UE. Zawarte w niej informacje obejmują obszary: edukacja, usługi (prowadzenie działalności gospodarczej i wytyczne dla branż), transport, granice, turystyka, gromadzenie się w miejscach publicznych.

[9] Platforma uruchomiona została 15 czerwca br., https://reopen.europa.eu/. Dostępne w czasie rzeczywistym informacje dotyczące m.in. sytuacji na granicach, dostępnych środków transportu, ograniczeń dotyczących podróżowania, środków w zakresie zdrowia publicznego i bezpieczeństwa, takich jak utrzymywanie dystansu fizycznego lub noszenie masek ochronnych, a także inne praktyczne informacje dla podróżnych.

[10] Przedstawicielką Polski w grupie jest Anna Adamkiewicz, szefowa Wydziału Polityki Informacyjnej Rządowego Centrum Bezpieczeństwa.

[11] Instrument ESI stworzony został w 2016 r. w związku z kryzysem migracyjnym w Europie Południowej i potrzebą kontraktowania przez KE pomocy humanitarnej na potrzeby wewnątrzunijne. Reaktywowany został w związku z pandemią. Wsparcie jest finansowane z budżetu ogólnego Unii oraz z wkładów, jakie mogą wnosić państwa członkowskie i inni darczyńcy publiczni lub prywatni. Na ten cel alokowano 2,7 mld EUR na 2020 r.

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

skoro koszty działań związanych z pandemią ponoszą także inne podmioty. I tak, pierwsze obszary objęte tym instrumentem to: wsparcie dla transportu zespołów medycznych i personelu medycznego wewnątrz UE oraz z państw trzecich do UE, transport ładunków, transport pacjentów wewnątrz UE oraz z UE do państw trzecich, a także zakup niektórych zapasów medycznych[12].

Aktualnie, ze względu na rosnącą liczbę zachorowań w UE, dyskusja toczona w ramach mechanizmu IPCR koncentruje się na koordynacji działań, w tym wprowadzanych kolejnych restrykcjach i ograniczeniach życia społecznego i gospodarczego tak, aby podejście UE (a tym samym poszczególnych krajów) była możliwie jak najbardziej spójna[13]. Jednym z aktualnych tematów jest chociażby długość obowiązkowej kwarantanny czy wypracowanie wspólnych wskaźników notyfikacji zachorowań. Ponadto, państwa są informowane przez ECDC o bieżącej sytuacji epidemiologicznej na świecie.

Sytuacja na Białorusi – obraz po dwóch miesiącach protestów społecznych

opracowanie zbiorowe: *Ośrodek Studiów Wschodnich im. Marka Karpia, Rządowe Centrum Bezpieczeństwa*

9 sierpnia br. na Białorusi miały miejsce wybory prezydenckie, których wynik – zwycięstwo Alaksandra Łukaszenki z wynikiem 80,1% głosów – został przez większość społeczeństwa uznany za sfałszowany. Opozycyjna kandydatka Swiatłana Cichanouska, według oficjalnych danych, uzyskała 10,1% głosów. Na Białorusi doszło do protestów i demonstracji społecznych, niemających precedensu w historii tego kraju.

Protesty przeciwko reżimowi Alaksandra Łukaszenki wybuchły natychmiast po ogłoszeniu wyniku wyborów, ale napięcie społeczne wzrastało już w okresie poprzedzającym głosowanie. Pod pretekstem zagrożenia epidemicznego utrudniono pracę dziennikarzy – białoruski MSZ radykalnie ograniczył wydawanie akredytacji korespondentom zagranicznym. Władze zablokowały również przyjazd międzynarodowych obserwatorów OBWE, zwlekając z wystosowaniem do nich zaproszenia. W trakcie głosowania dochodziło do masowych fałszerstw i naruszeń prawa wyborczego. Władze państw UE (m.in. Słowacji, Czech, Litwy, Łotwy, Estonii, Danii, Polski, Niemiec) oświadczyły, że nie uznają uzyskanej w niedemokratyczny sposób prezydentury. Do tego stanowiska dołączyły również USA, Kanada i Ukraina.

Głównym przejawem buntu społeczeństwa przeciwko reżimowi Łukaszenki są uliczne demonstracje i wystąpienia. Władze Białorusi niezmiennie odrzucają możliwość dialogu, ale ich postawa wobec sytuacji wewnętrznej w kraju wciąż ma charakter wyczekujący. Nie podejmują one ani decyzji o powrocie do masowych i brutalnych represji, ani też działań o charakterze politycznym, mogących w przewidywalnej perspektywie uspokoić nastroje społeczne. Widoczne jest jednak, iż stopniowo, ale sukcesywnie wzrasta brutalność funkcjonariuszy, szczególnie wobec uczestników mniejszych demonstracji w miastach obwodowych, gdzie poza środkami przymusu bezpośredniego stosowany jest gaz łzawiący, kule gumowe i granaty hukowo-błyskowe. Do najliczniejszych manifestacji dochodzi w Mińsku, gdzie niemal co tydzień dochodzi do niedzielnych manifestacji, gromadzących średnio ok. 100 tys. osób. Aktywne są też mniejsze ośrodki, przede wszystkim miasta obwodowe jak Grodno, Brześć czy Homel, gdzie, zwłaszcza w początkowym okresie, w demonstracjach uczestniczyło średnio od kilku do 10 tys. osób. Do zatrzymań dochodziło również podczas organizowanych cyklicznie sobotnich marszów kobiet w Mińsku. Działania represyjne podejmowane przez reżim wobec protestujących doprowadziły w połowie października do wyraźnego spadku liczebności uczestników demonstracji w mniejszych ośrodkach miejskich. Również starcia z oddziałami OMON-u i Wojsk Wewnętrznych MSW wciąż mają charakter ograniczony i dochodzi do nich jedynie w przypadku użycia brutalnej siły przez organy porządkowe. Wzrasta liczba osób zatrzymywanych podczas manifestacji. Zazwyczaj w trakcie

[12] Z instrukcji dla przedstawiciela Polski na 30. posiedzenie Komitetu Ochrony Ludności (CPC) 5 maja 2020 r., opracowanej przez KG PSP.,

[13] Propozycję takiej spójnej odpowiedzi opracowywane są przez prezydencję i przedkładane krajom członkowskim.

niedzielnych demonstracji zatrzymywano ok. 300-350 osób, w trakcie ostatniej liczba ta wzrosła do ponad 700 zatrzymanych, którzy zostali w większości ukarani grzywnami. Społeczny gniew wynikający z utrzymywania się Łukaszenki przy władzy nie powoduje radykalizacji protestów, choć stopniowo wzrasta napięcie, szczególnie wśród części demonstrantów nieobawiających się fizycznego przeciwstawienia się organom porządkowym. Jednocześnie zwiększa się samoorganizacja inicjatyw antyreżimowych i obserwuje się wykorzystywanie nowych metod protestu. Dzięki inicjatywie kanału Nexta stworzono i upubliczniono dane osobowe ponad 2 tys. zidentyfikowanych funkcjonariuszy organów porządkowych stosujących przymus fizyczny wobec demonstrantów. Akcja ta może obniżyć morale np. w organach MSW, zarazem jednak może być wykorzystywana przez władze do konsolidacji struktur siłowych w opozycji do protestujących. Kolejną formą aktywności wymierzonej przeciwko rządzącym jest działalność tzw. cyberpartyzantów, rekrutujących się z białoruskich informatyków. Ich cel to zakłócanie funkcjonowania reżimowych stron internetowych (m.in. MSW, służby podatkowej czy reżimowych mediów). W niektórych zakładach pracy zbierane są podpisy pod apelami o dymisję Łukaszenki i przeprowadzenie nowych wyborów, ale zasięg tej akcji nie jest duży.

Władze konsekwentnie kontynuują kreowanie rzekomej sytuacji zagrożenia zewnętrznego, czemu sprzyja wsparcie Moskwy. 16 września wizytę roboczą w Mińsku złożył minister obrony Rosji Siergiej Szojgu. Potwierdziła ona, że Kreml przywiązuje ogromną wagę do zagwarantowania swobody operowania swoich sił zbrojnych na terytorium Białorusi. Była też sygnałem skierowanym do NATO i USA, że Moskwa jest zdeterminowana, aby utrzymać reżim Łukaszenki. Zapowiedź intensyfikacji białorusko-rosyjskich ćwiczeń wojskowych wydaje się sygnalizować, że udział jednostek Sił Zbrojnych FR, które będą odbywać szkolenia na terytorium Białorusi, może – w zależności od rozwoju sytuacji politycznej – przybrać formę rotacyjnej obecności militarnej.

Destabilizacja sytuacji na Białorusi po wyborach prezydenckich nie wpłynęła dotychczas na modyfikację aktywności Sił Zbrojnych RB. Podejmowane bezpośrednio po rozpoczęciu społecznych protestów przedsięwzięcia poligonowe wpisywały się w standardowy proces szkolenia w okresie letnim, analogicznie do ćwiczeń prowadzonych przez armię rosyjską (zwłaszcza w Zachodnim Okręgu Wojskowym, z którym armia białoruska tworzy wspólne tzw. Regionalne Zgrupowanie Wojsk). Zakłóceniu nie uległy także zobowiązania zewnętrzne SZ RB – w tygodniu po wyborach, żołnierze białoruscy wraz z wyposażeniem przemieścili się na terytorium Rosji i Uzbekistanu, gdzie wzięli udział w kilkunastu konkurencjach, rozpoczętych 23 sierpnia tzw. Międzynarodowych Igrzysk Wojskowych. Na Białorusi – jako goszczącej trzy konkurencje ww. Igrzysk – znaleźli się z kolei uczestniczący w nich wojskowi z innych państw.

Bezprecedensowe jest natomiast medialne wykorzystanie aktywności wojsk RB przez prezydenta Alaksandra Łukaszenkę, co wiąże się ze świadomym sterowaniem społecznym poczuciem strachu i niepewności. Większość przedsięwzięć szkoleniowych, które dotąd przez lata, a nawet dekady, przechodziły bez echa, obecnie jest szeroko nagłaśniana jako działania na rzecz zapewnienia bezpieczeństwa w sytuacji rzekomego zagrożenia militarnego ze strony zachodnich sąsiadów Białorusi. Po pierwszym tygodniu demonstracji Łukaszenka poinformował o podniesieniu jednostek na zachodniej granicy RB w stan pełnej gotowości bojowej. W połowie września z kolei, podczas przemówienia do uczestniczek zorganizowanego w Mińsku przez władze Forum Kobiet, wielokrotnie przywoływał zagrożenie wojną, która jakoby grozi regionowi. Oświadczył, że jest zmuszony „połowę armii postawić pod broń, i zamknąć granicę państwową od zachodu, przede wszystkim z Litwą i Polską". Wydaje się jednak, że słowa Łukaszenki miały głównie znaczenie propagandowe. W kolejnych dniach Państwowy Komitet Graniczny Białorusi poinformował, że Białoruś wzmocniła ochronę swoich granic, ale ruch odbywa się w normalnym trybie, a przejścia graniczne obsługują podróżnych w granicach normalnej przepustowości. Informacje te potwierdziła także Straż Graniczna. Budowana i podtrzymywana jest atmosfera zagrożenia z jednej strony agresją NATO (przekaz do zwolenników Łukaszenki), z drugiej zaś możliwością wykorzystania SZ RB dla stłumienia społecznego niezadowolenia (ten przekaz kierowany jest do zwolenników opozycji, także do państw zachodnich). Osobną kwestią jest sugerowanie przez Łukaszenkę siłowego wsparcia dla jego reżimu ze strony Rosji. Mimo tych propagandowych akcentów, wykorzystanie przez reżim armii białoruskiej

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

do ewentualnych działań siłowych na rzecz utrzymania władzy prezydenta Łukaszenki należy ocenić jako mało prawdopodobne. Świadczy o tym przede wszystkim charakter realizowanych przedsięwzięć szkoleniowych, w których zasadniczą rolę odgrywają formacje nieprzystosowane do pełnienia jakichkolwiek funkcji z zakresu zapewnienia porządku wewnętrznego (lotnictwo, obrona powietrzna, artyleria). Zaangażowanie formacji ogólnowojskowych (pancernych i zmechanizowanych) oraz powietrzno-desantowych – jedynych, których pododdziały mogłyby realizować np. działania blokadowe – w aktualnej fazie należy uznać za nieznaczne (demonstracyjnie zapowiadane przez Łukaszenkę przerzucenie na zachodnią granicę Białorusi 103. Brygady Desantowo-Szturmowej z Witebska zakończyło się standardowym ćwiczeniem jednego batalionu na poligonie Gożskim w Obwodzie Grodzieńskim). Na przeszkodzie dowolności w wykorzystaniu wojska stoją także fizyczne możliwości jednostek – zaangażowanie przedstawicieli większości związków taktycznych (brygad) SZ RB na poligonach, automatycznie angażuje praktycznie całą ich logistykę. Nie można wykluczyć, że w rzeczywistym zamiarze władz w Mińsku zaangażowanie żołnierzy – w części pochodzących z poboru – ma odwrócić ich uwagę od rozwoju wydarzeń na Białorusi i powstrzymać ewentualny wzrost nastrojów antyreżimowych w szeregach armii białoruskiej.

Również za mało prawdopodobne należy uznać zaangażowanie Sił Zbrojnych Federacji Rosyjskiej w utrzymanie reżimu Łukaszenki (pod pretekstem przeciwdziałania agresji NATO). Istniejące porozumienia – wielostronne w ramach Organizacji Układu o Bezpieczeństwie Zbiorowym (OUBZ) i dwustronne w ramach Państwa Związkowego Rosji i Białorusi (głównie dotyczące Regionalnego Zgrupowania Wojsk) dają Rosji stosunkowo dużą swobodę wjazdu i przemieszczania formacji wojskowych na terytorium Białorusi. Decyzję o podjęciu „obrony" Białorusi przed zewnętrzną agresją Moskwa może podjąć de facto bez porozumienia z Mińskiem, poprzez dowództwo Regionalnego Zgrupowania Wojsk. Podobnie jednak jak w przypadku armii białoruskiej, armia rosyjska – z racji wysokiego stopnia uzawodowienia i utechnicznienia – jest w jeszcze mniejszym stopniu przydatna do działań w zakresie zapewnienia porządku wewnętrznego.

Kwestią istotną dla Rosji jest utrzymanie wpływu na sposób działania białoruskich służb specjalnych i zachowanie dotychczasowej formuły współpracy, gdzie strona rosyjska zachowuje pozycję dominującą. W kontaktach z Rosją pozycję białoruskich resortów odpowiedzialnych za bezpieczeństwo osłabia przyjęcie zasady roboczych, bezpośrednich relacji z rosyjskimi odpowiednikami, co otwiera zainteresowanym instytucjom rosyjskim możliwość infiltracji białoruskiego systemu bezpieczeństwa. Obie strony koordynują działania z zakresu wspólnej ochrony białoruskiej granicy z państwami UE, zwalczania zorganizowanej przestępczości, terroryzmu, przemytu narkotyków i współpracy wywiadowczej przeciwko NATO. Służby białoruskie przyzwalają często na swobodne działanie rosyjskiego FSB na terytorium Białorusi, czy też przekazują informacje będące w zainteresowaniu służb rosyjskich. W przypadku kontynuowania przez władze RB polityki tłumienia protestów społecznych, białoruski sektor siłowy może oczekiwać udzielenia przez Rosję pomocy materiałowej. W przypadku wyczerpywania się potencjału białoruskich sił porządkowych istnieje możliwość formalnego wsparcia pododdziałów rosyjskiej Gwardii Narodowej, np. w miastach wschodniej Białorusi, co zapowiedział prezydent W. Putin deklarując gotowość utworzenia tzw. sił rezerwowych, mogących w razie potrzeby udzielić pomocy białoruskim organom porządkowym.

Jednocześnie narasta konfrontacja w stosunkach Mińska z Zachodem. 29 września białoruski MSZ wprowadził sankcje wizowe wobec ok. 300 polityków, działaczy społecznych i dziennikarzy z Litwy, Łotwy i Estonii, które jako pierwsze w UE zdecydowały się na wprowadzenie zakazu wjazdu dla blisko 130 przedstawicieli białoruskich władz, odpowiedzialnych za fałszerstwa wyborcze i represje. W reakcji na unijną listę sankcyjną opublikowaną 2 października (zawierającą 44 nazwiska, wkrótce oczekiwana jest decyzja umieszczenia na liście Łukaszenki), Mińsk błyskawicznie wprowadził analogiczne sankcje wizowe wobec – jak to określono –„najbardziej uprzedzonych" do białoruskich władz przedstawicieli państw członkowskich oraz instytucji unijnych, w tym Parlamentu Europejskiego. Wszystkie listy sankcyjne Mińska mają charakter niepubliczny. Białoruski MSZ podkreślił przy tym, iż ograniczenia te będą obowiązywały również w Rosji, co potwierdziła rzeczniczka rosyjskiego MSZ. Ponadto, Mińsk zażądał od Polski i Litwy znaczącego zredukowania,

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

do 9 października, personelu dyplomatycznego (w przypadku polskich placówek – z 50 do 18 dyplomatów, zaś litewskich – z 25 do 14) i wezwania ambasadorów z tych państw na konsultacje do swoich stolic. Z kolei do Mińska zostali wezwani szefowie białoruskich placówek w Wilnie i Warszawie. Swoją decyzję białoruski MSZ uzasadnił „destrukcyjną działalnością" ze strony tych państw. Władze Białorusi zapowiedziały również przeprowadzenie ponownej akredytacji wszystkich korespondentów zagranicznych mediów.

Stanowcza reakcja białoruskiego MSZ na sankcje wizowe państw bałtyckich oraz całej UE potwierdza zupełny brak zainteresowania podjęciem rozmów w celu uregulowania kryzysu. Jest to również równoznaczne z wycofaniem się białoruskiej dyplomacji z próby jakichkolwiek konstruktywnych działań w polityce wobec Zachodu. Rezultatem konfrontacyjnej postawy Mińska jest najgłębszy kryzys w stosunkach z Zachodem po 1991 r. Jego efektem będzie daleko idąca izolacja międzynarodowa Białorusi, przy jednoczesnym zwiększeniu dominacji Rosji.

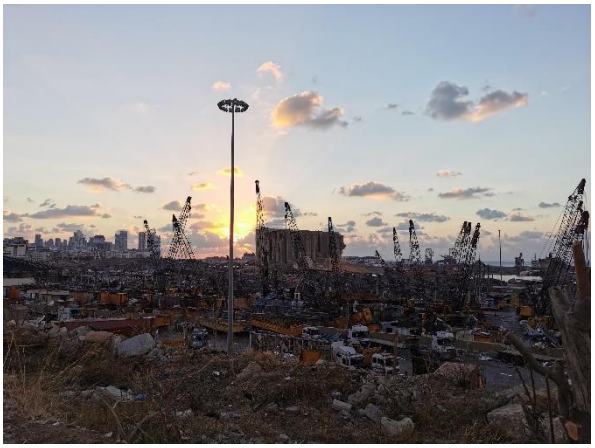
Na ratunek Libanowi

Grzegorz Borowiec

Oficer Łącznikowy USAR Poland, Komenda Główna Państwowej Straży Pożarnej

4 sierpnia br. o godzinie 18:10, najprawdopodobniej podczas wykonywania prac spawalniczych przy jednym z magazynów zlokalizowanych w bejruckim porcie (sekcja 12 portu), doszło do pożaru, a następnie eksplozji zgromadzonych wewnątrz magazynu materiałów chemicznych (azotan amonu, potocznie zwany saletrą amonową).

Eksplozja wywołała falę detonacyjną, która zniszczyła doszczętnie port oraz zgromadzone w portowych magazynach zapasy, w tym skład leków i materiałów ochronnych do walki z COVID-19, a także główny magazyn zboża dla Libanu. Zniszczeniu uległy 3 szpitale, a kolejne 2 zostały poważnie uszkodzone. Skutki wybuchu można było zaobserwować nawet w odległości ok. 10 kilometrów od epicentrum. Śmierć poniosło 190 osób, 6,5 tys. zostało rannych, a co najmniej 250 tys. osób pozostało bez dachu nad głową. Paradoksalnie, największy w Libanie silos zbożowy, wypełniony po brzegi ziarnem, przyczynił się do znacznego pochłonięcia energii eksplozji i powstrzymał częściowo falę uderzeniową przesuwającą się w kierunku zachodnim, przez co zniszczenia w dzielnicach na zachód od portu były zdecydowanie mniejsze.



UNIJNY MECHANIZM OCHRONY LUDNOŚCI

Państwowa Straż Pożarna, jako profesjonalna służba ratownicza, poza realizowaniem ustawowych zadań związanych z ratowaniem życia, zdrowia oraz zagrożonego mienia na terenie Rzeczpospolitej Polskiej, niejednokrotnie zaangażowana była w udzielanie pomocy ratowniczej poza granicami kraju. Po podpisaniu traktatu akcesyjnego do Unii Europejskiej, Polska stała się jednocześnie członkiem Mechanizmu Wspólnotowego Unii Europejskiej.

Unijny Mechanizm Ochrony Ludności jest systemem międzynarodowej pomocy ratowniczej, nadzorowanym i organizowanym przez Dyrekcję Generalną ds. Pomocy Humanitarnej i Ochrony Ludności (DG ECHO) Komisji Europejskiej. System ma na celu wspieranie państw/regionów całego świata, które dotknięte zostały katastrofą o skutkach wymagających międzynarodowej interwencji ratowniczej. W ramach Mechanizmu na miejsce katastrofy mogą zostać skierowane:

- specjalistyczne grupy ratownicze (moduły) tworzone przez kraje członkowskie Mechanizmu (27 krajów członkowskich UE oraz Wielką Brytanię, Islandię, Czarnogórę, Norwegię, Serbię, Macedonię Północną oraz Turcję);
- eksperci określonych specjalizacji, niezbędni na miejscu zdarzenia (wybierani przez Komisję

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

w oparciu o bazę danych zawierającą informacje na temat ww. ekspertów z terenu całej UE).

Moduły ochrony ludności tworzone są na zasadzie dobrowolności na bazie krajowych zasobów z jednego z państw członkowskich lub większej ich liczby. Przyczyniają się do rozwoju zdolności szybkiego reagowania w dziedzinie ochrony ludności, do którego wezwała Rada Europejska w swych konkluzjach z posiedzenia, które odbyło się 16 i 17 czerwca 2005 r. oraz Parlament Europejski w swej rezolucji z 13 stycznia 2005 r. w sprawie klęski tsunami.

Aby moduły ochrony ludności mogły właściwie reagować w obliczu poważnych katastrof, powinny spełniać określone wymagania przedstawione w Decyzji Komisji z 16 października 2014 r., ustanawiającej zasady wdrażania decyzji Parlamentu Europejskiego i Rady Europy nr 1313/2013/UE w sprawie Unijnego Mechanizmu Ochrony Ludności oraz uchylającej decyzję Komisji 2004/277/WE, Euroatom oraz 2007/606/WE, Euroatom.

Obecnie Polska dysponuje następującymi zasobami do działań międzynarodowych:

- 1 moduł średniej grupy poszukiwawczo-ratowniczej przeznaczonej do działań na terenach miejskich (MUSAR);
- 1 moduł ciężkiej grupy poszukiwawczo-ratowniczej przeznaczonej do działań na terenach miejskich (HUSAR);
- 4 moduły pomp wysokiej wydajności (HCP);
- 4 moduły wykrywania skażeń chemicznych, biologicznych, radiologicznych i jądrowych oraz pozbieranie próbek (CBRN);
- 6 modułów gaszenia pożarów lasów z ziemi, z użyciem pojazdów (GFFFV).

Z tego w systemie CECIS[1] zarejestrowane zostały:

- 1 moduł średniej grupy poszukiwawczo-ratowniczej przeznaczonej do działań na terenach miejskich (MUSAR);
- 1 moduł ciężkiej grupy poszukiwawczo-ratowniczej przeznaczonej do działań na terenach miejskich (HUSAR);
- 2 moduły pomp wysokiej wydajności (HCP);
- 1 moduł wykrywania skażeń chemicznych, biologicznych, radiologicznych i jądrowych oraz pozbieranie próbek (CBRN);
- 3 moduły gaszenia pożarów lasów z ziemi, z użyciem pojazdów (GFFFV).

DZIAŁANIA USAR POLAND W LIBANIE

Premier Libanu, Hassan Diab zwrócił się do społeczności międzynarodowej, w tym także do Unijnego Mechanizmu Ochrony Ludności Unii Europejskiej z formalną prośbą o pomoc, która obejmowała zapotrzebowanie na:

- grupy ratownicze do pobierania próbek powietrza i ich badania pod kątem zawartości substancji chemicznych (CBRN);
- 5 grup poszukiwawczo-ratowniczych (USAR), w tym 1 ciężka (HUSAR) i 4 średnie (MUSAR);
- sprzęt ochrony dróg oddechowych;
- zespoły strażaków do gaszenia pożaru statku, znajdującego się w porcie;
- sprzęt ochrony osobistej oraz sprzęt i leki do prowadzenia operacji medycznych w szpitalach;
- aktywację usługi obrazowania satelitarnego „Copernicus".

Prośba ta została przekazana przez centrum koordynacyjne ERCC w Brukseli do „Krajowych Punktów Kontaktowych" ds. Mechanizmu Ochrony Ludności, czyli w Polsce do całodobowego Stanowiska Kierowania Komendanta Głównego Państwowej Straży Pożarnej (SK KG PSP) mieszczącego się w Krajowym Centrum Koordynacji Ratownictwa i Ochrony Ludności (KCKRiOL). Rozpoczęła się procedura zgłaszania przez unijny system CECIS ofert pomocy z krajów członkowskich do Komisji Europejskiej, która przekazywała oferty do akceptacji Libanu.

Minister Spraw Wewnętrznych i Administracji podjął decyzję o wysłaniu do Libanu średniej Grupy Poszukiwawczo-Ratowniczej PSP, certyfikowanej wg kryteriów Międzynarodowej Grupy Doradczej ds. Poszukiwań i Ratownictwa (ang. INSARAG). Z uwagi na charakter zdarzenia, do grupy dołączono 4 strażaków – specjalistów z zakresu CBRN, wyposażonych w sprzęt do detekcji substancji niebezpiecznych. W środę (5 sierpnia) o godz. 15.35 polska oferta pomocy została zaakceptowana. Polscy ratownicy ze Specjalistycznych Grup Poszukiwawczo-

[1] **The Common Emergency Communication and Information** – System Komunikacji i Informacji Kryzysowej – system teleinformatyczny utworzony dla zapewnienia komunikacji pomiędzy państwami członkowskimi Unijnego Mechanizmu Ochrony Ludności oraz pomiędzy państwami członkowskimi i ERCC w Brukseli. CECIS jest jednym zasadniczych elementów mechanizmu z uwagi na fakt, że powinien on zagwarantować autentyczność, integralność i poufność informacji wymienianych między państwami uczestniczącymi w mechanizmie w rutynowych warunkach, jak również we wszelkiego rodzaju sytuacjach krytycznych.

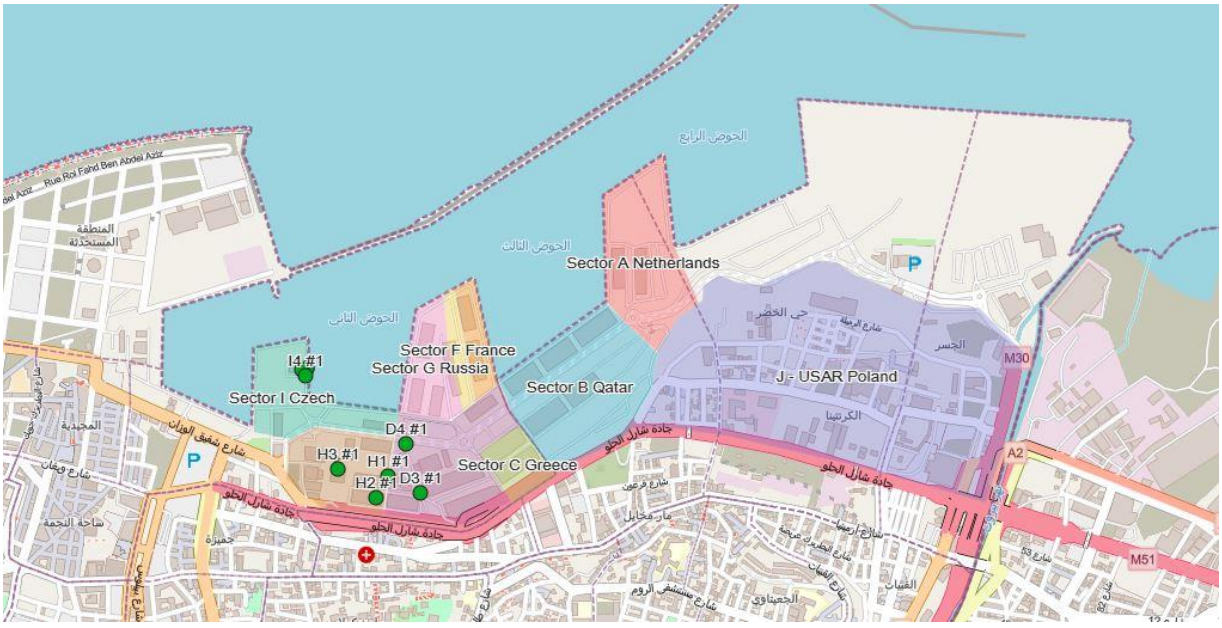
Rządowe Centrum Bezpieczeństwa
ul. Rakowiecka 2a, 00-993 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

Ratowniczych w Łodzi, Poznaniu, Nowym Sączu, Warszawie, Gdańsku, a także ratownicy z Komendy Głównej Państwowej Straży Pożarnej, gotowi byli do wylotu już o godzinie 17:30, kiedy to dotarli na lotnisko Chopina w Warszawie wraz z całym niezbędnym wyposażeniem. Po załadowaniu do samolotu dodatkowej pomocy humanitarnej (darowizny z Agencji Rezerw Materiałowych), grupa ratownicza PSP „Liban 2020" w składzie 42 ratowników oraz 4 psy ratownicze, a także 11 ton sprzętu, o godzinie 23:00 wystartowała do Bejrutu.

Bezpośrednio po wylądowaniu (6 sierpnia) wszyscy ratownicy poddani zostali badaniu na obecność COVID-19. Grupa została skierowana do bazy Marynarki Wojennej Libanu. Miejsce to, oddalone w linii prostej o około 500 metrów od epicentrum wybuchu, wskazane zostało jako miejsce na obozowisko. Do momentu otrzymania wyników badania na obecność koronawirusa, ratownicy rozstawili pełną infrastrukturę obozowiskową wraz z zapleczem sanitarnym.

O godzinie 11.00 po otrzymaniu wyników testów, odbyło się spotkanie Dowódców Grup USAR, na którym ustalono sposób koordynacji prac. Wiodącą rolę otrzymała armia libańska, wspierana przez komórkę ds. koordynacji prac USAR (ang. USAR Coordination Cell), do której każda z grup delegowała swoich przedstawicieli. Podczas spotkania przydzielono również sektory robocze dla poszczególnych grup. Polscy ratownicy dostali do przeszukania sektor H. Ze względu na ograniczenia narzucone przez wojsko (między innymi zakaz pracy po zmroku) Dowódca Grupy zdecydował o równoczesnym zadysponowaniu obu zespołów roboczych – w standardowych warunkach grupa MUSAR gotowa jest do działania 24/7 w jednym sektorze, wykorzystując 2 zespoły robocze rotacyjnie.

Następnego dnia (7 sierpnia), po zakończeniu działań w sektorze H, w którym nie stwierdzono obecności osób poszkodowanych, Grupa USAR Poland jako jedyna uzyskała zgodę na rozpoczęcie działań poszukiwawczo-ratowniczych poza portem. Sektor J podlegający jurysdykcji Obrony Cywilnej Libanu stanowił ogromne wyzwanie. Liczba obiektów oraz wielkość sektora, a także liczne budynki mieszkalne dawały spore szanse na odnalezienie poszkodowanych. Polscy ratownicy otrzymali zadanie przeprowadzenia przeszukania budynków oraz przeszkolenia lokalnych strażaków w zakresie technik poszukiwawczo-ratowniczych.



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

Do działań w sektorze J skierowano oba zespoły ratownicze oraz ekspertów CBRN. W trakcie działań jeden z psów ratowniczych wskazał miejsce, gdzie potencjalnie mógł znajdować się żywy poszkodowany, jednak po weryfikacji miejsca przy pomocy specjalistycznego sprzętu, nie potwierdzono obecności osób żywych. Po dwóch dniach działań i gruntownym przeszukaniu wszystkich zawalonych obiektów stwierdzono, że pod gruzami nie przebywają żadne osoby poszkodowane.

8 sierpnia w godzinach popołudniowych Rząd Libanu ogłosił zakończenie fazy ratowniczej działań. Wraz z tą decyzją zakończyły się poszukiwania osób zaginionych, a wszyscy ratownicy powrócili do obozowiska. Grupa opuściła Liban 10 sierpnia o godz. 16.30.

Terroryzm nadal poważnym zagrożeniem dla światowego bezpieczeństwa

Sebastian Wojciechowski
Instytut Zachodni i UAM w Poznaniu

Pomimo pandemii COVID-19, stanowiącej jeden z największych problemów globalnych, także w aspekcie bezpieczeństwa, świat cały czas zmagać się także musi z wieloma innymi, bardzo zróżnicowanymi zagrożeniami i wyzwaniami. Wśród nich kluczową rolę wciąż odgrywa problem terroryzmu. Wbrew potocznym opiniom, w minionym roku, pomimo rozbicia ISIS, liczba ataków terrorystycznych na świecie nie uległa obniżeniu.

Sytuację związaną z zagrożeniem terrorystycznym szczegółowo ukazuje najnowszy raport Departamentu Stanu ,,Country Reports on Terrorism 2019'' z którego wynika, że w skali globu odnotowano o 3% incydentów terrorystycznych więcej niż w 2018 r. (wzrost do 8 302 przypadków). Dotyczyły one prawie 90 państw, a aż 84% koncentrowała się w trzech regionach geograficznych: Azji Zachodniej, Azji Południowej i Afryce Subsaharyjskiej. Wśród państw szczególnie zagrożonych terroryzmem wymienić należy: Afganistan, Syrię, Indie, Irak, Somalię, Nigerię, Jemen, Filipiny, Kolumbię i Kongo (łącznie 74% wszystkich ataków). Absolutnym liderem wciąż pozostaje Afganistan, gdzie bardzo znacząco (+35%) wzrosła liczba ataków (do 1 750 w 2019 r.). Na drugim miejscu była Syria +18% (1 028), a na trzecim, co może być sporym zaskoczeniem, Indie – mimo spadku o 2% (655 incydentów).

W minionym roku, jak wynika z powyższego raportu, na skutek ataków terrorystycznych zginęło 25 082 osób (spadek w porównaniu z 2018 r. o 24%), 19 924 odniosło rany (-12%), a ponadto odnotowano 2 895 porwań (-18%). Najwięcej ofiar (zabici i ranni) zarejestrowano w Afganistanie (ponad 16 tys.) oraz Syrii (prawie 5 tys.). Na szczególną uwagę zasługuje przypadek Afganistanu, gdzie było 36% wszystkich światowych ofiar terroryzmu. Wśród nich w skali globu największą grupę stanowili mundurowi (30%), a w dalszej kolejności ,,miejscowa społeczność'' (27%) oraz urzędnicy (19%). Wskaźniki te były jednak dość mocno zróżnicowane w poszczególnych częściach świata, co wynikało z profilu działających tam organizacji. Na przykład Boko Haram czy ISIS częściej atakowały ,,miejscową społeczność'', a Talibowie albo al-Shabaab przedstawicieli wojska i rządu. Różnorodne były również metody stosowane przez terrorystów obejmujące łącznie około 30 różnorodnych form działania. Na przykład: 41% przypadków to użycie broni palnej, 15% min oraz improwizowanych ładunków wybuchowych, 13% ataki bombowe, 3% porwania, 3% uszkodzenia mienia, a 2% zamachy samobójcze.

Sprawcami ataków były przede wszystkim osoby powiązane z różnymi formacjami terrorystycznymi. Łącznie w raporcie scharakteryzowano ich ponad 60. Do najbardziej niebezpiecznych, a zarazem aktywnych grup zaliczono: Talibów (1 459 incydentów, w porównaniu z 2018 r. wzrost +35%), The Islamic State in Iraq and Syria – ISIS (575, spadek -11%), al-Shabaab (484, spadek -10%), Communist Party of India-Maoist (292, wzrost +65%) oraz Boko Haram (272, wzrost +24%). Podkreślić przy tym należy, iż Departament Stanu osobno rozpatruje poszczególne grupy afiliowane czy współpracujące z ISIS. Wskazano ich łącznie 19 na obszarze 26 państw. Tylko w 2019 r. doprowadziły one do ponad 900 incydentów

terrorystycznych. Podobny przypadek dotyczy grup funkcjonujących w ramach tzw. sieci Al-Qaidy, które wymieniono w raporcie 10. W minionym roku były one łącznie odpowiedzialne za ponad 700 zdarzeń o charakterze terrorystycznym.

Ważnym, z punktu widzenia terrorystów, celem ataków wciąż pozostaje Unia Europejska. Choć w skali całego świata ataki terrorystyczne w tym regionie nie są obecnie częste (kilka procent ogółu) i ich liczba spada, to jednak UE ze względu na znaczenie polityczne, ekonomiczne czy medialne, a także z uwagi na występujące w jej obrębie różnice kulturowo-religijne nadal jest istotnym ich celem. Potwierdzają to m.in. informacje zamieszczone w najnowszym raporcie Europolu ,,European Union Terrorism Situation and Trend Report 2020'' (TE-SAT, 2020) obejmującym przede wszystkim wydarzenia, które miały miejsce w 2019 roku.

W zeszłym roku na obszarze UE zarejestrowano 119 nieudanych, udaremnionych i przeprowadzonych ataków terrorystycznych. Jest to ich najniższy poziom od wielu lat. Dla porównania w 2018 r. było 129, a w 2017 r. 205 przypadków. Taka sytuacja wynika przede wszystkim ze zwiększonej współpracy i skuteczności w zakresie zwalczania terroryzmu (np. jak poinformowały brytyjskie służby w ciągu trzech ostatnich lat udaremniły 25 ataków, z kolei we Francji atak, statystycznie rzecz biorąc, udaremniany jest raz w miesiącu), osłabienia wpływów i oddziaływania między innymi ISIS czy ograniczenia napływu ich zwolenników, w tym powrotu osób walczących w szeregach terrorystów. W analizowanym okresie do ataków terrorystycznych doszło w 13 państwach członkowskich UE. Najwięcej spośród nich miało miejsce w Wielkiej Brytanii – 64, Włoszech – 28 i Francji – 7. Ponadto, 4 przypadki zarejestrowano w Grecji, po 3 w Niemczech i Hiszpanii, po 2 w Czechach, Danii i Niderlandach oraz po 1 w Belgii, Bułgarii, Polsce i na Litwie. Prawie połowa ataków (57) miała podłoże nacjonalistyczno-separatystyczne (niemal wszystkie dotyczyły W. Brytanii). Po raz kolejny zatem nie znalazła potwierdzenia dość powszechna, choć błędna, opinia o dominacji na obszarze Unii ataków o podłożu islamistycznym. Ponadto, 26 zamachów sklasyfikowano jako skrajnie lewicowe (głównie Włochy oraz Grecja i Hiszpania), 21 dżihadystyczne (Francja, Niemcy, W. Brytania, Niderlandy, Włochy, Dania, Belgia oraz Bułgaria), 6 skrajnie prawicowe (W. Brytania, Litwa i Polska). Oprócz tego 6 ataków nie zaliczono do żadnej kategorii, a 3 przypadki uznano za tzw. terroryzm jednej sprawy. W porównaniu z 2018 r. oznacza to wzrost incydentów o podłożu skrajnie prawicowym (z 1 do 6) i skrajnie lewicowym (z 19 do 26) oraz spadek tych, wynikających z pobudek dżihadystycznych (z 24 do 21) i nacjonalistyczno-separatystycznych (z 83 do 57). W 2019 r. w wyniku ataków terrorystycznych na obszarze UE zginęło 10 osób, a 27 zostało rannych. Wszystkie zgony, a także obrażenia 26 ofiar były skutkiem działalności islamistów, natomiast jedna osoba została ranna w następstwie ataku skrajnie prawicowych terrorystów. Jest to znacząca zmiana skali tego zjawiska, albowiem np. w 2017 r. zabito 62 osoby i zraniono 844.

O tym, iż terroryzm wciąż pozostaje poważnym zagrożeniem dla UE świadczy między innymi duża liczba osób aresztowanych z tego powodu (1 004). W 2018 r. takich przypadków było 1 056. W minionym roku najwięcej zatrzymanych utożsamiało się z ideologią dżihadystyczną 436 (rok wcześniej 511) – prawie połowa przypadków dotyczyła Francji. Znacząco wzrosła także (z 34 w 2018 r. do 111 w 2019 r.) liczba osób aresztowanych za skrajnie lewicową działalność terrorystyczną (głównie we Włoszech). W tym samym okresie obniżył się natomiast odsetek zatrzymanych i podejrzewanych o skrajnie prawicowy terroryzm (z 44 do 21). Innym przykładem skali zagrożenia, ale również zaangażowania poszczególnych państw UE w walkę z terroryzmem jest zamieszczone w raporcie zestawienie dotyczące zakończonych postępowań sądowych w sprawie przestępstw terrorystycznych. W zeszłym roku odnotowano ich 520, a w 2018 r. – 664. Utrzymywanie się wysokiego poziomu zagrożenia atakami potwierdza też dalsze zaostrzanie lub niełagodzenie przez niektóre państwa przepisów dotyczących zwalczania terroryzmu (m.in. kazus Francji, Niemiec czy Wielkiej Brytanii).

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

Terroryzm nadal pozostaje poważnym światowym zagrożeniem, o czym świadczy m.in. ponad 8 tys. incydentów, które miały miejsce w minionym roku. Statystycznie rzecz biorąc oznacza to ponad 20 tego typu zdarzeń dziennie. Najbardziej aktywnym, a zarazem niebezpiecznym sprawcą ataków terrorystycznych na świecie są Talibowie, którzy ponoszą odpowiedzialność za 18% ogółu ataków (około 1,5 tys.). Jest to wzrost o 35% w porównaniu do roku poprzedniego. Bardzo groźne, pomimo spadku aktywności, są wciąż grupy pośrednio lub bezpośrednio powiązane z ISIS (łącznie ponad 900 incydentów) czy Al-Qaidą (ponad 700). Poziom współczesnego zagrożenia terrorystycznego oceniać należy nie tylko w oparciu o informacje dotyczące liczby nieudanych, udaremnionych i przeprowadzonych ataków oraz towarzyszących temu ofiar. Choć są to bardzo ważne wskaźniki, trzeba je jednak uzupełnić o inne kluczowe dane, takie, jak na przykład: liczba osób aresztowanych i skazanych z powodu terroryzmu, skala pozyskiwanych przez terrorystów środków finansowych oraz werbowanych osób, zakres i skuteczność propagandy terrorystycznej, poziom społecznego poparcia dla ich działalności oraz wsparcia z zewnątrz, a także wiele innych aspektów.

Ransomware w nowej odsłonie

Ireneusz Tarnowski

ekspert ds. cyberzagrożeń w Santander Bank Polska

Po atakach WannaCry, czy Petya/NotPetya wydawało się, że powiedziane zostało już wszystko, a my poznaliśmy techniki i motywację cyberprzestępców. Jednak za sprawą wykorzystania nowych technik oraz wielu wektorów szantażu, od końca 2019 r., obserwujemy znaczące zmiany i wzrost skuteczności przestępców. Po masowych, niszczących atakach, pojawił się model Ransomware-as-a-Service (RaaS) i dobrze przygotowane ataki na mniejsze firmy i instytucje. Malware tego typu stał się produktem w świecie cyberprzestępców. W pewnym momencie odporność na samą niedostępność danych (główny cel takiego ataku) wzrosła na tyle, że prowadzone operacje przez cyberprzestępców nie były już tak atrakcyjne. Przestępcy znaleźli inny sposób na to, jak zarabiać na ransomware – dodano szantaż związany z ujawnieniem wrażliwych danych. Z nowym modus operandi pojawiły się nowe techniki. Ataki te są bardziej hybrydowe i skomplikowane, wykorzystując taktyki oraz techniki znane dla innego rodzaju cyberataków.

PIERWSZE ATAKI ŻĄDANIA OKUPU

Ransomware to rodzaj ataku DoS (Denial-of-Service, niedostępność usługi lub systemu komputerowego). W swej idei ma on na celu zatrzymać możliwość pracy na komputerze. Historycznie, pierwszym ransomware był złośliwy program AIDS, którego działanie polegało na szyfrowaniu nazw plików na dysku C. Począwszy od roku 2005, wraz z powszechnością internetu, zaczęły pojawiać się złośliwe programy, które blokowały ekran oraz wybrane funkcje systemu Windows, uniemożliwiając pracę. W pierwszych atakach ofiary wybierano losowo, wykorzystując metodę „wodopoju". Szybko jednak opracowano instrukcje w jaki sposób ją zneutralizować i przywrócić komputer do pełnej funkcjonalności. W tych pierwszych atakach wyświetlano komunikat podszywający się pod Policję, czy inne służby bezpieczeństwa i grożono konsekwencjami w przypadku nie zapłacenia kary. Od roku 2013 cyberprzestępcy zaczęli używać ransomware szyfrującego pliki. Pojawił się malware o nazwie Cryptolocker, który rozprzestrzeniał się za pośrednictwem zainfekowanych stron internetowych i złośliwych załączników do wiadomości e-mail. Utworzenie kryptowalut (Bitcoin, 2009) stworzyło metodę, by opłata okupu stała się anonimowa. To znacząco uprościło schemat działania przestępców. Cryptolocker używał algorytmu AES-256 do szyfrowania plików oraz wykorzystywał serwery zarządzające (Command and Control, C2) rozproszone w botnecie Zeus, a komunikacja pomiędzy ofiarą a serwerem dystrybuującym klucze do odszyfrowania odbywała się przez sieć Tor. Wszystkie te techniki sprawiły, że znacznie trudniej było wyśledzić stojących za tymi atakami przestępców. Użycie serwerów zarządzających (C2) przez Cryptolockera znacząco przyczyniło się do jego upadku. Botnet Zeus został w dużej części zniszczony

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

w 2014 roku i malware opierający swoje działanie na infrastrukturze Zeusa przestał być groźny.

WANNACRY, PETYA, NOTPETYA

12 maja 2017 r. nastąpił światowy atak WannaCry [7][8], po którym każdy już usłyszał i zrozumiał znaczenie ransomware. Można powiedzieć, że nowy malware stanowił połączenie dwóch dobrze znanych technik:

- Szyfrowanie zawartości dysku (jak typowy cryptoloker);
- Samodzielne rozprzestrzenianie się w sieciach komputerowych, jak typowy wirus typu robak (wykorzystywał lukę w obsłudze protokołu Microsoft Server Message Block 1.0 (SMBv1) pozwalającą na zdalne wykonanie dostarczonego kodu na komputerze ofiary. Jest to podatność, którą opublikował Microsoft 17.03.2017 roku w biuletynie bezpieczeństwa MS17-010; kod wykorzystujący tę podatność to eksploit EternalBlue).

W 2018 roku odpowiedzialność za ten atak przypisano grupie hackerskiej Lazarus (APT38).

Niespełna miesiąc po zawirowaniach wynikających z WannaCry, świat odczuł kolejny bardzo destrukcyjny atak. W dniach 27–28.06.2017 r. zaatakowane zostały niemal wszystkie systemy komputerowe na Ukrainie. Wektorem ataku było oprogramowanie księgowego o nazwie MEDoc, używane przez każdą firmę, która rozliczała się z podatków lub prowadziła przedsiębiorstwo. Atak tym samym obejmował około 400 000 klientów, co stanowiło 90% krajowych firm. Początkowo uznawano, że to ransomware Petya (obserwowane zachowanie i ekran okupu był taki sam), jednak po dokładniejszych analizach uznano, że to inny malware, nazwano go NotPetya. NotPetya za pomocą MEDoc podczas startu pobrał uaktualnianie serwera upd.me-doc[.]ua. Okazało się, że backdoor był obecny w systemie aktualizacji już od kwietnia. Wyznaczonego dnia, o wyznaczonej godzinie rozpoczął szyfrowanie komputerów. Podczas zakończenia szyfrowania Master File Table (MFT – umożliwiał dostęp do plików na komputerze) wyświetlone zostało żądanie okupu. Malware został uzbrojony w możliwość propagacji przez sieć poprzez eksploity takie jak: Eternalblue i Eternalromacne, Doublepulsar (podobnie jak WannaCry). Ze względu na powiązania biznesowe światowych koncernów z ukraińskimi firmami, zainfekowane zostały duże korporacje (jedna z największych to Maersk). W dalszych analizach ustalono, że atak NotPetya nie miał na celu wymuszenie okupu. Z pozoru tak wyglądał, lecz w istocie był to destrukcyjny atak niszczący zawartość dysków (tzw. wiper). Do tej pory nie dokonano dla niego pewnej atrybucji.

EWOLUCJA ATAKÓW I NOWA GENERACJA RANSOMWARE

Przestępcy zauważyli, że ataki stały się nieopłacalne, gdyż ofiary nie płaciły okupu. Natomiast stałe poprawianie złośliwego kodu to koszt. W pewnym momencie jeden z malware – GrandGrab, który był zaawansowanym koniem trojańskim z opcją szyfrowania plików, zmienił swój model biznesowy. Jego twórca postanowił poprawić narzędzie i zrobić z niego usługę internetową. W ten sposób powstał model RaaS – Ransomware-as-a-Service [9]. Oprogramowanie musiało być stale rozwijane i uwzględniać nowe podatności do wykorzystania oraz nowe techniki detekcji (aby je omijać). W połowie 2019 roku twórca tego oprogramowania ogłosił sprzedaż kodów malware [10]. Początkowo wszyscy myśleli, że era ataków wymuszających okup, w których szyfrowane są dyski dobiega końca. Największy program nie jest już rozwijany, firmy stały się odporne, a dostarczenie malware i infekcja jest coraz trudniejsza. Pojawił się następca – Sodinokibi. Przyjmuje się, że na bazie kodów GrandCrab wytworzona została nowa generacja malware.

31 grudnia ub.r. przeprowadzono skuteczny cyberatak na Travelex – jedną z największych na świecie firm obsługujących wymianę walut. Najpierw wykradziono około 5 GB danych, a następnie rozpoczęto szyfrowanie systemów. Początkowo przestępcy domagali się 3 mln dolarów okupu, jednak szybko zwiększyli wysokość żądania do 6 mln dolarów. To często stosowana strategia – szybka płatność daje niższą cenę, a gdy ofiara zastanawia się za długo, opłata za odszyfrowanie rośnie. Jednakże w tym przypadku przestępcy żądali okupu nie tylko za odblokowanie dostępu do systemów, ale także za nieupublicznianie wykradzionych z firmy informacji. Przedmiotem kradzieży padły wrażliwe dane klientów firmy Travelex, w tym numery kart kredytowych i informacje o transakcjach finansowych. Atak najprawdopodobniej udał się dzięki brakom w aktualizacjach krytycznych usług. Przestępcy bacznie poszukują najsłabszego punktu w organizacjach. Takim punktem w firmie Travelex

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

była infrastruktura, a dokładniej serwery VPN Pulse Secure.

CVE-2019-11510 to krytyczna luka w zabezpieczeniach, upubliczniona 22 marca 2019 r., umożliwiająca zdalne ujawnienie plików w Pulse Connect Secure. Wykorzystanie tej luki jest bardzo łatwe – poziom jej ważności wyceniono na 10 w dziesięciostopniowej skali Common Vulnerability Scoring System (CVSS). Błąd może pozwolić zdalnemu, nieuwierzytelnionemu atakującemu na uzyskanie nazw użytkowników i haseł w postaci jawnego tekstu z podatnych serwerów. Luka została wykorzystana do uzyskania dostępu do sieci wewnętrznej. Mając dostęp do wewnętrznej infrastruktury (poprzez przejęte serwery VPN) malware wykorzystał podatność związaną z deserializacją w serwerze Weblogic (CVE-2019-2725) oraz podatność typu Elevation of Privilege w sterowniku Win32k (CVE-2018-8453) w systemie Windows. W ten sposób uzyskano konto i uprawnienia administratora domeny. Do poruszania się po sieci (element Lateral Movement) wykorzystano VNC, zainstalowano psexec jako plik java.exe. Następnie wyłączono mechanizmy bezpieczeństwa na komputerach końcowych, a malware Sodinokibi został przekazany do wszystkich systemów przez psexec.

To był przypadek, w którym stawką nie było tylko odzyskanie danych, aby zapewnić utrzymanie ciągłości działania firmy, ale także ochrona ich poufności. Finalnie przestępcy opublikowali najpierw próbkę danych, po czym wszystkie, wykradzione informacje.

Atak ten otworzył nową epokę ataków ransomware – opłata za nieujawnianie tajemnic firmowych.

NOWY MODEL OPERACYJNY

Przestępcy wyszukują luki w infrastrukturze (znane podatności, słabe hasła, błędy konfiguracyjne) i zdobywają tzw. przyczółek w organizacji. Nie atakują zwykłych internautów, lecz skupiają się na dużych korporacjach, bankach, instytucjach, ministerstwach. W kolejnym kroku starają sie przejąć kontrolę nad jak największą liczbą komputerów, poprzez przejęcie kluczowych systemów (np. Serwer Active Directory) lub zdobyć systemy z wartościowymi informacjami, np. serwery plików, systemy finansowe, czy też serwery zespołów naukowych R&D. Kluczowym elementem ataku, jest wytransferowanie plików z firmy i zaszyfrowanie tych, które pozostały. Na końcu pozostaje publiczne ogłoszenie ataku i negocjacje cenowe.

Analiza znanych ataków z 2020 roku pokazuje, że istnieje 67 znanych podatności, z których korzystają przestępcy do przełamania zabezpieczeń, podniesienia uprawnień oraz propagacji malware po wewnętrznej infrastrukturze [1][2][3].

Od 1 stycznia 2020 r. do 25 września 2020r. zarejestrowano 700 ofiar tego typu ataków oraz 17 grup cyberprzestępców [4]. Grupy te związane są poszczególnymi rodzinami złośliwego oprogramowania i są to: Maze, Sodinokibi (REvil), Netwalker, WestedLocker, RagnarLocker, Conti, DoppelPaymer, Nefilim, AKO, Sekhmet, Suncrypt, DarkSide, Avaddon, Clop.

Każda z grup publikuje listę swoich ofiar wraz z informacjami o etapie negocjacji. Najbardziej znane ofiary ataków to:

- Garmin – malware WastedLocker, potwierdzone zapłacenie 10 mln dolarów okupu;
- Banco Estado Chile – malware Sodinokibi;
- Canon USA – malware Maze;
- Orange S.A. – malware Nefilim;
- The Volksvagen Group – malware Conti.

JAK SIĘ CHRONIĆ

Kluczowym elementem ataku jest zdobycie przyczółka w organizacji. Infrastruktura oraz umiejętność zarządzania bezpieczeństwem komponentów eksponowanych do internetu stały się priorytetowe dla bezpieczeństwa. Praktycznymi metodami ochrony przed atakami jest aktualizacja podatnych komponentów infrastruktury (PulseSecure VPN – CVE-2019-11510, WebLogic – CVE-2019-2725, Microsoft Windows – CVE-2018-8453). Trzeba zauważyć, że w roku 2019 ujawniono znacznie więcej niż wcześniej krytycznych luk w komponentach i oprogramowaniu, będących bramami do sieci wewnętrznej (tj. Fortigate SSL VPN, Pulse Secure SSL VPN, Global Protect Palo Alto Networks czy Citrix ADC / Citrix Gateway). Każdy, kto nie załatał tych podatności, musi liczyć się z tym, że jest łatwym celem dla cyberprzestępców. Oczywiście nadal system pocztowy i spearphishing pozostaje wektorem ataku. Po uzyskaniu początkowego dostępu, przestępcy przechodzą do fazy podniesienia uprawnień, rozprzestrzeniania się poziomego w infrastrukturze, tworzenia kodów, wykradania danych i finalnie szyfrowania.

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

Poniżej lista działań „utwardzających", mających na celu ograniczenie ekspozycji na atak ransomware:

- Stała analiza i identyfikacja podatności we własnej infrastrukturze. Eliminacja wszystkich znanych podatności. Szczególną uwagę należy zwrócić na podatności w komponentach dostępnych z internetu.
- Analiza konfiguracji serwisów i aplikacji (eliminacja domyślnych ustawień, domyślnych haseł, zbędnych usług). Ograniczenie do niezbędnego minimum używania kont serwisowych.
- Silna segmentacja sieci, z dokładnie ustalonymi regułami komunikacji pomiędzy strefami.
- Ograniczenie dostępu z zewnątrz do usług typu RDP (Remote Desktop).
- Wykrywanie i blokowanie używania programów kradnących hasła (m.in. mimikatz) oraz podnoszących uprawnienia.
- Uniemożliwienie wykorzystania narzędzia PsExec oraz innych narzędzi administracyjnych, których nie kontrolujemy jako firma. W tym kontekście, należy przeanalizować narzędzia typu LOLBins (Living off the Land Binaries) [5] i wdrożyć mechanizmy wykrywania niewłaściwego ich użycia. Tu szczególnie należy zwrócić uwagę na Powershell (najlepiej ograniczyć używania go tylko do podpisanych skryptów).
- Wykrywanie zmian w rejestrach systemów oraz harmonogramie zadań (w szczególności dodawania wpisów mających na celu uruchomianie programów po restarcie systemu, zmianę ustawień sieci, zmianę certyfikatów, czy konfiguracji programów antywirusowych).
- Hardening polityki domeny windowsowej (GPO).
- Ograniczenie możliwość komunikacji z infrastrukturą przestępców (serwery C2) poprzez wdrożenie reputacyjnych usług DNS oraz proxy dostępu do internetu, mogących wykrywać tunelowanie ruchu, czy komunikację zwrotną do C2 (C2 callbacks, beaconning).

Jednak nie wystarczy patrzeć na „tu i teraz", na „dzisiaj". Trzeba zbudować politykę bezpieczeństwa infrastruktury, uwzględniającą proces pozyskiwania informacji o słabościach, usuwania tych słabości, wykonywania regularnych testów bezpieczeństwa. Historia malware typu ransomware pokazuje, jak przestępcy adaptują się do zmieniających się okoliczności i szybko potrafią zaatakować w coraz to nowy i bardziej dotkliwy sposób.

Źródła:

1. *https://us-cert.cisa.gov/ncas/alerts/aa20-133a*
2. *https://go.recordedfuture.com/hubfs/reports/cta-2020-0204.pdf*
3. *https://risksense.com/wp-content/uploads/2019/09/RiskSense-Spotlight-Report-Ransomware.pdf*
4. *https://twitter.com/darktracer_int*
5. *https://www.sentinelone.com/blog/how-do-attackers-use-lolbins-in-fileless-attacks/*
6. *https://www.cbronline.com/news/ransomware-top-5-vulnerabilities*
7. *https://www.cert.pl/news/single/wannacry-ransomware/*
8. *https://gist.github.com/rain-1/989428fa5504f378b993ee6efbc0b168*
9. *https://zvelo.com/raas-ransomware-as-a-service/*
10. *https://www.bleepingcomputer.com/news/security/gandcrab-ransomware-shutting-down-after-claiming-to-earn-2-billion*

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

Sfera cywilna i wojskowa wspólnie w ćwiczeniach

Florian Naumczyk, Robert Rey
Rządowe Centrum Bezpieczeństwa

Aktualne – konwencjonalne i niekonwencjonalne, wieloaspektowe – wyzwania dla bezpieczeństwa obszaru euroatlantyckiego, którego integralną częścią jest Polska, wymagają adekwatnej odpowiedzi. Jednym ze sprawdzianów reakcji na zagrożenia są ćwiczenia, które w porównaniu do okresu bezpośrednio post-zimnowojennego, charakteryzują się nowym podejściem. Polega ono m.in. na ścisłym współdziałaniu sfery cywilnej i wojskowej – tak, by jak najlepiej przygotować państwa członkowskie i cały obszar Sojuszu Północnoatlantyckiego na ewentualność niebezpiecznego rozwoju sytuacji.

Ćwiczenia – zarówno krajowe jak i międzynarodowe, zwłaszcza sojusznicze – są jednym z najbardziej skutecznych narzędzi służących sprawdzeniu mechanizmów reagowania, regulacji prawnych, na podstawie których mechanizmy te są uruchamiane oraz procedur odpowiedzi na szybko narastającą sytuację kryzysową w obliczu zagrożenia, również tego o dużej skali – do wojennego włącznie. Ćwiczenia winny „wymuszać" interoperacyjność w działaniu wielu podmiotów ze sfery cywilnej i wojskowej.

Do niedawna układ pozamilitarny był w ćwiczeniach wojskowych często tylko „podgrywany", i to przeważnie przez samych wojskowych. Było to sztuczne, nieodpowiadające realiom, w których miałaby być przeprowadzona rzeczywista operacja militarna, opierająca się m.in. o zasoby cywilne. Dokonujący się ostatnio (m.in. dzięki staraniom Rządowego Centrum Bezpieczeństwa) rosnący udział podmiotów cywilnych w ćwiczeniach wojskowych niweluje tę sztuczność. Pozwala na szersze, a przede wszystkim rzeczywiste, sprawdzenie m.in. takich istotnych elementów jak: współpraca cywilno-wojskowa na wypadek realnego zagrożenia, rozwiązania prawne obowiązujące w danym kraju i ich adekwatność względem aktualnej sytuacji powstałej na przykład w następstwie zagrożeń hybrydowych, a także wymiana i obieg informacji.

Znaczenie wspólnych ćwiczeń cywilno-wojskowych jest wyjątkowo duże, jeżeli mają one za przedmiot operację sojuszniczą, wynikającą z zasady obrony kolektywnej ujętej w Traktacie Waszyngtońskim. Ćwiczenia wojskowe, ale też cywilne, przeprowadzane w ramach NATO obejmują swoim zasięgiem albo cały obszar sojuszniczy albo jakiś jego fragment, np. flankę północno-wschodnią. Angażują gremia polityczne oraz odpowiednie dowództwa różnych szczebli, jak np. Naczelne Dowództwo Sojuszniczych Sił Europy (SHAPE), Sojusznicze Dowództwo Sił Połączonych NATO w Brunssum (JFCBS) czy Sojusznicze Dowództwo Wojsk Lądowych w Izmirze (LANDCOM) oraz władze i struktury dowódcze w państwach członkowskich, a niekiedy też partnerskich. Pozwala to na poznanie – zarówno na płaszczyźnie krajowej jak i międzynarodowej – różnorakich punktów widzenia na dane zagadnienie czy problem. Ułatwia zrozumienie motywacji, którą kierują się dane państwa, dowództwa, a nawet ćwiczący z innej instytucji przy podejmowaniu decyzji w określonej sytuacji ćwiczebnej, będącej odzwierciedleniem realnych i potencjalnych zagrożeń (warto bowiem podkreślić, że realizm teraźniejszej sytuacji geopolitycznej stał się nieodzownym elementem każdego większego ćwiczenia). Wzajemne zrozumienie pomiędzy ćwiczącymi podmiotami – czy to krajowymi czy międzynarodowymi – jest jednym z kluczowych elementów budowania interoperacyjności, niezbędnej dla pomyślnego, solidarnego współdziałania.

Z powyższych względów kwestia ćwiczeń, mających się rozgrywać w realnym otoczeniu i obejmować wszelkie powiązane z nim aspekty cywilne i wojskowe, jak np. zaopatrzenie sił zbrojnych w energię czy zapewnienie im bezpiecznego przerzutu i tranzytu, stała się jedną z kluczowych w bieżącym funkcjonowaniu Sojuszu Północnoatlantyckiego. Wielką wagę przykłada się do odpowiedniego wszechstronnego przygotowania samych ćwiczeń jak też opracowania wniosków z nich płynących i rekomendacji na przyszłość.

W szczególności dotyczy to ćwiczeń zarządzania kryzysowego NATO z serii CMX. Zatwierdzany przez Radę Północnoatlantycką raport z każdego z ćwiczeń tej serii przyczynia się do doskonalenia zarządzania kryzysowego w NATO i w państwach członkowskich oraz adaptacji Sojuszu do dynamicznie zmieniających się zewnętrznych uwarunkowań jego funkcjonowania,

wyznaczanych we współczesnej dobie przede wszystkim zagrożeniami hybrydowymi. Po każdym ćwiczeniu NATO z serii CMX, w Polsce sporządzany jest Raport Krajowy, przyjmowany przez Radę Ministrów (która sprawuje zarządzania kryzysowe na terytorium RP). Rekomendacje zawarte w takim raporcie to z kolei element działań służących doskonaleniu polskiego systemu zarządzania kryzysowego i niektórych narodowych rozwiązań prawnych, w tym odnoszących się do współpracy cywilno-wojskowej.

Udział sfery cywilnej w ćwiczeniach pozwala – szerzej niż na podstawie regulacji wynikających z zadań państwa-gospodarza (HNS) – na poznanie potrzeb wojska w potencjalnej sytuacji kryzysowej bądź ewidentnego zagrożenia. Zarazem stwarza możliwość cywilnym instytucjom biorącym udział w ćwiczeniu przekazywania, jakich informacji potrzebują, aby móc zapewnić wsparcie siłom zbrojnym, ale też, aby uzyskać wsparcie od wojska w celu ochrony ludności lub infrastruktury krytycznej i zapewnienia ciągłości kluczowych usług. Te właśnie aspekty są dla układu pozamilitarnego bardzo ważne, o czym mógł się przekonać każdy uczestnik kolejnych seminariów, dotyczących wsparcia dla polskich i sojuszniczych sił zbrojnych, które były organizowane przez Rządowe Centrum Bezpieczeństwa. Komunikacja wzajemna dotycząca potrzeb i oczekiwań jest kluczowa w procesie decyzyjnym.

Ćwiczenia cywilno-wojskowe, zwłaszcza te, których przedmiotem jest zarządzanie kryzysowe (a tu przypomnijmy, iż „zarządzania kryzysowe" rozumiane jest różnie w Polsce i w NATO[1]), pozwalają na zidentyfikowanie luk czy niedostatków nie tylko w procedurach i mechanizmach reagowania na zagrożenia, lecz także w zdolnościach każdej z tych sfer. Dla całego układu pozamilitarnego i jego poszczególnych struktur takim miernikiem jest stan odporności na zagrożenia. Może on być oceniany według kryteriów odporności wyspecyfikowanych przez NATO[2]. Niektóre z nich zostały sformułowane z myślą przede wszystkim o wsparciu sił zbrojnych. Mają więc bezpośrednie odniesienie do współdziałania cywilno-wojskowego i dlatego podlegają ćwiczeniom. Tak więc ćwiczenia są także metodą umożliwiającą ocenę stopnia odporności i z tego punktu widzenia mają duże znaczenie dla różnych podmiotów cywilnych. Prace nad odpornością postępują po stronie NATO równolegle z rozwojem koncepcji zwiększenia udziału sfery cywilnej w ćwiczeniach wojskowych.

Tu wyłania się pytanie o rolę w tych ćwiczeniach podmiotów cywilnych, w tym RCB. W przypadku wspomnianego ćwiczenia CMX, w którym uczestniczy tez MON i Siły Zbrojne, RCB jest głównym polskim koordynatorem odpowiedzialnym za przygotowanie, przeprowadzanie ćwiczenia oraz za wypracowanie wniosków. Z kolei w ćwiczeniach wojskowych wypracowano mechanizm, w którym RCB odpowiada za koordynację kontaktów na linii wojsko – sfera cywilna, będąc swoistym hubem i współpracując z poszczególnymi instytucjami i urzędami, przede wszystkimi tymi zaangażowanymi w działania w ramach wykazu przedsięwzięć i procedur systemu zarządzania kryzysowego[3]. Podmioty te delegują ekspertów, którzy są w stanie udzielić potrzebnych informacji w trakcie planowania i przeprowadzania ćwiczenia. To właśnie ich udział w ćwiczeniach wojskowych sprawia, że ćwiczenie jest rozgrywane realistycznie, a nie „podgrywane". Udział ekspertów z różnych dziedzin pozwala ponadto na identyfikowanie współzależności pomiędzy różnymi dziedzinami składającymi się na system bezpieczeństwa.

Tak więc poznanie, poprzez wspólne ćwiczenia, uwarunkowań funkcjonowania struktur militarnych i cywilnych w konkretnych sytuacjach prowadzi do lepszej współpracy pomiędzy nimi w codziennej pracy czy to na forum krajowym czy międzynarodowym. W tym miejscu należy jednak zwrócić uwagę na ograniczoną aktywność Unii Europejskiej, mimo tego, że są podejmowane działania mające na celu szersze włączenie UE do ćwiczeń NATO. Należy zarazem docenić, iż także w UE ćwiczenia o charakterze cywilno-wojskowym nabierają znaczenia. Przykładem mogą być trwające właśnie ćwiczenia „Integrated Resolve", jak również podejmowane wspólnie z NATO wysiłki zmierzające do przeprowadzenia wspólnego ćwiczenia zarządzania kryzysowego. Świadczą o tym ćwiczenia z serii PACE.

[1] Zarządzanie kryzysowe w NATO: https://rcb.gov.pl/wspolpraca-w-ramach-nato/#_ftn1

[2] 1) zapewnienie ciągłości administracji i świadczenia kluczowych usług; 2) zapewnienie dostaw energii; 3) zdolność do radzenia sobie z ofiarami na skalę masową; 4) zdolność do skutecznego radzenia sobie z niekontrolowanym przepływem osób; 5) oporność zasobów żywności i wody; 6) odporność systemów łączności; 7) odporność systemu transportu cywilnego.

[3] https://rcb.gov.pl/wp-content/uploads/Zarz.-nr-5-PRM-2019-wykaz-procedur-zarz%C4%85dzanie-kryzysowe.pdf

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

Ale ciągle w zbyt małym stopniu uwzględnia się w ćwiczeniach rolę sektora prywatnego. Tymczasem doświadczenia z walki z pandemią COVID-19 pokazują, jak ważna jest jego rola zapewnianiu ciągłości działania kluczowych usług i w jak bezpośredni sposób dotyka to kwestii bezpieczeństwa całego społeczeństwa, w tym także funkcjonowania sfery militarnej. Stąd oczywista staje się potrzeba szerszego uwzględniania tych aspektów w planowaniu i prowadzeniu ćwiczeń. Zostało to wyartykułowane podczas wspomnianych seminariów dotyczących wsparcia dla polskich i sojuszniczych sił zbrojnych, organizowanych przez RCB. Zaangażowanie podmiotów prywatnych, które wykonują zadania ważne z punktów widzenia bezpieczeństwa i obronności państwa powinno być traktowane jako niezbędny element przyszłych ćwiczeń, głównie krajowych. Udział sfery cywilnej w krajowych ćwiczeniach wojskowych organizowanych w Polsce ma bowiem już miejsce (np. ostatnie ćwiczenia DRAGON-19, JESION-19, czy planowane, DRAGON-21).

Nie ma lepszego sprawdzianu przygotowania państw i całego NATO na zagrożenia bezpieczeństwa niż ćwiczenia. Wobec zagrożeń współczesnych, a więc hybrydowych, czy podprogowych klasyczny podział na domenę militarną i cywilną stał się właściwie nieaktualny. Powinna go zastąpić interakcja cywilno-wojskowa. Kluczowym wyzwaniem staje się konieczność holistycznego (całościowego) podejścia do bezpieczeństwa, w tym do poprawy odporności zarówno w wymiarze cywilnym (politycznym, gospodarczym, informacyjnym itp.), jak i ściśle militarnym. Adekwatna odpowiedź na zagrożenia nie jest też możliwa bez szerokiej, wielowymiarowej współpracy międzynarodowej. Dotyczy to w szczególności współpracy w wymiarze sojuszniczym i unijnym. Doświadczenia wynikające z walki z pandemią COVID-19 w pełni potwierdzają te tezy. Implikują ponadto potrzebę szerszego uwzględniania roli sektora prywatnego i jego współdziałania ze sferą cywilną i militarną w rozwiązywaniu sytuacji kryzysowych, w tym w zapewnianiu ciągłości dostaw i funkcjonowania kluczowych usług. Poszukiwania skutecznych środków opanowania pandemii wskazują na potrzebę współpracy sektora cywilnego, prywatnego i militarnego oraz budowania odporności, w tym – co jest nowym elementem – odporności społecznej – w skoordynowany sposób. Cykliczne ćwiczenia, angażujące komponenty wszystkich wskazanych sfer, wydają się być najbardziej adekwatnym sposobem wypracowania pożądanych mechanizmów współpracy.

Susza rolnicza w 2020 roku oraz wdrożenie nowego systemu zbierania danych o stratach w rolnictwie

Andrzej Doroszewski
Instytut Uprawy Nawożenia i Gleboznawstwa – Państwowy Instytut Badawczy

Beata Gawlik-Pliszka
Ministerstwo Rolnictwa i Rozwoju Wsi

Częstotliwość i nasilenie wystąpienia suszy w Polsce jest w ostatnich latach coraz bardziej istotnym problemem, zarówno dla gospodarki kraju jak i dla środowiska. Większa częstotliwość wystąpienia suszy jest wynikiem obserwowanych zmian klimatycznych, zwłaszcza wzrostem temperatury powietrza w okresie wegetacyjnym.

Wyróżniane są cztery rodzaje suszy: najpierw występuje susza atmosferyczna, później rolnicza, następnie hydrologiczna, a na końcu geologiczna. W zależności od wielkości deficytu wody oraz trwania występowania suszy, generowane są odpowiedniej wielkości straty w gospodarce oraz w środowisku.

Instytut Uprawy Nawożenia i Gleboznawstwa – Państwowy Instytut Badawczy (IUNG-PIB) w Puławach stworzył System Monitoringu Suszy Rolniczej (SMSR) dla obszaru Polski. System ten przy wyznaczaniu obszarów z suszą dla poszczególnych upraw uwzględnia czynniki pogodowe i podatność gleb na niedobory wody. Baza danych pogodowych potrzebna jest do obliczenia klimatycznego bilansu wodnego (KBW), za pomocą którego wyznacza się obszary objęte suszą rolniczą.

Głównymi elementami meteorologicznymi decydującymi o wielkości suszy rolniczej są: opad atmosferyczny, temperatura i wilgotność powietrza, usłonecznienie, prędkość wiatru. W 2020 r. IUNG-PIB włączył do SMSR dane publikowane przez Instytut Meteorologii i Gospodarki Wodnej – Państwowy Instytut Badawczy (IMGW-PIB), pochodzące z naziemnych radarów mierzących wielkość opadów atmosferycznych. Dane uzyskane z radarowej sieci POLRAD pozwalają na znaczne uszczegółowienie pola opadów dla całego kraju. Zwiększenie dokładności określenia wielkości opadu na terenie Polski spowodowało, że nastąpiła zdecydowana poprawa wyznaczenia granic obszarów objętych suszą rolniczą. W systemie uwzględniana jest również informacja o glebach, a zwłaszcza dane o retencji wodnej, która wyjaśnia duże lokalne zróżnicowanie strat w plonach w następstwie niedoboru opadów. Informacja o glebach wykorzystywana jest za pomocą cyfrowej mapy glebowo-rolniczej, zwiększając dokładność oceny zasobów wody dostępnej dla roślin. W systemie uwzględniane są również wymagania dotyczące zasobów wodnych dla poszczególnych grup i gatunków roślin w zależności od ich fazy rozwojowej w sezonie wegetacyjnym.

System wykorzystuje nowoczesne aplikacje GIS (Geographic Information System) do przetwarzania i interpolacji danych przestrzennych. Aplikacje komputerowe integrują dane meteorologiczne oraz dane z cyfrowej mapy glebowo-rolniczej obrazującej przestrzenne zróżnicowanie retencji wodnej różnych kategorii agronomicznych gleb. W SMSR zastosowano procedury pozwalające na szczegółową prezentację wyników za pomocą systemu internetowego. Informacje dotyczące suszy przedstawiane są w formie tabel i map dla każdej gminy Polski, dla 14 grup i gatunków roślin oraz dla 4 kategorii gleb. W SMSR susza oznaczana jest jako deficyt wody powodujący straty w plonach wynoszące przynajmniej 20% w skali gminy w stosunku do plonów uzyskanych w średnich wieloletnich warunkach pogodowych.

Przejawem trendu występowania dużych niedoborów wody była ekstremalna susza w 2006 r., w wyniku której średnie krajowe plony niektórych upraw były niższe nawet o 30% w stosunku do plonów uzyskanych w średnich wieloletnich warunkach pogodowych. Do lat zaliczanych jako bardzo suche, powodujące bardzo duże straty w rolnictwie należą: 2008, 2015, 2018 oraz 2019 rok. Szczególnie niesprzyjające warunki dotyczące zasobów wodnych dla roślin uprawnych wystąpiły w latach 2015, 2018 oraz 2019, w których deficyt wody odnotowano we wszystkich 14 monitorowanych uprawach. We wszystkich województwach kraju susza wystąpiła w 2015 i 2019 r. w siedmiu uprawach, a w 2018 roku w pięciu uprawach.

WARUNKI TERMICZNE

Kwiecień w tym roku był ciepły, temperatura wahała się od 6 do ponad 10˚C. Najcieplej było w południowo-zachodniej części kraju (od 9 do ponad 10˚C, cieplej od normy od 1 do ponad 1,5˚C). Im dalej w kierunku północno-wschodnim, tym było zimniej od 6 do 8˚C. Na bardzo dużej powierzchni kraju temperatura powietrza tego miesiąca była wyższa od normy wieloletniej od 0,5 do 1˚C. Należy natomiast zwrócić uwagę na bardzo duże usłonecznienie tego miesiąca, wynoszące w południowych rejonach kraju ponad 300 godz. tj. większe od normy o 100%, a w północno-wschodnich obszarach notowano ponad 270 godz. ze Słońcem tj. więcej od normy o 70%. Takie warunki termiczno-solarne sprawiły, że w kwietniu wystąpiła wyjątkowo wysoka ewapotranspiracja, czyli całokształt procesów związanych z odpływem do atmosfery wody parującej z powierzchni gleby (ewaporacja) pokrytej roślinnością (transpiracja).

Maj natomiast był w tym roku zimny, szczególnie na północy kraju, gdzie temperatura kształtowała się w przedziale od 9 do 11˚C. Na Ziemi Lubuskiej, gdzie było najcieplej, utrzymywała się na poziomie ok. 12˚C, a na przeważającym obszarze Polski notowano temperaturę od 11 do 12˚C. Na dużej powierzchni kraju notowano temperaturę niższą od średniej wieloletniej o ok. 1 do 2,5˚C, a na Wyżynach Polskich, Mazowszu, Warmii i Mazurach nawet niższą o ponad 2,5˚C. Temperatura powietrza tegorocznego maja w wielu rejonach kraju była najniższa w ciągu ostatnich 30 lat.

W czerwcu warunki termiczne poprawiły się. Najcieplej było w szerokim pasie Polski środkowej oraz we wschodnich rejonach kraju od 18 do ponad 19˚C. We wschodnich terenach Polski notowano temperaturę wyższą od wieloletniej od 2 do ponad 2,5˚C, a na pozostałych obszarach wyższą od normy od 1 do 2˚C. W południowych, a zwłaszcza w północnych rejonach kraju było chłodniej – od 14 do 16˚C i na tych terenach notowano temperaturę w normie wieloletniej.

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

W lipcu temperatura znowu spadła, chłodno było zwłaszcza w północno-zachodniej oraz miejscami w południowej części kraju, gdzie temperatura była niższa od normy wieloletniej o ok. 0,5˚C. Na pozostałym obszarze Polski temperatura powietrza utrzymywała się w normie. Najcieplej było w południowych i południowo-zachodnich rejonach Polski, ponad 19˚C. Na przeważającym terytorium kraju notowano od 17 do 19˚C, jedynie na północy było nieco chłodniej od 15 do 16˚C.

Natomiast tegoroczny sierpień i wrzesień były ciepłe. W sierpniu, w zachodnich rejonach Polski oraz w Kotlinie Sandomierskiej notowano temperaturę od 20 do ponad 21˚C i na tych obszarach było cieplej od normy wieloletniej o ponad 2˚C. Na pozostałym terytorium kraju również było ciepło – od 18 do 20˚C, cieplej od normy o 1-2˚C. We wrześniu notowano temperaturę powietrza wyższą od normy wieloletniej o 1 do 2˚C. Najcieplej było na Ziemi Lubuskiej ponad 16˚C. Na pozostałym obszarze Polski notowano od 14 do16˚C.

WARUNKI OPADOWE

Opady w kwietniu były bardzo małe. Szczególnie niskie, poniżej 10 mm wystąpiły w północnej części kraju, stanowiły one na tych terenach od 10 do 20% poniżej normy wieloletniej. Im dalej w kierunku południowym tym opady były nieco większe, wynoszące od 10 do ponad 30 mm i na tych obszarach stanowiły od 20 do ponad 40% normy.

W maju opady atmosferyczne były bardzo zróżnicowane. Najwyższe stwierdzono we wschodnich i południowych terenach kraju – od 60 do 150 mm i stanowiły od100 do 160% normy wieloletniej. Natomiast najniższe – od 30 do 60 mm występowały w północno-zachodniej części Polski i stanowiły od 50 do 100% normy.

W czerwcu opady były wysokie lub bardzo wysokie na dużej powierzchni Polski, wynoszące od 60 do nawet ponad 240 mm, stanowiły od 100 do ponad 300% normy wieloletniej. Jedynie w północno-zachodniej obszarach notowano mniejsze opady od 30 do 60 mm (tj. 50-100% normy).

Opady lipca charakteryzowały się dużym zróżnicowaniem. Szczególnie małe opady poniżej 30 mm notowano w południowo-zachodniej i północno-wschodniej części kraju, stanowiące poniżej 40% normy. Natomiast najwyższe opady wynoszące ponad 150 mm notowano w południowej części kraju oraz nieco mniejsze od 60 do 90 mm w północnej Polsce, stanowiły 90-110% normy. Na przeważającym terytorium kraju notowano opady od 30 do 60 mm (40-90% normy).

W sierpniu na bardzo dużym obszarze Polski notowano opady od 60 do 120 mm (od 100 do 160% normy wieloletniej), jedynie w północnych rejonach oraz na Wyżynie Lubelskiej, Małopolskiej oraz w Kotlinie Sandomierskiej opady były nieco niższe od 40 do 60 mm (60-100% normy).

Tegoroczny wrzesień w Polsce pod względem opadów atmosferycznych był bardzo zróżnicowany. Od bardzo małych, poniżej 20 mm na północno-wschodnich obszarach kraju, gdzie stanowiły zaledwie 20% normy. Im bardziej przemieszczając się w kierunku południowo-zachodnim były one już większe, osiągając na linii Terespol-Siedlce-Mława-Kwidzyń -Słupsk-Ustka 60 mm (100% normy). Na pozostałym terytorium kraju notowano już większe opady od 60 do100 mm (100-140% normy), a na Wyżynie Lubelskiej oraz w południowych rejonach Polski były już wysokie – od 100 do 140 mm tj. 140-200% normy.

Występujące tegoroczne niedobory wody spowodowały, że susza rolnicza notowana była wśród wszystkich czternastu grup i gatunków roślin monitorowanych przez SMSR.

Oznacza to, że tegoroczne plony tych upraw będą niższe z powodu występującego deficytu wody w stosunku do plonów uzyskanych w średnich wieloletnich warunkach pogodowych.

W poniższej tabeli zamieszczono wyniki dotyczące suszy rolniczej w Polsce w 2020 roku. Natomiast bardziej szczegółowe informacje dotyczące suszy prezentowane są na stronie internetowej www.susza.iung.pulawy.pl.

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

Lp.	Uprawa	Liczba gmin z suszą	Udział gmin z suszą [%]	Udział powierzchni gruntów ornych z suszą [%]
1.	kukurydza na kiszonkę	1024	41.34	8.57
2.	kukurydza na ziarno	945	38.15	7.70
3.	zboża jare	922	37.22	12.24
4.	krzewy owocowe	785	31,69	8,73
5.	rzepak i rzepik (jesień)	770	31.09	4.55
6.	zboża ozime	761	30,72	8,93
7.	truskawki	609	24,59	7,60
8.	rośliny strączkowe	580	23.42	4.56
9.	ziemniak	654	26.40	3.67
10.	warzywa gruntowe	268	10,82	1,30
11.	rzepak i rzepik	247	9,97	2,52
12.	tytoń	196	7,91	1,03
13.	chmiel	192	7,75	0,74
14.	burak cukrowy	112	4.52	0.51
15.	drzewa owocowe	19	0,77	0,05

NOWY SYSTEM ZBIERANIA DANYCH Z WOJEWÓDZTW O STRATACH W ROLNICTWIE

Od 2020 roku wnioski o oszacowanie strat spowodowanych przez suszę producenci rolni mogą składać wyłącznie za pomocą publicznej aplikacji. Za pomocą tej aplikacji producent rolny, korzystając z własnego Profilu Zaufanego, określa zakres i stopień strat spowodowanych przez suszę w uprawach rolnych w jego gospodarstwie rolnym.

Wprowadzane przez producenta rolnego dane są automatycznie weryfikowane przez aplikację z danymi:

- Agencji Restrukturyzacji i Modernizacji Rolnictwa w zakresie upraw rolnych zgłoszonych do wniosku o dopłaty bezpośrednie oraz danymi dotyczącymi liczby zwierząt zawartymi w Systemie Identyfikacji i Rejestracji Zwierząt;
- Instytutu Uprawy, Nawożenia i Gleboznawstwa w Puławach w zakresie zasięgu i zakresu suszy wynikającego z Systemu Monitoringu Suszy Rolniczej.

W aplikacji wygenerowany jest automatycznie protokół oszacowania szkód powstałych w wyniku suszy, jeżeli szkody wynoszą powyżej 30% średniej rocznej produkcji rolnej w gospodarstwie rolnym z ostatnich trzech lat poprzedzających rok, w którym wystąpiła susza. Średnia roczna produkcja rolna jest ustalana na podstawie danych Instytutu Ekonomiki Rolnictwa i Gospodarki Żywnościowej w Warszawie, pochodzących z Systemu Zbierania Danych Rachunkowych (FADN).

Producent rolny ma prawo do kilkukrotnego uzupełniania strat w poszczególnych uprawach w miarę ich obejmowania suszą wskazywaną przez System Monitoringu Suszy Rolniczej – do momentu potwierdzenia ostatniego zgłoszenia poprzez podpisanie wniosku Profilem Zaufanym. Podpisanie wniosku uruchamia proces generowania protokołu strat w gospodarstwie rolnym przekazywanym do zatwierdzenia przez wojewodę i uniemożliwia dokonywanie dalszych zgłoszeń.

Każdy producent rolny może otrzymać w danym roku jeden protokół oszacowania szkód w gospodarstwie rolnym spowodowanych przez suszę.

Mając na względzie, iż 2020 rok jest pierwszym rokiem funkcjonowania aplikacji, termin składania wniosków o oszacowanie szkód spowodowanych wystąpieniem suszy został wydłużony do 30 listopada br.

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