RCB
Rządowe Centrum Bezpieczeństwa

BIURO
ANALIZ I REAGOWANIA

BIULETYN

KWARTALNY

NUMER 33 KWIECIEŃ – CZERWIEC 2021

Zespół redakcyjny

Biuletynu kwartalnego Rządowego Centrum Bezpieczeństwa:

Grzegorz Świszcz

Martyna Olejnik-Kołodziej

Anna Zasadzińska-Baraniewska

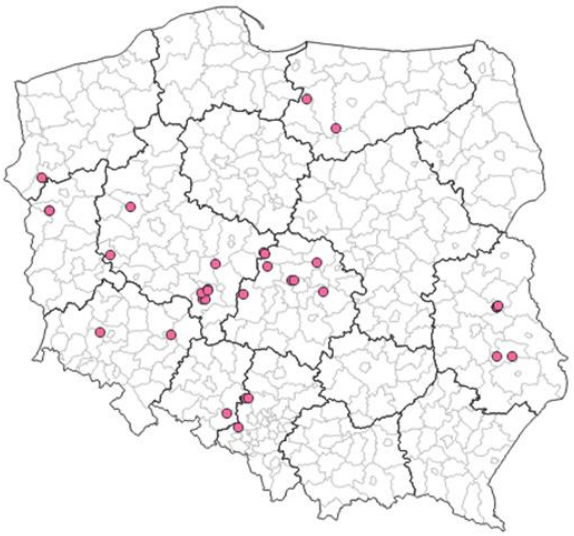
Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l

Wysoce zjadliwa grypa ptaków (HPAI)

Paweł Meyer
Główny Inspektorat Weterynarii

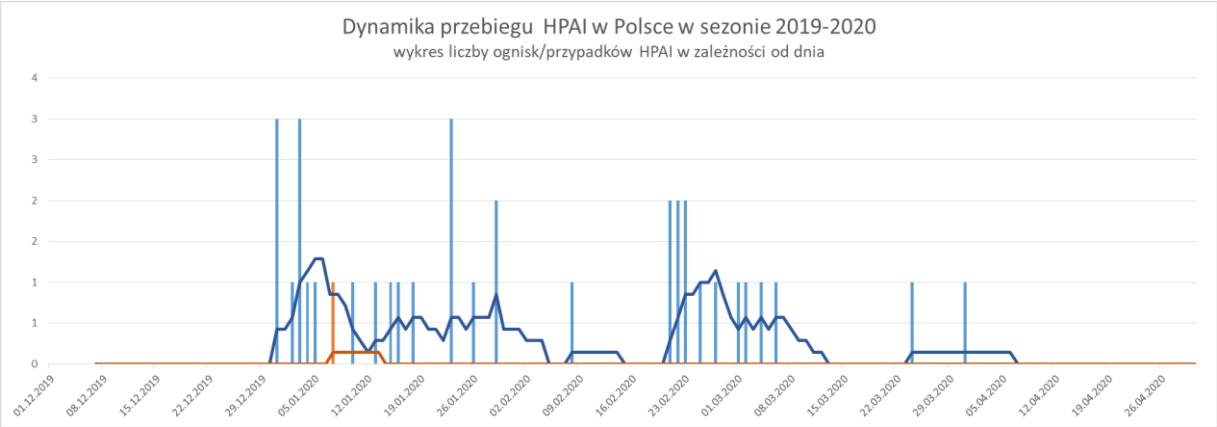
Wysoce zjadliwa grypa ptaków (HPAI) jest niezwykle zakaźną i zaraźliwą chorobą drobiu, objętą obowiązkiem zwalczania. Jest chorobą wirusową o bardzo dużym znaczeniu ekonomicznym, wywierającą przy tym bardzo duży wpływ na gospodarkę narodową kraju. Wirusy grypy charakteryzują się dużym stopniem zmienności genetycznej. Podkreślenia wymaga fakt, że nie ma skutecznego sposobu jej leczenia u drobiu, a skuteczność szczepionek jest bardzo ograniczona. Stąd też aktualnie jedyną, efektywną bronią w walce z grypą ptaków jest szybkie wprowadzenie metody administracyjnej zwalczania choroby. Polega ona przede wszystkim na natychmiastowym wdrażaniu działań w przypadku podejrzenia wystąpienia choroby, szybkiej diagnostyce laboratoryjnej, likwidacji ptaków w ognisku choroby i gospodarstwach kontaktowych oraz wprowadzeniu tymczasowych restrykcji na obszarze występowania grypy wraz z wdrożeniem procedury uboju prewencyjnego w gospodarstwach znajdujących się w pobliżu ogniska tak, aby zapobiec jej dalszemu rozprzestrzenieniu. Zasadnicze znaczenie w tym przypadku ma szybkość działań oraz ustalenie wektorów choroby, w tym przede wszystkim przerwanie łańcucha epizootycznego. W związku z powyższym, na wszystkich szczeblach, inspekcja weterynaryjna monitoruje sytuację epizootyczną dotyczącą chorób zakaźnych zwierząt, w tym również, w zakresie grypy ptaków. Każdy przypadek stwierdzenia choroby analizowany jest indywidualnie przez terenowe organy inspekcji weterynaryjnej, w tym na szczeblu wojewódzkim, przez wojewódzkiego lekarza weterynarii i powołane przy tym organie zespoły ds. dochodzeń epizootycznych. Sytuacja w regionie dotkniętym chorobą w odniesieniu do całego kraju, nadzorowana jest i koordynowana ze szczebla centralnego, wraz z bieżącym modelowaniem prowadzonych działań w terenie. Działania takie częstokroć prowadzone są na posiedzeniach Wojewódzkich Zespołów Zarządzania Kryzysowego zwoływanych przez wojewodę, na których minister rolnictwa i rozwoju wsi lub Główny Lekarz Weterynarii rekomenduje działania spersonalizowane indywidualnie na konkretne zagrożenie i sytuację w danym regionie.

Analizując sytuację epizootyczną w zakresie grypy ptaków należy stwierdzić, że występuje ona sezonowo, przy czym największe zagrożenie odnotowujemy od końca października do kwietnia następnego roku kalendarzowego. Potwierdza to rok 2020, kiedy w I półroczu stwierdzono 1 przypadek choroby u dzikiego ptactwa oraz 32 ogniska HPAI u drobiu, a ostatni w przypadek odnotowano 31 marca.



Województwo	Liczba ognisk	Liczba ptaków
wielkopolskie	10	181 200
lubelskie	8	92 414
łódzkie	6	118 455
śląskie	3	53 756
dolnośląskie	2	623
lubuskie	2	123 144
warmińsko-mazurskie	2	7 246
opolskie	1	6 960
zachodniopomorskie	1	22 629
Suma	**35**	**626 427**

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



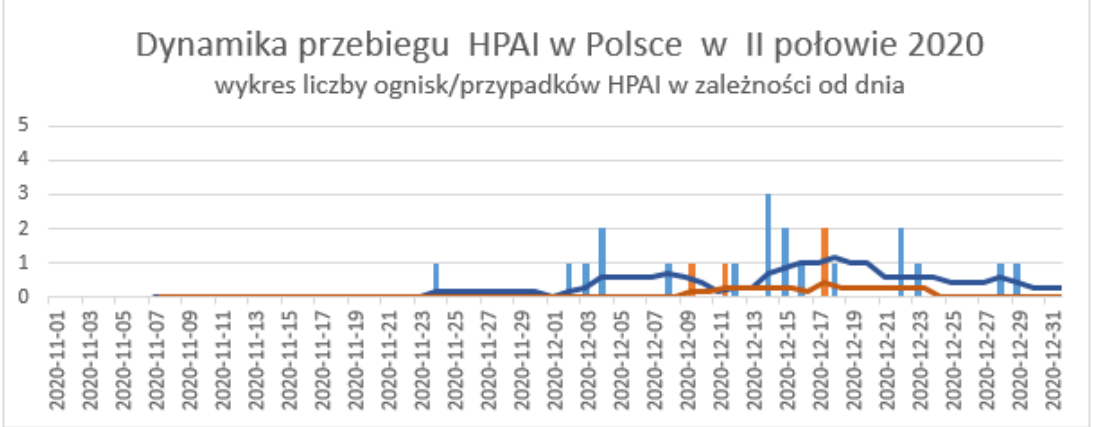
Kolejne fale grypy ptaków i nowe ogniska choroby wystąpiły już w II półroczu 2020 roku po ponad 7 miesięcznej przerwie od ostatniego ogniska. Do końca II półroczu 2020 roku wystąpiło 19 ognisk u drobiu i 4 przypadki u dzikich ptaków.

Województwo	Ognisk	Ptaków w ognisku
dolnośląskie	2	276
lubelskie	1	53 504
mazowieckie	3	151 582
pomorskie	1	269 697
warmińsko-mazurskie	2	40 253
wielkopolskie	9	2 012 845
zachodniopomorskie	1	662
RAZEM	**19**	**2 528 819**

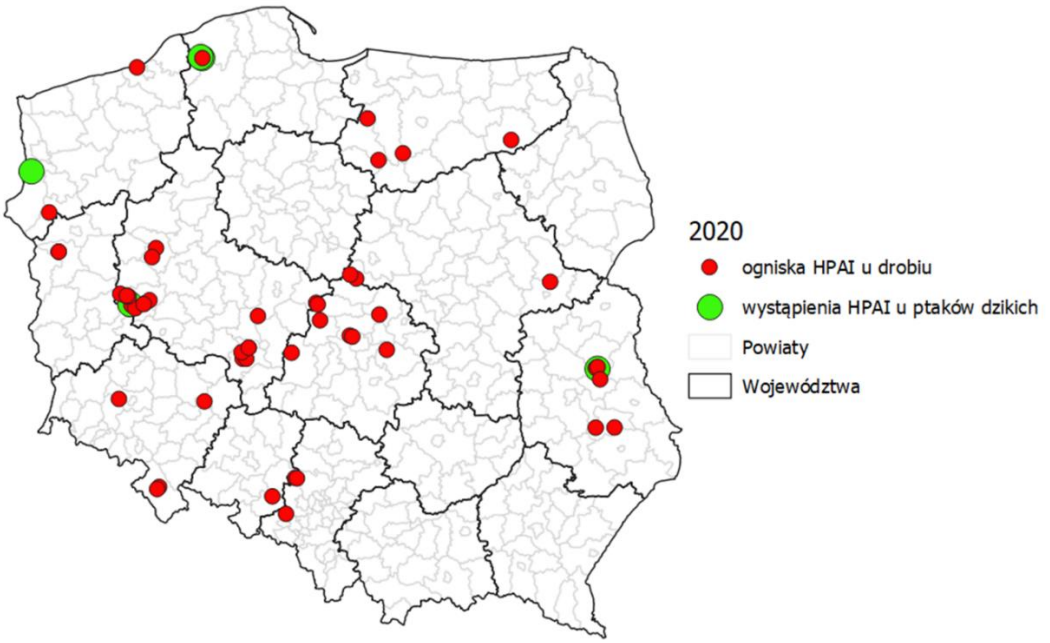
Reasumując, w 2020 roku na terytorium Polski stwierdzono 51 ognisk wysoce zjadliwej grypy ptaków (HPAI), w których utrzymywano 3 155 246 sztuk drobiu oraz 5 przypadków choroby u dzikiego ptactwa, przy czym ogniska choroby stwierdzono na terenie 9 województw (mapa poniżej) w dwóch etapach przedzielonych kilkumiesięczną przerwą pomiędzy wystąpieniem ognisk.

Podział na gatunki drobiu.

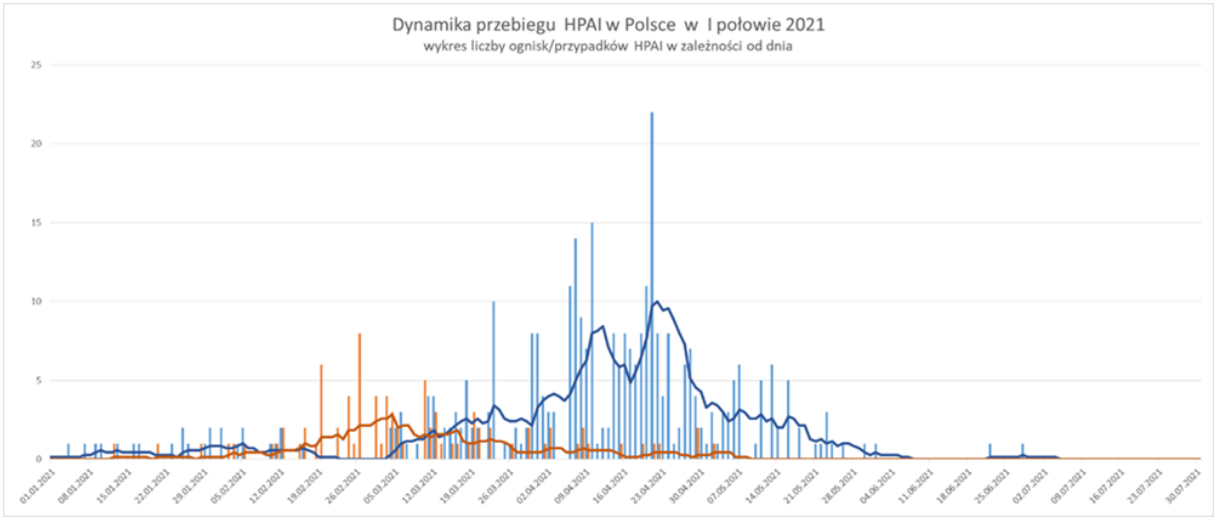
Gatunek/typ produkcyjny	Ognisk	Ptaków w ogniskach
Kura hodowlana	0	0
Brojler kurzy	0	0
Kura nioska	5	2 123 718
Kura ogólnoużytkowa	0	0
Kura przydomowa	4	348
Indyk hodowlany	0	0
Indyk rzeźny	9	350 689
Indyk przydomowy	0	0
Kaczka hodowlana	0	0
Kaczka rzeźna	1	53 458
Kaczka ogólnoużytkowa	0	0
Kaczka przydomowa	0	0
Gęś hodowlana	1	600
Gęś rzeźna	0	0
Gęś ogólnoużytkowa	0	0
Gęś przydomowa	1	6
Perlica	0	0
Gołąb	0	0
Bażant	0	0
Kuropatwa	0	0
Przepiórka	0	0
Paw	0	0
RAZEM	**21**	**2 528 819**



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



Sytuacja epizootyczna w bieżącym roku miała odmienny przebieg, a ponadto była bardzo zróżnicowana pod względem charakteru i dynamiki przebiegu choroby. Można stwierdzić, że do końca lutego tendencja przebiegu choroby była podobna do wcześniej występujących w kraju. Niepokojącym zaś sygnałem, który wskazywał na możliwość niestandardowego przebiegu choroby w bieżącym roku był fakt dużej liczby padłych dzikich ptaków, u których stwierdzano występowanie wirusa HPAI. Dodatkowo, zwłoki padłych ptaków były zazwyczaj w terenie, gdzie stwierdzano następnie ogniska choroby. Należy podkreślić, że czynnikiem sprzyjającym rozwojowi epizoocji, szczególnie w czasie dynamicznego rozwoju choroby o charakterze kryzysowym, była duża zjadliwość wirusa terenowego oraz łatwość jego przenikania ze środowiska do miejsc utrzymywania drobiu. Od marca następował stopniowy wzrost zachorowań, osiągając epicentrum epizoocji w kwietniu, zmniejszając intensywność występowania choroby w maju i czerwcu, doprowadzając do stwierdzenia ostatniego ogniska 28 czerwca br. (mapa liczby ognisk tygodniowo oraz dynamiczny wykres przebiegu choroby).



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

W związku z czym, w 2021 roku na terytorium Polski stwierdzono 338 ognisk HPAI, w których utrzymywano 11 479 909 sztuk drobiu na terenie 15 województw. Jedynym województwem, na terenie którego nie stwierdzono ognisk grypy ptaków u drobiu było województwo podlaskie (tabela poniżej).

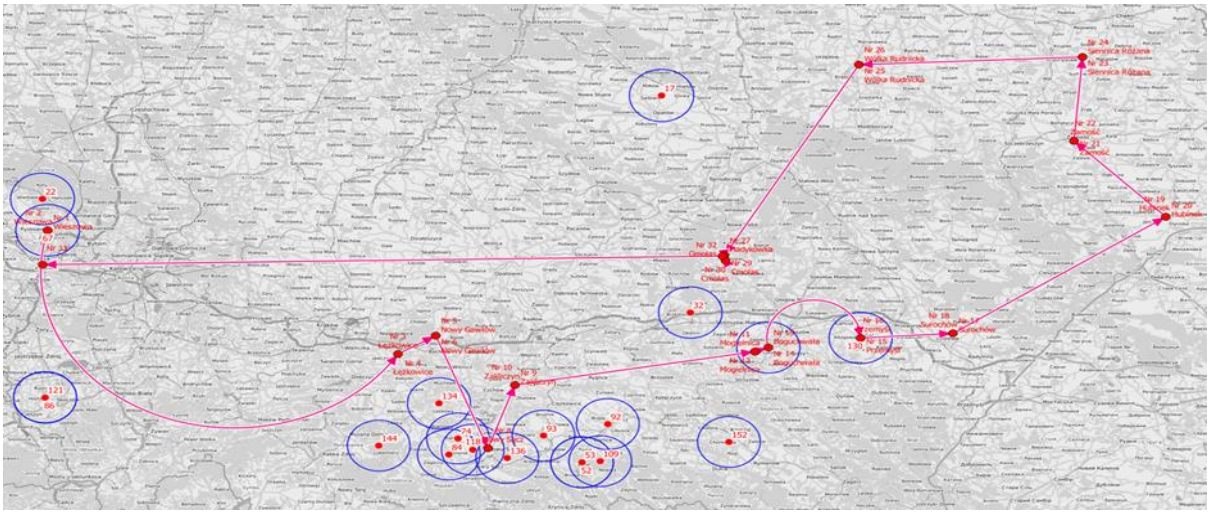
Województwo	Ognisk	Ptaków w ognisku
dolnośląskie	2	57 154
kujawsko-pomorskie	7	168 882
lubelskie	6	31 202
lubuskie	6	114 320
łódzkie	10	95 558
małopolskie	13	53 739
mazowieckie	128	7 628 479
opolskie	4	23 327
podkarpackie	4	65 203
podlaskie	0	0
pomorskie	21	156 882
śląskie	6	218 149
świętokrzyskie	2	97
warmińsko-mazurskie	36	583 398
wielkopolskie	91	2 264 056
zachodniopomorskie	2	19 463
RAZEM	**338**	**11 479 909**

Z uwagi na liczne przypadki zakażeń u ptaków dzikich w Europie, należy je uznać za najbardziej prawdopodobny wektor wprowadzenia wirusa. Dzikie ptactwo, szczególnie wodne (kaczki, gęsi, łabędzie), stanowi główny rezerwuar oraz wektor w transmisji choroby. Wirus może przeżyć w wodzie i innym wilgotnym środowisku przez wiele tygodni, szczególnie w niskiej temperaturze, dlatego zbiorniki wodne, w pobliżu których przebywają dzikie ptaki, mogą być w okresie jesienno-zimowym długotrwałym źródłem zakażenia dla drobiu. Do zakażenia dochodzi nie tylko w wyniku kontaktu bezpośredniego drobiu i dzikiego ptactwa, ale również drogą pośrednią, np. poprzez wprowadzenie do gospodarstwa zanieczyszczonej przez dzikie ptaki słomy czy paszy. Bardzo dużą rolę odgrywa w tym przypadku również czynnik ludzki – dla przykładu mapa, która obrazuje powiązania między ogniskami choroby oraz wpływ człowieka na rozprzestrzenianie się choroby. W takich przypadkach nieodzowne jest prowadzenie dalszego dochodzenia wraz z podejmowaniem działań w stosunku do gospodarstw powiązanych. Takie działania również wymagają zaangażowania innych służb państwa w prowadzeniu postępowań wyjaśniających.

Podział na gatunki zwierząt.

Gatunek/typ produkcyjny	Ognisk	Ptaków w ogniskach
Kura hodowlana	46	1 709 592
Brojler kurzy	17	2 898 663
Kura nioska	47	3 584 451
Kura ogólnoużytkowa	11	255 109
Kura przydomowa	65	4 649
Indyk hodowlany	0	0
Indyk rzeźny	68	1 674 765
Indyk przydomowy	2	34
Kaczka hodowlana	10	122 948
Kaczka rzeźna	74	980 097
Kaczka ogólnoużytkowa	2	47 057
Kaczka przydomowa	24	296
Gęś hodowlana	7	31 832
Gęś rzeźna	17	158 837
Gęś ogólnoużytkowa	1	3 530
Gęś przydomowa	7	196
Perlica	11	4 767
Gołąb	2	59
Bażant	1	3 017
Kuropatwa	0	0
Przepiórka	1	4
Paw	1	6
RAZEM	**414**	**11 479 909**

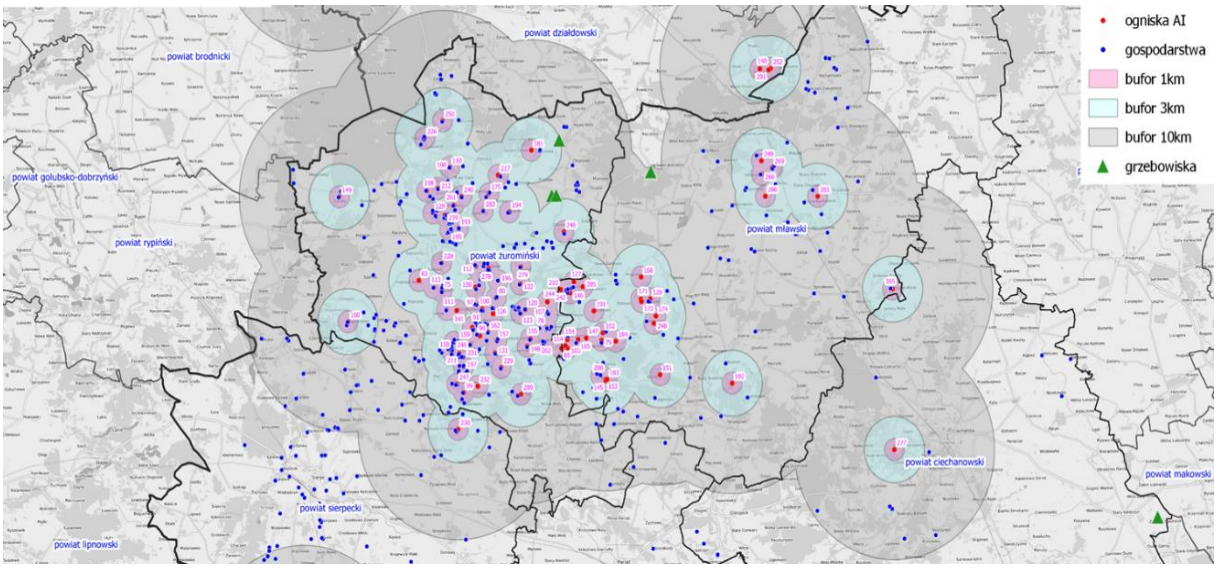
Rządowe Centrum Bezpieczeństwa
Al. Ujazdowskie 5, 00-583 Warszawa | fax. +48 22 361 69 75
poczta@rcb.gov.pl | www . r c b . g o v . p l



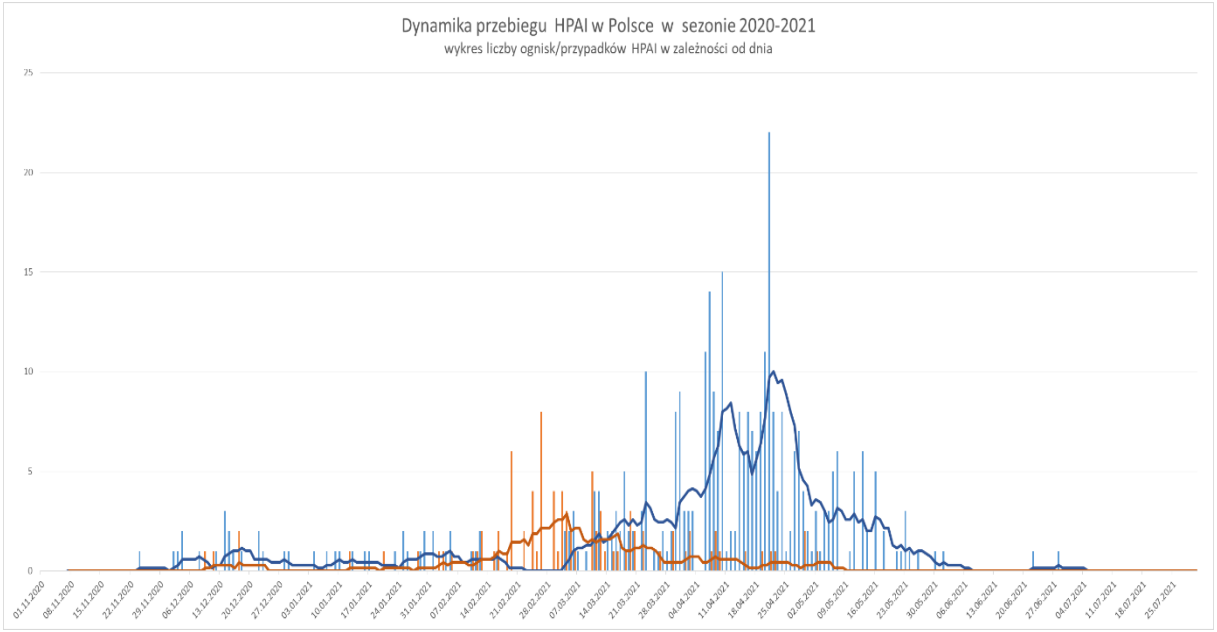
Ponadto należy zaznaczyć, że większość ognisk HPAI stwierdzonych w Polsce od listopada 2020 r. do tej chwili, wykryto w gospodarstwach położonych w pobliżu cieków wodnych (rzeki, stawy, jeziora), stanowiących miejsca ostoi i bytowania migrującego ptactwa wodnego lub na terenie, gdzie występowały sztuczne zbiorniki wodne np. retencyjne lub przeciwpożarowe, niezabezpieczone odpowiednio przed dzikim ptactwem.

Szczególnie niekorzystna i trudna sytuacja epizootyczna w bieżącym roku wystąpiła na terenie województwa wielkopolskiego oraz północnej części mazowieckiego – w powiecie żuromińskim i powiatach ościennych. Dużą rolę odegrała tu koncentracja produkcji drobiu na ograniczonym, małym terenie, co skutkowało wystąpieniem ognisk w niedalekiej odległości od siebie oraz w krótkich odstępach czasu wraz z cyklicznym ich „wysypem" i tzw. efektem domina. Na taką sytuację złożyło się wiele czynników, które wymagały ponadstandardowego podejścia do zwalczania choroby w celu jej szybkiego opanowania. Szczególnie ważnym elementem wpływającym na możliwość zahamowania szerzenia się choroby przy takiej koncentracji produkcji oraz przerwaniu i zatrzymaniu łańcucha występowania nowych ognisk, było wprowadzenie działań prewencyjnych, w tym przede wszystkim zmniejszenie koncentracji pogłowia zwierząt wrażliwych, szczególnie w promieniu 1 km od ognisk, mając na uwadze możliwość przenoszenia się wirusa HPAI przez wiatr. Dużą rolę odgrywało również szybkie zabezpieczenie ogniska choroby, przeprowadzenie szczegółowego dochodzenia epizootycznego ze wskazaniem wektorów wniknięcia choroby do gospodarstwa oraz wszystkich możliwych powiązań w tym zakresie. Obecnie w Głównym Inspektoracie Weterynarii wprowadzane są dodatkowe narzędzia, które w wyniku nabytych doświadczeń z grypy ptaków w sezonie 2020/2021 pozwolą jeszcze lepiej przygotować się do kolejnego sezonu grypowego. W tym celu została przygotowana aplikacja ZID-AI (Zintegrowany Interfejs Drobiowy – Avian Inflenza), który przyspieszy i doprowadzi do większej mobilności działań, wraz z możliwością generowania i mapowania analizy ryzyka.

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



Należy dodatkowo podkreślić, że zgodnie z informacjami Państwowego Instytutu Weterynaryjnego – Państwowego Instytutu Badawczego w Puławach, z badań nad identyfikacją molekularnych markerów zagrożenia zdrowia człowieka (miejsca wiązania receptorów, intensywność replikacji w komórkach ssaków) wynika, że wirusy grypy H5N5 (jedno wystąpienie u dzikich ptaków w lutym 2021 r.) i H5N8 (wszystkie ogniska i pozostałe przypadki) stwierdzone w Polsce nie posiadają cech zwiększonej zakaźności oraz patogenności dla ludzi. Przeprowadzona w Instytucie w Puławach analiza genomu szczepu wirusa grypy H5N8 potwierdza jego wysoki stopień podobieństwa do szczepów wirusa krążących w Europie, co jednoznacznie wskazuje na ich wspólne pochodzenie. Uzyskane wyniki nie pozwalają jednak na precyzyjne określenie obszaru geograficznego, z którego wirus trafił do Polski, gdyż identyczny poziom podobieństwa genetycznego występuje zarówno w sekwencjach wirusów wykrytych w państwach leżących na zachód od Polski (np. w Niemczech, Danii, Belgii, Holandii, Wielkiej Brytanii), jak również na wschód od naszego kraju (Rosja). Z kolei wirus H5N5 powstał w wyniku reasortacji wirusów H5N8 występujących w Europie oraz nisko patogennych wirusów grypy krążących w euroazjatyckiej populacji dzikich ptaków.



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

Odnosząc się do sezonu grypowego 2020-2021 należy stwierdzić, że była to największa jak dotąd epizoocja wysoce zjadliwej grypy ptaków (HPAI) która dotknęła Europę w dotychczasowej jej historii, zarówno pod względem czasu jej trwania jak i liczby stwierdzonych ognisk choroby. W całym sezonie w Unii Europejskiej wykryto ponad 1350 ognisk u drobiu oraz blisko 2900 przypadków u dzikiego ptactwa, z tego we Francji stwierdzono 438 ognisk, a w Niemczech 209 i ponad 820 przypadków u dzikiego ptactwa.

W Polsce w tym czasie potwierdzono 357 ognisk (19 ognisk w 2020 r. i 338 w 2021r.) oraz 92 przypadki u dzikich ptaków (5 w 2020 r. i 88 w 2021 r.), co tylko potwierdza niespotykany i groźny charakter epidemii grypy ptaków w tym sezonie. Należy pamiętać, że duży stopień zmienności genetycznej oraz mutacje wirusa grypy ptaków mogą powodować w przyszłych sezonach podobną skalę epizoocji, dlatego tak ważne jest prowadzenie działań prewencyjnych zarówno przez administrację państwową, ale również, a może przede wszystkim, przez samych producentów i hodowców drobiu. Szczególnie ważnym elementem przeciwdziałania i niedopuszczenia do osiągnięcia stanu krytycznego epizoocji jest zachowanie wysokiego poziomu bioasekuracji gospodarstw drobiarskich, uwzględniając jej złożony i zróżnicowany profil produkcji, szczególnie w okresie jesienno-zimowym, najbardziej narażonym na występowanie licznych ognisk choroby.

Pamiętajmy jednak, że obecnie, pomimo braku stwierdzanych ognisk choroby, w Europie w dalszym ciągu występują jeszcze przypadki grypy ptaków u dzikiego ptactwa, co wskazuje na wciąż istniejące zagrożenie i presję wirusa w środowisku, pomimo warunków pogodowych, które powinny już całkowicie wyciszyć bieżącą sytuację.

Terroryzm w Unii Europejskiej w cieniu Covidu i Brexitu

Sebastian Wojciechowski
Instytut Zachodni i UAM w Poznaniu

Covid-19 oraz inne, rozliczne problemy występujące w poszczególnych częściach świata spowodowały, iż społeczność międzynarodowa coraz częściej zapomina o zagrożeniu terrorystycznym. Ono jednak niestety wciąż istnieje, a w niektórych przypadkach wręcz narasta. Potwierdza to na przykład najnowszy raport Europolu „European Union Terrorism Situation and Trend Report 2021". Jest to już dwunasta edycja tego specjalistycznego opracowania, obejmująca tym razem 2020 rok. Ze względu na Brexit, raport zawiera przede wszystkim dane uwzględniające Unię Europejską w obecnym kształcie czyli bez Wielkiej Brytanii. W tekście są jednak dość liczne odniesienia i do tego państwa.

Analizując najważniejsze aspekty zawarte w tym obszernym (ponad stustronicowym) opracowaniu warto przede wszystkim zwrócić uwagę na następujące kwestie:

SKALA ATAKÓW TERRORYSTYCZNYCH

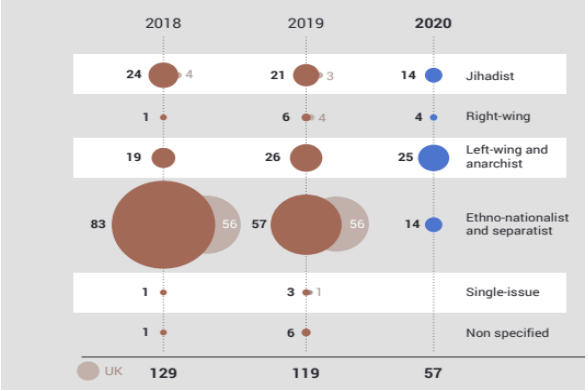
W Unii Europejskiej (włącznie z Wielką Brytanią) w 2020 r. (podobnie, jak rok wcześniej) doszło do 119 przeprowadzonych, nieudanych i udaremnionych ataków terrorystycznych. Uwzględniając natomiast przypadki bez Wielkiej Brytanii było ich 57 (a w 2019 r. 55). W minionym roku na skutek terroryzmu w UE (wraz z WB) zginęły 24 osoby (rok wcześniej odnotowano łącznie 13 ofiar śmiertelnych). Powyższy wzrost to między innymi następstwo krwawego zamachu przeprowadzonego w lutym w Niemczech, w wyniku którego zginęło 9 osób.

PROFIL IDEOLOGICZNY SPRAWCÓW

W 2020 r. zamachy (z pominięciem WB) miały charakter: skrajnie lewicowy i anarchistyczny (25), dżihadystyczny (14), etnonacjonalistyczny i separatystyczny (14) oraz skrajnie prawicowy (4). Dotyczyły sześciu państw: Włoch (24), Francji (15), Hiszpanii (9), Niemiec (6), Belgii (2) i Austrii (1). W ocenie Europolu, nadal najbardziej niebezpiecznym nurtem terroryzmu w Unii Europejskiej jest dżihadyzm. Z taką sytuacją mamy do czynienia pomimo spadku liczby ataków w tej kategorii. W 2019 r. (bez WB) było ich 18, a rok później 14. Szczegółowa analiza pokazuje jednak, że w minionym roku (w przeciwieństwie do 2018 r. czy 2019 r.) liczba przeprowadzonych ataków islamistycznych ponad dwukrotnie przewyższyła zakres tych udaremnionych (proporcja 10:4), co pokazuje charakter problemu. Istotny wpływ na występowanie powyższego

zagrożenia ma nie tylko działalność dżihadystów w państwach członkowskich UE, ale także wydarzenia rozgrywające się poza terytorium Unii. Przykładem jest funkcjonowanie ISIS czy Al-Kaidy oraz powiązanych z nimi organizacji, które cały czas są aktywne np. na Bliskim Wschodzie, w Afryce czy Azji. Na wzmożoną uwagę zasługują również i pozostałe nurty terroryzmu. Niektóre z nich np. terroryzm skrajnie lewicowy i anarchistyczny od lat utrzymują się na zbliżonym poziomie aktywności (19 ataków w 2018 r., 26 w 2019 r. i 25 w 2020 r.). Pośrednio dotyczy to też terroryzmu skrajnie prawicowego – 1 atak w 2018 r., 6 w 2019 r. (w tym 4 w WB) oraz 4 w 2020 r. Bardzo duża zmiana wystąpiła natomiast w przypadku zagrożenia etnonacjonalistycznego i separatystycznego. Szczegółowo ukazuje to poniższe zestawienie.

Zakres i profil zagrożenia terrorystycznego w UE w latach 2018-2020



Źródło: ,,European Union Terrorism Situation and Trend Report 2021", https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2021-tesat

METODY DZIAŁANIA TERRORYSTÓW

Na uwagę zasługuje także forma przeprowadzonych ataków. Prawie wszystkie były realizowane przez tzw. samotne wilki. W niektórych przypadkach sprawcy mieli jednak powiązania z innymi osobami lub grupami o charakterze terrorystycznym, niejednokrotnie też zostali zradykalizowani przez Internet lub pobyt w więzieniu. U części z nich zaobserwowano zespolenie skrajnych poglądów z zaburzeniami psychicznymi. Dotyczy to m.in. dżihadystów oraz prawicowych ekstremistów. W minionym roku ataki często były realizowane z wykorzystaniem broni palnej lub noży, a zatem nie wymagały ani zaawansowanego zaangażowania technologicznego, ani finansowego. Nie odnotowano żadnego poważnego aktu z użyciem materiałów wybuchowych. Może to wynikać z różnych przyczyn – począwszy od ograniczeń i utrudnień pandemicznych, poprzez osłabienie zdolności logistycznych terrorystów, a kończąc na instrukcjach przekazywanych np. przez ISIS, aby przeprowadzać zamachy z wykorzystaniem najprostszych środków.

ARESZTOWANIA EKSTREMISTÓW

W Unii Europejskie (bez WB) znacząco spadła liczba osób aresztowanych za działalność terrorystyczną z 723 w 2019 r. do 449 w 2020 r. Według autorów raportu, trudno jednoznacznie stwierdzić czy świadczy to o zmniejszonej aktywności terrorystów czy też jest rezultatem ograniczonych zdolności służb podczas pandemii. Większość przypadków (ok. 57%) dotyczyła terroryzmu dżihadstycznego – 254, a ponadto niesklasyfikowanych jego form – 69, skrajne lewicowego i anarchistycznego – 52, etnonacjonalistycznego i separatystycznego – 39, skrajnie prawicowego – 34 i innych rodzajów – 1. Najwięcej osób aresztowano we: Francji – 127, Belgii – 61, Hiszpanii – 57, Włoszech – 45 i Niemczech – 44. W Polsce odnotowano 9 zdarzeń – 8 o charakterze dżihadystycznym i 1 skrajnie prawicowym. Na podkreślenie zasługuje coraz młodszy wiek zatrzymanych oraz fakt, że niejednokrotnie są to osoby niepełnoletnie.

ESKALACJA ISLAMIZMU

W kolejnych miesiącach dżihadystyczne zagrożenie w UE może się nasilić, co będzie związane m.in. z wycofywaniem sił NATO z Afganistanu oraz ukazywaniem tego wydarzenia przez fundamentalistów jako spektakularny przykład zwycięstwa ,,islamu nad Zachodem". Ma to być także zachęta do kontunuowania walki w innych częściach świata, również na obszarze UE. Na wzrost aktywności islamistów wpłynie też zapewne np. słabnięcie pandemii, znoszenie lockdownu i innych ograniczeń, zwiększony ruch osobowy (choćby wakacyjny), napływ migrantów czy kolejna fala powrotu do Europy osób, które na różne sposoby wspierały ISIS. Istotną przesłanką może być także zbliżająca się 20. rocznica ataków z 11.09 2001 r. Jest ona interpretowana przez dżihadystów jako moment triumfu oraz impuls do dalszych akcji.

PROPAGANDA W INTERNECIE

W raporcie podkreślono, iż terroryści wykorzystują każdą sposobność do szerzenia strachu czy propagandy. W tym kontekście Covid-19 oraz towarzyszący temu wzrost wykorzystania Internetu okazał się dla nich bardzo sprzyjającą okazją

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

– z jednej strony do propagowania nienawiści, natomiast z drugiej do integrowania zwolenników. Od momentu utrudnienia możliwości korzystania z komunikatora Telegram (koniec 2019 r.) islamiści mają problemy ze znalezieniem uniwersalnego kanału komunikacyjnego. W związku z tym, ich propaganda jest rozproszona na różnych platformach. Nadal jednak pozostaje skuteczna i groźna. W Internecie wzrasta także aktywność innych grup ekstremistycznych m.in. skrajnie prawicowych czy lewicowych. Obok tradycyjnej tematyki chętnie podejmują one nowe wątki związane np. problematyką ekologiczną, technologiczną czy pandemiczną.

KONKLUZJE

Zjawisko terroryzmu można przyrównać do wciąż mutującego wirusa, który występuję w różnych częściach świata. Jego obecny zakres czy charakter ciągle ulega zmianie. Choć zamachy terrorystyczne w UE w skali świata stanowią tylko kilka procent ogółu. Unia, ze względu na swoje znaczenie polityczne, ekonomiczne czy medialne, a także występujące w jej obrębie różnice religijne i etniczne, pozostaje ich ważnym celem. Wpływają na to też inne przesłanki, np. eskalacja różnego rodzaju ekstremizmów, napięć i frustracji związanych z Covid-19 czy przekonanie głoszone przez część radykałów, że teraz jest najlepszy moment, aby zaatakować osłabione i wciąż skoncentrowane na walce z pandemią państwa członkowskie. Nie można również pominąć uwarunkowań zewnętrznych w postaci m.in. destabilizacji sytuacji w różnych częściach świata, odradzania się ISIS czy AL-Kaidy, wycofania NATO z Afganistanu i sukcesów Talibów, a także bardzo niebezpiecznej i realizowanej na różne sposoby polityki mocarstw lub innych państw niedemokratycznych. Powoduje to, że podmioty pozapaństwowe, jak i państwowe stosujące terroryzm, będą używać równocześnie bardzo zróżnicowanych metod – począwszy od środków klasycznych, przez cyberterroryzm czy cyberprowokacje, a kończąc nawet na elementach bioterroryzmu (wykorzystując m.in. wnioski z ostatniej pandemii). Pozwoli im to uzyskać efekt zaskoczenia, paniki czy paraliżu w wybranym miejscu, czasie i skali. Niestety wskazane zagrożenia w coraz większym stopniu, cojuż obserwujemy, będą dotyczyć także i Polski. Kwestia ta wymaga jednak odrębnego omówienia.

Technologia a bezpieczeństwo w dobie zagrożeń hybrydowych

Kamil Stobnicki

Rządowe Centrum Bezpieczeństwa

W nowym środowisku bezpieczeństwa, determinowanym zagrożeniami hybrydowymi, coraz bardziej zacierają się pojęcia pokoju, kryzysu i wojny, stwarzając wrogom nieograniczone pole oddziaływania m.in. z wykorzystaniem potężnego instrumentarium technologicznego. Nigdy wcześniej postęp technologiczny nie wywierał tak przemożnego wpływu na bezpieczeństwo – nie tylko zwiększając poziom zagrożeń. Jednocześnie stworzył możliwości i narzędzia służące przeciwdziałaniu tym zagrożeniom.

Podobnie jak poprzednie rewolucje technologiczne, tak i obecna – zmienia, acz wyjątkowo dynamicznie – równowagę sił. W istniejący system bezpieczeństwa włączają się coraz aktywniej nowe podmioty, tzw. aktorzy niepaństwowi *(non-state actor),* na przykład duże koncerny medialne czy technologiczne, organizacje przestępcze lub prywatne firmy militarne. Coraz szerzej dostępne nowe technologie oferują – zarówno podmiotom państwowym, jak i tym niepaństwowym – nowe narzędzia. Te z kolei mogą zostać wykorzystywane do penetrowania luk w systemie bezpieczeństwa narodowego i międzynarodowego, a także podatności – nie tylko w odniesieniu do sił zbrojnych, ale także lub w szczególności wobec ludności cywilnej czy infrastruktury krytycznej.

Weźmy za przykład sektor energetyczny – wzajemne powiązania globalnego łańcucha dostaw surowców energetycznych zapewniają z jednej strony dużo większą wydajność tego sektora, z drugiej strony, mnogość wzajemnych połączeń stwarza większe możliwości ataku. Zauważalny jest zwłaszcza znaczący wzrost aktywności przestępców cybernetycznych, często na usługach innego państwa, którzy rozmieszczają złośliwe oprogramowanie zdolne do zakłócenia całych łańcuchów dostaw. Obecni „aktorzy hybrydowi" posiadają zdolności cybernetyczne do sparaliżowania całych systemów

przesyłu – nie tylko energii, lecz i innych dóbr jak woda czy ropa lub gaz.

Powyższe wpisuje się w obserwowane trendy, które wpływają bardzo mocno na obecne środowisko bezpieczeństwa, szczególnie w kontekście zwalczania ingerencji hybrydowych.

Wspólne Centrum Badawcze Komisji Europejskiej *(Joint Research Centre, JRC)* stworzyło portal internetowy *The Megatrends Hub,* na którym prezentuje długoterminowe globalne trendy, które już mają, bądź względnie będą mieć, znaczący wpływ na środowisko bezpieczeństwa UE i jej sąsiedztwo:[1]

- postępująca cyfryzacja,
- rosnące nierówności ekonomiczne,
- zmiany klimatyczne i degradacja środowiska,
- rosnące znaczenie migracji,
- rosnąca konsumpcja,
- pogłębiający się niedobór zasobów,
- rosnące dysproporcje demograficzne,
- rosnące wpływy Wschodu i Południa,
- przyspieszanie zmian technologicznych, w tym w dziedzinie łączności,
- zmiana charakteru pracy,
- zmiana modelu edukacji i uczenia się,
- nowe wyzwania zdrowotne,
- postępująca urbanizacja,
- rosnący wpływ nowych systemów, modeli rządzenia,
- zmiana paradygmatu bezpieczeństwa.

Z kolei Sojusz Północnoatlantycki, a konkretnie tzw. Grupa Refleksyjna opracowała raport *NATO 2030. United for a New Era*, który odnosi się do uwarunkowań i perspektyw rozwoju środowiska bezpieczeństwa do 2030 r.[2] Najważniejsze kwestie (a jednocześnie obecne i przyszłe wyzwania, jakim musi stawić czoła Sojusz) wymienione w raporcie dotyczą:

- Rosji,
- Chin,
- przełomowych technologii,
- terroryzmu,
- Południa,
- kontroli zbrojeń i odstraszania jądrowego,
- bezpieczeństwa energetycznego,
- klimatu,
- bezpieczeństwa ludzkiego i sytuacji kobiet,
- pandemii i katastrof naturalnych,
- zagrożeni hybrydowych i cybernetycznych,
- przestrzeni kosmicznej,
- komunikacji strategicznej,
- dyplomacji publicznej,
- zwalczania dezinformacji.

Bycie skutecznym w środowisku współczesnych wyzwań i zagrożeń wymusza – zarówno na państwach jak i organizacjach międzynarodowych (NATO i UE), systematyczną intensyfikację wysiłków w celu przeciwdziałania zagrożeniom hybrydowym, stale uwzględniając nowe z nich, które mają bardziej społeczny i ekonomiczny charakter – ale równie duży wpływ na bezpieczeństwo, co zagrożenia militarne. Zasada ta kierowała zarówno Sojuszem Północnoatlantyckim, kiedy to w 2016 roku podczas szczytu w Warszawie przywódcy Sojuszu zobowiązali się do wzmacniania odporności w siedmiu obszarach, jak i Unią Europejską, która poprzez szereg działań podkreśla konieczność budowania odporności w takich sektorach jak transport, komunikacja, finanse lub regionalna infrastruktura bezpieczeństwa. Kroki takie podejmuje się, aby oprzeć się chociażby propagandzie, kampaniom dezinformacyjnym, próbom osłabienia zaufania do władzy, osłabienia samych społeczeństw, a także atakom na infrastrukturę związana z cyberprzestrzenią.

Innym tego typu przykładem jest przedstawiony przez KE plan działania na rzecz synergii między przemysłem cywilnym, obronnym i kosmicznym.[3] Stwarza on możliwości zwiększenia europejskich zdolności w zakresie innowacji poprzez badanie i wykorzystywanie przełomowego potencjału technologii w sektorach obronności, przestrzeni kosmicznej oraz w sferze cywilnej (np. chmura, procesory, technologie cybernetyczne i kwantowe oraz sztuczna inteligencja).

[1] Wyselekcjonowano i opisano 14 trendów istotnych z punktu widzenia przyszłości UE: https://knowledge4policy.ec.europa.eu/foresight/tool/megatrends-hub_en

[2] Grupa Refleksyjna to zespół 10 ekspertów powołany przez Sekretarza Generalnego NATO, który przedstawił rekomendacje, jak doprowadzić do wzmocnienia mechanizmów konsultacji i politycznego wymiaru Sojuszu. Jednym z ekspertów była b. minister spraw zagranicznych RP, Anna Fotyga.

[3] Action Plan on Synergies between Civil, Defence and Space Industries, z dnia 22 lutego br.

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

Tym, co jednak w najbliższej przyszłości najbardziej zmieni nasze życie, będzie sztuczna inteligencja (*Artificial Intelligence, AI*),[4] która niesie ze sobą zarówno zagrożenia, jak i możliwości. Może być wykorzystywana do wykrywania i identyfikowania schematów czy pewnych symulacji, umożliwiając m.in. postępy w dziedzinie rozpoznawania głosu i rysów twarzy. Wszystkie te zdolności mogą być kluczowe dla np. zwalczania terroryzmu, obrony cywilnej czy reagowania w przypadku katastrof. Sztuczna inteligencja może przyczynić się do lepszej działalności wywiadowczej, świadomości sytuacyjnej, analiz oraz – co za tym idzie – do podejmowania trafniejszych decyzji. Te państwa, które mogą decydować o infrastrukturze i standardach wspierających działania w obszarze AI, uzyskają przewagę strategiczną nad pozostałymi. Te i inne kwestie sprawiły, że Parlament Europejski pracuje nad pierwszym pakietem przepisów koncentrującym się na budowaniu zaufania do sztucznej inteligencji.

Ze sztuczną inteligencją wiąże się kwestia, która może dotyczyć każdego z nas, czyli tzw. inteligentnego miasta (*smart city*). Jego koncepcja reprezentuje pewien rodzaj utopii ideału, w którym potrzeby mieszkańców doskonale współgrają z zaawansowaną technologią. W *smart city* inteligentne rozwiązania są niemal wszędzie – od samochodów, po sprzęt AGD. Zastosowane w nich technologie – i coraz częściej sztuczna inteligencja – obliczają i reagują na potrzeby obywateli, poprawiając jakość ich życia i bezpieczeństwo. Oznacza to uwolnienie ludzi od konieczności dostosowywania się do pewnych ograniczeń miasta, takich jak korki i niedostępność, a także umożliwienie miastu dostosowania się do potrzeb ludzi w obliczu postępującej urbanizacji, starzejącej się populacji czy zmian klimatycznych. Oznacza to jednak z drugiej strony rosnącą zależność od inteligentnych infrastruktur, dostawców technologii i nadzoru, tworząc nowe nieznane środowisko. Korzyści, możliwości, zagrożenia i słabości są nadal nieznane.

W środowisku bezpieczeństwa, w którym zagrożenia hybrydowe stały się jednym z głównych wyzwań dla społeczeństw demokratycznych, środowisko inteligentnego miasta stwarza jednak nowe możliwości dla wrogich działań, chociażby poprzez gromadzenie, przechowywanie i analizowanie ogromnej ilości danych, które mogłyby zostać wykorzystane przez adwersarza. Inteligentne miasto może być celem kampanii hybrydowej zarówno w czasie pokoju, poniżej progu otwartego konfliktu, jak i w czasie wojny. Formy oddziaływania hybrydowego w kontekście miast są nadal badane.

Przy tej kwestii należy nawiązać do technologii 5G, która jest warunkiem funkcjonowania i rozwijania się inteligentnego miasta. Era 5G stworzy funkcje sieciowe i usługowe, które wcześniej nie były dostępne, umożliwiając prawdziwy *Internet Rzeczy*. Dzięki 5G coraz więcej urządzeń może być podłączonych do sieci, co pozwala im utrzymywać łączność w dowolnym momencie i w dowolnym miejscu. Dzięki rozwiązaniom w zakresie przetwarzania w *chmurze* i technologii *big data* jesteśmy o krok bliżej do inteligentnej rzeczywistości miejskiej, w której znajdują się urządzenia komunikujące się ze sobą w czasie rzeczywistym w oparciu o ogromną ilość przetworzonych i szybko przeanalizowanych danych.

Unijna komórka *Hybrid Fusion Cell* (*HFC*), współpracując z NATO, opracowała niejawny raport nt. dezinformacji z wykorzystaniem *AI*. Sztuczna inteligencja stanowi w ocenie autorów jedno z kluczowych wyzwań dla współczesnego bezpieczeństwa. Skutecznym sposobem przeciwdziałania może być wykorzystanie *AI* zgodnie z zasadą: „*Only AI can counter AI*", stąd tak kluczowy rozwój tej technologii na poziomie krajowym i unijnym. Chociażby w zakresie zwalczania deep-fakes[5], już teraz istnieją takie algorytmy, które są w stanie poprawnie rozpoznać czy wyłapać takie fałszywe pliki, np. materiały wizualne, powstałe tą metodą. Obecnie trwa wyścig o posiadanie *AI*, która musi działać w oparciu zarówno o odpowiednie algorytmy, jak i masowe bazy danych oraz odpowiednią infrastrukturę.[6]

[4] Sztuczna inteligencja to zdolność maszyn do wykonywania pewnych zadań, wymagających ludzkiej inteligencji, takich jak np. rozpoznawanie schematów, uczenie się z doświadczeń, wyciąganie wniosków lub przewidywanie.

[5] Dynamicznie rozwijającą się w przestrzeni komunikacyjnej kategoria. Technologia (algorytm uczenia maszynowego) wykorzystuje sztuczną inteligencję do tworzenia realistycznych fałszywych filmów, w których podstawia się głos lub zdjęcie innej osoby. Deep-fake nie zawsze wyrządza szkody, np. gdy wykorzystywany jest w produkcji filmowej, może jednak stanowić poważne zagrożenie dla demokracji i bezpieczeństwa, a także dla indywidualnych osób, które mogą stać się obiektem zniesławień czy szantażu.

[6] Wykorzystano informację ze sprawozdania z nieformalnej wideokonferencji HWP ERCHT z 24.02.2021. We wrześniu 2017 roku podczas przemówienia do studentów w Moskwie prezydent Władimir Putin wygłosił słynną tezę, iż dowolne państwo, które stanie się liderem w badaniach nad sztuczną inteligencją (SI) „stanie się władcą świata".

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

Jednym z istotniejszych trendów w zakresie zagrożeń hybrydowych są coraz bardziej wyrafinowane metody ataków na infrastrukturę krytyczną. Sprzyja temu powszechna cyfryzacja, zwiększona podatność systemów sterowania przemysłowego, rozwój sztucznej inteligencji (ułatwia monitorowanie w czasie rzeczywistym dużych zasobów danych oraz błyskawiczne wykrywanie anomalii w ruchu sieciowym), komputerów kwantowych czy *big data*. Ostatni raport EUROPOL-u potwierdza, że infrastruktura krytyczna państw członkowskich UE będzie celem cyberprzestępców w ciągu najbliższych lat. Istotny wpływ na to będą mieć takie kwestie, jak: rozwój Internetu Rzeczy, powszechność wykorzystania sztucznej inteligencji, zastosowania danych biometrycznych czy dostępność pojazdów autonomicznych.[7] Istotnym elementem jest tutaj również rosnąca współzależność infrastruktur jak np. w dziedzinie energetycznej czy też medycznej co powoduje możliwość zakłócenia dystrybucji na coraz szerszym obszarze.

Za przykład takiej sytuacji niech posłuży cyberatak na szpital uniwersytecki w Brnie w marcu 2020 roku, który to paraliżując system informatyczny zakłócił pracę szpitala, zmuszając m.in. do zmiany terminów operacji czy też wpływając negatywnie na działanie samego laboratorium, w którym przeprowadzane były testy na obecność koronawirusa (skutkowało to niemożnością wysłania informacji do centralnej bazy danych). Jednocześnie, biorąc pod uwagę, że taki atak mógł kosztować życie pacjentów, coraz częściej państwa atakowane będą mierzyć się z pytaniem – czy tym razem jest to jeszcze działanie podprogowe czy już otwarty akt agresji? Trendem jest zwiększająca się liczba ataków, które w pośredni sposób mogą przyczynić się do utraty życia lub zdrowia lub „wyłączyć" na określony czas dany obszar życia społecznego.

Istotnym trendem, na który zwraca się uwagę, jest tendencja do większego uwzględniania tzw. sfery behawioralnej przy reagowaniu na zagrożenia hybrydowe. Obecne działania podejmowane we wszystkich pięciu domenach – powietrznej, lądowej, morskiej, kosmicznej i cyber – są ukierunkowane na to, aby wywrzeć wpływ, skłonić do określonego zachowania. Dlatego pojawiają się głosy, że, być może, nadszedł czas, aby NATO uznało znaczenie szóstej domeny operacyjnej – human domain. W opracowaniach na ten temat pojawia się postulat przykładania większej wagi do obecnie za mało docenianego czynnika behawioralnego. Aktywność „przeciwnika hybrydowego" pośród wielu obszarów ukierunkowana jest na oddziaływanie na psychikę jednostki. Wojna w Afganistanie pokazała, że nie da się osiągnąć pewnych celów politycznych, nie próbując zrozumieć środowiska (i mentalności ludzi), w którym się działa. Istnieją trzy kluczowe wektory, które zasługują na rozważenie przez decydentów: aktorzy działań, przekazywane treści i zachowania. W większości dyskusja koncentruje się na dążeniu do zrozumieniu intencji aktorów i natury treści. Wobec niedostatecznej uwagi poświęcanej czynnikowi behawioralnemu pojawia się odczucie, że cały czas pozostaje się w tyle za przeciwnikiem. A warto pamiętać, że ludzkim zachowaniem rządzą stosunkowo stabilne zasady, pomimo szybko zmieniającego się środowiska technologicznego.

[7] https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment

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

Konfrontacja macierzy manipulacyjnych (własnej p-ko macierzy przeciwnika) jako narzędzie dezinformacji i aktywnej obrony podczas procesu rozpoznania aktywności aktora państwowego, w tym grup APT

Kamil Basaj
Fundacja INFO OPS Polska

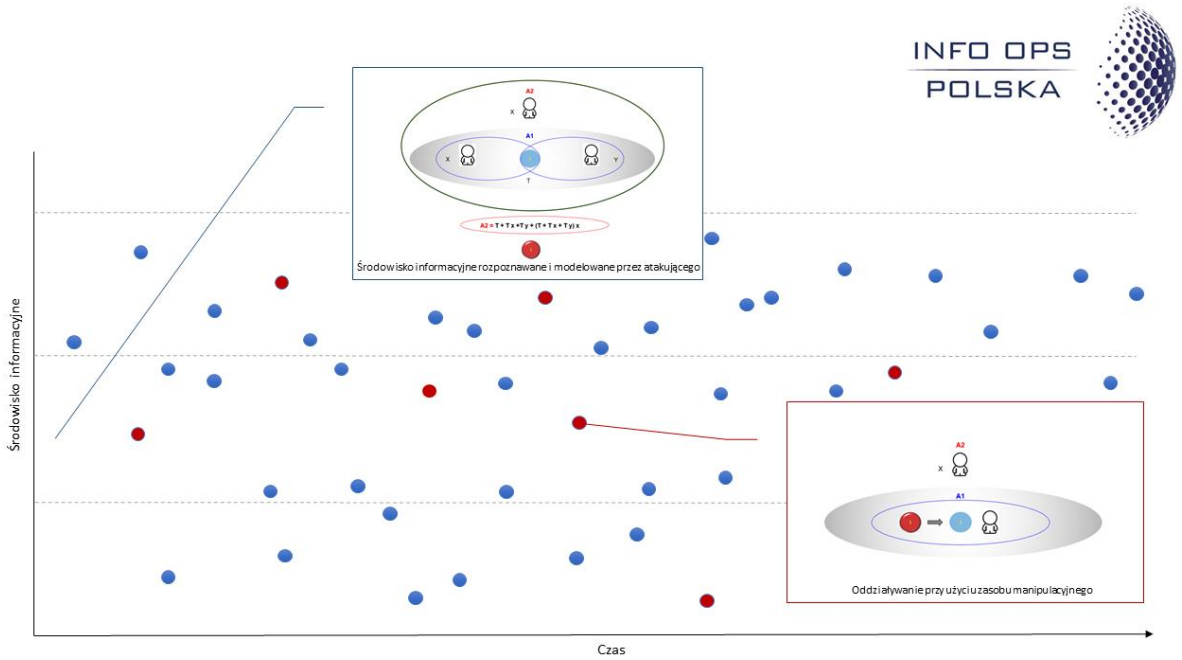
Rozpoznanie to ciągły proces konfekcjonowania informacji, zgodnie z obszarem odpowiedzialności danej organizacji. Każde zdarzenie, którego analiza może być niezbędna na potrzeby definiowania incydentu, pozostawia ślad, a jego umiejętne zdefiniowanie ułatwia stawianie pytania wywiadowczego i wstęp do procesu prowadzenia właściwego rozpoznania.
Przestrzeń informacyjna rozpoznawana pod kątem bodźców, które ją kształtują, to wzajemnie przenikające się wymiary: fizyczny, wirtualny i społeczno-poznawczy, a oddziaływanie tych wymiarów, ich relacje, sekwencje zdarzeń i wzajemne odwzorowania składają się na ciąg informacji, który kształtuje świadomość sytuacyjną analityka odpowiedzialnego za definiowanie incydentu.

Uzyskanie kontroli, rozumianej jako zdolność do prowadzenia rozpoznania w środowisku informacyjnym, umożliwia określenie i osadzenie w kwerendach rozpoznania danych, wystąpienie których może oznaczać zastosowanie przez aktora zaawansowanych modeli manipulacyjnych kształtujących środowisko informacyjne. Dane te mogą towarzyszyć aktywności aktora lub wprost stanowić narzędzie ataku. Jednym z elementów wspomagających proces rozpoznania zagrożeń, wynikających z aktywności aktorów państwowych, w tym grup APT, jest uzyskanie przez analityka stanu kontroli środowiska informacyjnego poprzez zastosowanie zdolności do określenia obiektów (osobowych i nieosobowych) i ich oddziaływania (kinetycznego i niekinetycznego) oraz zastosowanych modeli kształtujących środowisko informacyjne w obszarze odpowiedzialności analityka lub obszarze potencjalnego zainteresowania adwersarza.

Prawidłowo zidentyfikowana informacja, wyodrębniony zespół bodźców, umożliwia analitykowi określenie potencjalnej sekwencji działań przeciwnika oraz określenie bodźców, którymi będzie się posługiwał kształtując środowisko informacyjne w przyszłości. Precyzyjne określenie i predykcja bodźca (tj. informacji) w kontekście działań o charakterze manipulacyjnym umożliwia również wstępne określenie czy atakujący posługuje się specjalistycznymi technikami operacji informacyjnych, narzędziami kontroli odbitej, modelami subiektywizmu, czy macierzy manipulacyjnych.

Dane wejściowe, rozpoznane w środowisku, dają zatem analitykowi możliwość ustalenia modelu działań przeciwnika, który na poziomie taktycznym będzie składał się z określonych (wymaganych w danym modelu) bodźców i sekwencji zdarzeń. Zrekonstruowany w ten sposób obraz aktywności przeciwnika umożliwia analitykowi, w dalszej kolejności, określenie tropów, które będą służyły do pogłębionego rozpoznania, a docelowo do uzyskania kontroli środowiska, która nastąpi w momencie objęcia rozpoznaniem przestrzeni informacyjnej (lub jej określonej części) za pomocą precyzyjnych tropów.

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



Jednym z narzędzi wspomagających działania aktywne aktorów państwowych – w tym np. cyberataki motywowane działalnością wywiadowczą – mogą być macierze manipulacyjne. Ich tworzenie wymaga zastosowania przez atakującego zaawansowanych technik aktywnego rozpoznania (w tym przy użyciu komunikacji sondującej) i profilowania prowadzonego w celu uzyskania zespołu informacji o bodźcach, które mogą zostać efektywnie wykorzystane przeciwko obiektowi oddziaływania. Badanie i dekompozycja procesu tworzenia takiej ofensywnej macierzy manipulacyjnej kieruje analityka na ścieżkę podejścia przeciwnika pod rozpoznanie, które prowadził przy użyciu procesu oddziaływania informacyjnego wobec obiektu lub organizacji i celu ataku. W dalszej kolejności może służyć próbie odtworzenia danych zawartych w macierzy wykorzystywanej przez przeciwnika. Odwrócenie tego modelu działań przeciwnika umożliwi wczesne zidentyfikowanie w rozpoznanych zasobach danych, bodźców, których wystąpienie nie byłoby możliwe bez zastosowania macierzy manipulacyjnej. Stworzenie z odtworzonych danych dedykowanych kwerend rozpoznania umożliwia analitykowi prowadzenie obserwacji aktywności przeciwnika przy zastosowaniu rozpoznanej macierzy.

Bezpieczeństwo środowiska informacyjnego jest procesem, a nie stanem, zatem czynności podejmowane na rzecz jego zapewnienia powinny mieć charakter ciągły. Ciągłość działań jest istotna przede wszystkim w obliczu zagrożeń, w których atakujący, w celu zakonspirowania własnych działań, podejmuje skrytą aktywność sondującą i penetracyjną, unika powielania tych samych działań, aby podnieść jakość maskowania operacji.

Pozostawiane przez atakującego ślady we wczesnym etapie działania, np. podczas prowadzonego namierzania i rozpoznania obiektu (osobowego i nieosobowego) mogą naprowadzać analityka na informacje, które służą do szacowania ryzyka i predykcji dalszej aktywności manipulacyjnej atakującego bez względu na to czy atakujący posługiwał się pasywnym, aktywnym czy mieszanym modelem rozpoznania celu.

Większość stosowanych technik rozpoznania będzie zawierała bodźce, za pomocą których atakujący dąży do uzyskania informacji o reakcji celu ataku na własną aktywność, a to z kolei pozostawia ślady i jest szczególnie widoczne przy zastosowaniu przez atakującego modelu rozpoznania aktywnego. Proces analizy musi jednak każdorazowo uwzględniać ryzyko, że pozostawione przez atakującego tropy mogą służyć dezinformowaniu atakowanego, być elementem działań pozorowanych prowadzonych w celu związania jego sił i środków, w tym odwrócenia uwagi.

Zapewnienie stanu kontroli środowiska informacyjnego ma na celu wczesne rozpoznanie i analizę wszelkich informacji mogących mieć związek z działalnością atakującego. Dalsze analizy i korekty wprowadzane do procesu rozpoznania mogą pomóc określić jakie bodźce, w jakim kontekście sytuacyjnym i wobec jakiego obiektu będą stosowane przez atakującego, w tym na użytek działań o charakterze wywiadowczym i przestępczym.

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

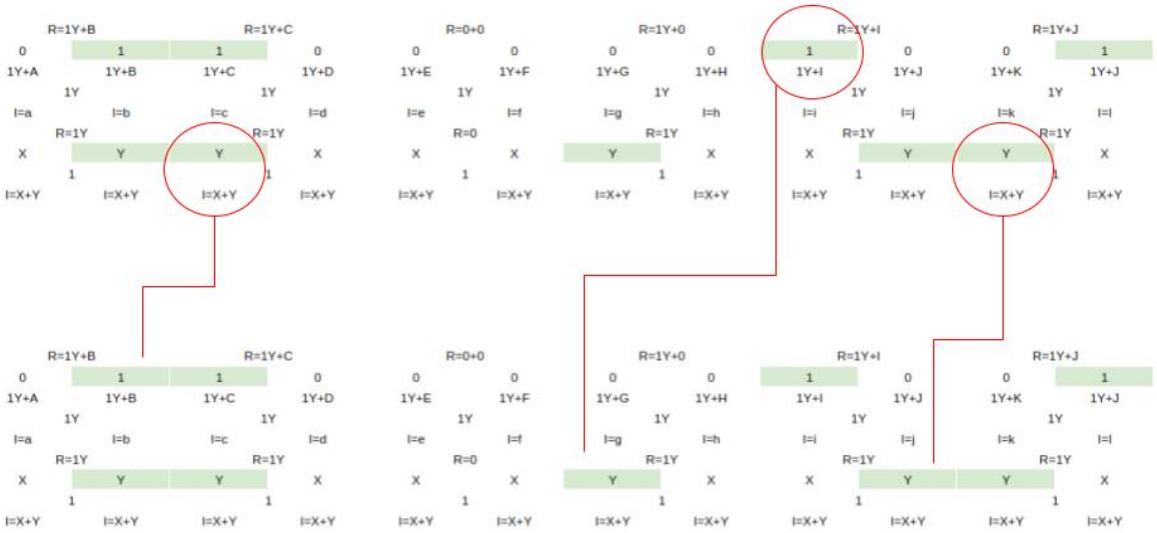
Wczesne zidentyfikowanie działań o charakterze pasywnego lub aktywnego rozpoznania może również pomóc ustalić czy atakujący dąży do wykorzystania podatności psychologicznych obiektu ataku oraz w jaki sposób dąży do ich eksploatacji podczas ataku, presji psychologicznej, szantażu, próby werbunku czy zwykłego cyberszpiegostwa. Dlaczego? Ponieważ każda aktywność atakującego i zastosowany model działania będzie pozostawiał informacje, w tym bodźce, strukturę informacji, obszary występowania, ścieżkę zaadresowania bodźca, czas i miejsce zastosowania.

Z uwagi na złożoność modeli manipulacyjnych, które niejednokrotnie są wprost oparte na wynikach badań modeli poznawczych człowieka, zdecydowana większość zdarzeń kwalifikowanych do danego modelu manipulacyjnego nie będzie przypadkowa, lecz będzie wprost wynikać z metodyki ich stosowania.

Ścisły nadzór nad tego typu aktywnością umożliwia niejednokrotnie predykcję jednego ze stałych etapów operacji, czyli procesu korekty działań, który będzie wprowadzał atakujący, a to umożliwia zastosowanie modeli aktywnej obrony poprzez wczesne przechwycenie i próbę uzyskania kontroli nad procesem rozpoznania realizowanym przez przeciwnika.

Taki proces może być efektywnie oparty na manipulacji danymi, które atakujący chce pozyskać, stosując własną (ofensywną) macierz manipulacyjną. W takim przypadku można zastosować złożony i prowadzony na poziomie taktycznym proces operacji dezinformacyjnej opartej na konfrontacji dwóch macierzy manipulacyjnych: przeciwstawieniu własnej macierzy powstałej w odpowiedzi na rozpoznaną i odtworzoną macierz przeciwnika, a więc – w uproszczeniu – dezinformowanie ofensywnej macierzy manipulacyjnej przeciwnika poprzez zastosowanie macierzy własnej, defensywnej.

INFO OPS POLSKA



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

Zagrożenia hybrydowe dla infrastruktury krytycznej

Aleksandra Gasztold
Uniwersytet Warszawski

Zagrożenie hybrydowe to termin, który często pojawia się we współczesnej debacie politycznej na temat bezpieczeństwa państwa. Wywodzi się on z teorii tzw. wojen asymetrycznych, wskazujących na niekonwencjonalne metody prowadzenia działań wojennych. Wojny takie są znane od czasów starożytnej Grecji, a od XIX wieku są prowadzone przez państwa i niepaństwowych aktorów sceny międzynarodowej[1]. Podobnie jak terroryzm, pojęcie zagrożeń hybrydowych charakteryzuje pewne zjawiska, które w sposób dotkliwy godzą w wartości chronione przez państwo. Dlatego z reguły używane jest w liczbie mnogiej (zagrożenia hybrydowe) bez jednoznacznego definiowania. Oddziaływanie hybrydowe jak i terroryzm z perspektywy ich zwalczania tworzą zespół splątanych zagrożeń dla bezpieczeństwa państwa[2].

Wyróżnikiem zagrożeń hybrydowych jest umiejętnie stosowana przez przeciwnika (państwowego i niepaństwowego lub korelacji różnych podmiotów) mieszanka współczesnych broni, taktyk oraz innych działań, które mogą być stosowane równocześnie i wykazują wysokie zdolności adaptacyjne. Kombinacja środków politycznych, wojskowych, ekonomicznych, społecznych i informacyjnych wraz z wybraną metodą, np. walką konwencjonalną, nieregularną, dywersją, terroryzmem lub przestępczością zmierza do realizacji celów politycznych przez podmioty, które je stosują[3]. Warto nadmienić, że wspomniany terroryzm służyć może w całokształcie oddziaływania hybrydowego jako narzędzie, a nie tylko jako taktyka. Pojawiają się głosy w debacie naukowej, że terroryzm obok dyplomacji jest najważniejszym składnikiem zagrożeń hybrydowych[4].

Agresor oddziałujący hybrydowo na innych aktorów posiada pełną zdolność do elastycznej integracji militarnych i pozamilitarnych środków, zdobywając przewagę poprzez skoordynowane działania w wielu sektorach. Generowanie zagrożeń hybrydowych jest często zamaskowane, nieukazujące pełnych intencji jego autora, w tym struktur organizacyjnych, zaangażowanych w całe spektrum działań przeciwko konkretnemu podmiotowi, jakim jest najczęściej państwo lub koalicja państw. Celem pośrednim oddziaływania jest władza państwowa, bezpośrednim m.in. społeczności lokalne, obywatele, miejsca użyteczności publicznej, a także cele symboliczne. Głównymi „atraktorami" (wspomniane cele bezpośrednie) – podobnie jak w przypadku zagrożeń o charakterze terrorystycznym – pozostaje ludność cywilna, a w tym istotna dla jej witalnych funkcji – infrastruktura krytyczna (IK). Zagrożenia hybrydowe generowane poniżej progu ataku zbrojnego mogą tworzyć kaskadowe sytuacje kryzysowe, których rezultatem będzie oczekiwana przez przeciwnika zmiana polityczna. Krajowe dysfunkcje systemu przeciwdziałania zagrożeniom hybrydowym mogą przyczyniać się do eskalacji zaistniałego kryzysu poza granicami państwa.

Kluczowym wydają się działania nakierowane na sektor społeczny, gdzie za pomocą komponentu konfliktu hybrydowego jakim jest walka informacyjna, wpływa się psychologicznie na daną społeczność w celu m.in:

- wzmacniania wewnętrznych podziałów,
- rozpowszechniania fałszywych informacji (np. o szczepionkach, szkodliwości technologii 5G) ,
- przekierowania uwagi opinii publicznej na tematy społecznie kontrowersyjne,
- wzmacniania lokalnych nacjonalizmów,
- zaostrzania konfliktu między wsią a miastem,
- generowania i wzmacniania regionalnej rywalizacji,
- hiperbolizowania narracji historycznej w sposób niezgodny z faktami, w celu zahamowania procesu pojednania między sąsiednimi krajami,

[1] Zob. szerzej: I. Arreguín-Toft, *International How the Weak Win Wars: A Theory of Asymmetric Conflict*, ,,International Security", Vol. 26, No. 1 (lato 2001), s. 93-128; A. Mack, *Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflict*, ,,World Politics", Vol. 27, No. 2 (styczeń 1975), s. 175-200.

[2] A. Gasztold, P. Gasztold, *The Polish Counterterrorism System and Hybrid Warfare Threats*, ,,Terrorism and Political Violence" online: czerwiec 25, 2020.

[3] B. Balczerowicz, *Zagrożenie hybrodowe*, w: *Encyklopedia Bezpieczeństwa Wewnętrznego*, red. A. Misiuk, J. Itrich-Drabarek, M. Dobrorowolska-Opała, Dom Wydawniczy Elipsa, Warszawa 2021 s. 295. Por. F.G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars*, Potomac Institute for Policy Studies, Arlington, TX: 2007.

[4] Zob. szerzej: R. Youssef, *State Support of Terrorist Organizations As a Potential Means of HybridTthreat Projection*, w: *Networked Insecurity – Hybrid Threats in the 21st Century*, red. A, Dengg, M. Schurian, Federal Ministry of Defence and Sports Vienna: 2016.

- promowania agentów wpływu w przestrzeni medialnej,
- utrudniania zdolności decyzyjnych na różnych szczeblach życia społecznego,
- podważania zaufania do instytucji publicznych,
- paraliżowania funkcjonowania administracji państwowej i lokalnej w sytuacji kryzysowej (dezinformowanie obywateli w sytuacji trwającego ataku terrorystycznego, czy awarii technicznej obiektu przemysłowego).

Powyższy katalog wyraźnie ukazuje istotną rolę krajowych systemów bezpieczeństwa w rozpoznaniu tego typu aktywności. Najbardziej widocznymi działaniami w obszarze informacji są: czarna propaganda, dezinformacja, sponsoring mediów ekstremistycznych, kampanie w mediach społecznościowych, itp. Ze względu na zakres działań w cyberprzestrzeni i kreatywność podmiotów odpowiedzialnych za intencjonalne wywoływanie kryzysów, możliwości oddziaływania są nieograniczone. Nieujawnione i nieprzypisane aktywa służące do osłabienia przeciwnika wychodzą daleko poza elementy działań informacyjnych. Instrumenty użyte będą zależały od rozpoznanych luk w systemie, skali wrażliwości społecznej i odporności oraz potencjalnego efektu oddziaływania.

Ważną kwestią w budowaniu odporności państwa na działania mające naturę zagrożeń hybrydowych jest stabilność polityczna, ekonomiczna i społeczna państwa, a przede wszystkim zdolność systemu bezpieczeństwa do rozpoznania zagrożeń, przeciwnika i możliwość podjęcia przez zagrożone państwo działań prewencyjnych. Mylnie zakłada się, że obszary w których państwo ma przewagę strategiczną są zazwyczaj pomijane w oddziaływaniu hybrydowym. Błąd ten wynika z zaufania do statystyk, podejrzliwości w stosunku do nietuzinkowych prognoz i analiz oraz entuzjastycznej wiary w dotychczas przyjęte rozwiązania systemowe.

Zainteresowanie państwa w „zabezpieczanie" infrastruktury krytycznej jest przejawem sekurytyzacji, czyli przechodzenia wyzwań dla kategorii zagrożeń i konieczności ich eliminacji (lub złagodzenia ich skutków)[5]. Postępujący, politycznie uzasadniany, proces sekurytyzacji wiąże ze sobą trzy wzajemnie powiązane kryteria: 1) wspominaną kwestię bezpieczeństwa, a właściwie eksponowanie egzystencjalnych zagrożeń dla niego; 2) stosowanie środków nadzwyczajnych; 3) przekroczenie codziennych norm i rutyn[6]. Bardziej odnosi się do wyobrażenia oddziaływania potencjalnego agresora i ma budować wspólnotę, niż wzmacniać system zapobiegania. Środki nadzwyczajne, w imię bezpieczeństwa, koncentrują się na wybranym problemie, często upolitycznianym, bez całościowego rozpoznania wszystkich możliwych zagrożeń i scenariuszy ich rozwoju. Zagrożenia ewoluują, natomiast oceniane są przez pryzmat istniejących rozwiązań systemowych i kultury strategicznej, co wpływa na obniżenie efektywności w ich zwalczaniu. Podejście instytucjonalne jest dominujące.

Najczęściej rekomendowaną strategią przeciwdziałania zagrożeniom hybrydowym jest wzmacnianie zdolności obronnych społeczeństwa[7]. Podobnie jak w przypadku zagrożeń o charakterze terrorystycznym, edukacja na rzecz bezpieczeństwa winna być elementem budowania odporności i służyć odstraszaniu. **Ukierunkowane kampanie i inicjatywy społeczne mogłyby wzmocnić zdolność społeczeństwa do wytrzymywania presji, rozpoznania manipulacji i przetrwania kryzysów wywołanych przez oddziaływanie hybrydowe. Gotowość cywilna to fundamentalna kwestia w kształtowaniu odporności IK**[8]. Aktorzy prywatni stanowią pierwszą linię prewencji, choć odporność cywilna jest niewystarczającym elementem bez adaptacyjnej ochrony infrastruktury krytycznej. Nieustanne szacowanie ryzyka pozostaje w dalszym ciągu działaniem kluczowym. Wyzwaniem pozostaje stworzenie takiego systemu monitorowania zagrożeń, który w sposób ciągły i holistyczny nadzorowałby poziom odporności systemów bezpieczeństwa oraz ochronę obiektów, w tym obiektów budowlanych, urządzeń, instalacji usług newralgicznych dla bezpieczeństwa państwa i jego obywateli[9].

[5] Zob. R. Zięba, *Teoria bezpieczeństwa*, w: *Teorie i podejścia badawcze w nauce o stosunkach międzynarodowych* red. R. Zięba, S. Bieleń, J. Zając, WDiNP UW: Warszawa 2015, s. 94-95.

[6] B. Buzan, O. Waever, J. de Wilde, *Security: A New Framework For Analysis*, London: Renner 1998.

[7] Zob. A. Cederberg, P. Eronen, *How Can Societies Be Defended Against Hybrid Threats*, ,,Strategic Security Analysis", No. 9, wrzesień 2015.

[8] Gotowość cywilna to szczególny rodzaj gotowości „używanym do określania stanu zdolności sektora cywilnego do wypełnienia warunków podjęcia i realizacji zadań ciążących na tym sektorze w każdym ze stanów, czasu pokoju, kryzysu i okresu wojny. Podkreśla się czas pokoju, jako że gotowość cywilną sprowadzono przede wszystkim do tego stanu, mając na uwadze bezpieczeństwo ludności." za: R. Kalinowski, *Od gotowości cywilnej do zarządzania kryzysowego*, „Przegląd Naukowo-Medyczny. Edukacja dla Bezpieczeństwa" 2013, nr 4, s. 98.

[9] Systemy infrastruktury krytycznej – Rządowe Centrum Bezpieczeństwa – Portal Gov.pl (www.gov.pl)

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

W oddziaływaniu zagrożeń hybrydowych można wyróżnić dwie fazy: przygotowawczą i operacyjną[10]. Pierwsza faza dotyczy rozpoznania uwarunkowań, systemu, przestrzeni, interakcji i napięć w systemie politycznym i społecznym oraz stopniowego zakotwiczania quasi-legalnych i subtelnych środków oddziaływania, jak np. stowarzyszenia, fundacje, aktywność w mediach społecznościowych, popularyzacja – właściwie absorpcja – określonej wiedzy opartej na zbiorze zdań prawdziwych i fałszywych o rzeczywistości. W dalszej kolejności zaczyna się realizacja założeń „projektu hybrydowego" poprzez dotkliwsze oddziaływanie. Szczególnie istotne jest zrozumienie wrażliwości na tego typu ataki wobec infrastruktury krytycznej. **Współzależność fizycznych i informacyjnych aktywów IK i potencjalne skutki zakłóceń sprawiają, że jest to priorytetowa strefa zapewniania bezpieczeństwa.** Rozpoznanie asymetrii między słabymi stronami celu a siłą aktora hybrydowego określa strefę oddziaływania[11]. Kryterium istotności krajowej jest dominujące w tworzeniu niepublicznego katalogu obiektów i systemów podlegających ochronie, krytyczność jest funkcją skali, a w tym częściowo określana jest poprzez zapotrzebowanie społeczeństwa.

Analizując problem zagrożeń hybrydowych dla obiektów i systemów składających się na infrastrukturę krytyczną należy postawić kilka pytań[12]:

- Co to znaczy, że coś jest krytyczne (właściwe kluczowe, istotne)? To pytanie wiąże się z poszukiwaniem znaczenia i oddziaływania dla systemu społecznego i politycznego, ale także i ekonomicznego danego obiektu. Czyli upraszczając: jakie skutki wywoła wyłączenie, uszkodzenie lub sparaliżowanie danego podmiotu.
- Dla kogo jest problem kluczowy? To pytanie pomoże operatorom jak i instytucjom zaangażowanym w zapewnianie bezpieczeństwa zrozumieć jego witalne znaczenie dla całokształtu użytkowników cywilnych oraz nie-cywilnych jaki i wszystkich użytkowników systemu.
- Jaki jest zasięg krytyczności? Czy negatywne oddziaływanie hybrydowe na dany podmiot wywoła skutki na poziomie lokalnych, państwowym, regionalnym czy globalnym?
- Kiedy obiekt/system jest krytyczny? Wykrywanie zależności między np. porą roku, potrzebami społecznymi, zależnością od technologii itd.

Postawione wyżej pytania wyraźnie ukazują znaczenie i rolę aktorów cywilnych w kształtowaniu odporności na zagrożenia hybrydowe. Zadania skoncentrowane na ich wykrywaniu i reagowaniu realizowane są przez instytucje państwowe (głównie Rządowe Centrum Bezpieczeństwa, Agencję Bezpieczeństwa Wewnętrznego, Policję i Żandarmerię Wojskową), ale w eliminowaniu pomocne jest wyedukowane społeczeństwo. Podejście społeczne wykorzystywane jest w krajowych systemach przeciwdziałania zagrożeniom o charakterze hybrydowym i terrorystycznym między innymi w Finlandii i Holandii[13]. Perspektywa instytucjonalna i regulacyjna jest niewystarczająca szczególnie w kontekście oddziaływania hybrydowego w sferze informacyjnej. Cel postawiony w polskiej strategii Bezpieczeństwa Narodowego z 2020 jakim jest wdrożenie modelu ochrony infrastruktury krytycznej, polegającego na zapewnieniu jej ciągłości działania oraz świadczonych przez nią usług[14] winien uwzględnić kształtowanie odporności społecznej w dobie współczesnych zagrożeń. **Tylko społeczeństwo dysponujące rzetelną wiedzą o zagrożeniach może być na nie odporne i właściwie reagować. Zadanie to powinno zostać ustawowo przypisane tej instytucji państwowej, która dysponuje w tym obszarze największym zasobem kadrowym, organizacyjnym i posiada już niezbędne uprawnienia do reagowania w sytuacjach kryzysowych, czy budowaniu odporności społecznej na zagrożenia. Istnieje konieczność wyboru krajowego lidera ochrony IK przed zagrożeniami hybrydowymi. Czas na dyskusję już minął.**

[10] Por. Hybrid threats as a concept – Hybrid CoE – The European Centre of Excellence for Countering Hybrid Threats (05.07.2021).

[11] Zob. F. Bekkers, R. Meessen, D. Lassche, *Hybrid Conflicts: The New Normal?*, The Hague Center for Strategic Studies, December 2018, s. 7-8, źródło: Hybrid-conflicts.-The-New-Normal-HCSS-TNO-1901-_0.pdf (05.07.2021).

[12] Por. W. Steele, K. Hussey, S. Dovers, *What's Critical about Critical Infrastructure?*, ,,Urban Policy and Research" 2017, vol. 35, nr 1, s. 74-86.

[13] Zob. szerzej: K. Wijnja, *Countering hybrid threats: does strategic culture matter?*, ,,ADefence Studies" online: 26 czerwca 2021.

[14] *Strategia Bezpieczeństwa Narodowego Rzeczpospolitej Polskiej 2020*, BBN, Warszawa 2020, pkt. 2.8.

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

Edukacja antyterrorystyczna a kultura bezpieczeństwa. Nowa platforma e-learningowa Centrum Prewencji Terrorystycznej Agencji Bezpieczeństwa Wewnętrznego

Barbara Wiśniewska-Paź

Centrum Studiów i Edukacji na rzecz Bezpieczeństwa Uniwersytetu Wrocławskiego

„Oczekiwanie na niebezpieczeństwo jest gorsze niż moment, gdy ono na człowieka spada. Wielu ludzi zna fakty […] a nie potrafi ich należycie połączyć. Poznanie faktów to tylko połowa pracy." (A. Hitchcock)

Cytat, który rozpoczyna artykuł to dość sugestywna i tylko pozornie abstrakcyjna obszarowo myśl, którą co jakiś czas zdarza mi się przywoływać, zwłaszcza przy podejmowaniu wątków dotyczących społecznych i edukacyjnych kontekstów bezpieczeństwa zarówno personalnego, jak i strukturalnego oraz towarzyszących im wzajemnych korelacji i koegzystencji trzech obszarów – społeczeństwa, bezpieczeństwa i edukacji[1], w tym funkcjonujących w ich ramach problemów. Uważam bowiem, że w bardzo obrazowy i syntetyczny sposób wprowadza czytelnika w „przestrzeń myślenia", tłumaczy sens i konieczność podejmowania działań prewencyjnych w obliczu obecnych i przyszłych zagrożeń (o których będzie mowa w tym artykule) oraz cel powoływania do tego rodzaju zadań instytucji inicjujących i koordynujących pożądane działania i procesy w tym zakresie.

BUDOWA ŚWIADOMOŚCI ANTYTERRORYSTYCZNEJ

Centrum Prewencji Terrorystycznej jest jednostką Agencji Bezpieczeństwa Wewnętrznego, która powstała trzy lata temu (w 2018 roku)[2] w celu wzmocnienia ochrony antyterrorystycznej naszego kraju oraz pozycji Polski w budowaniu bezpieczeństwa ze szczególnym naciskiem położonym na obszar Europy Środkowo-Wschodniej we współpracy z partnerami strategicznymi – państwami wchodzącymi w skład Inicjatywy Trójmorza[3]. Misją tej instytucji jest kształtowanie kultury bezpieczeństwa poprzez proces budowania świadomości antyterrorystycznej w społeczeństwie. Prewencja i edukacja stanowią zatem bazę funkcjonowania tej jednostki. Do zadań Centrum należy m.in. opracowywanie programów szkoleniowych i prowadzenie szkoleń z zakresu prewencji terrorystycznej, tworzenie sprofilowanych rekomendacji, opracowywanie materiałów informacyjnych, organizacja seminariów i warsztatów, prowadzenie współpracy z ekspertami krajowymi i zagranicznymi czy realizacja kampanii społecznych[4].

Mimo kilkuletniego okresu działania ma ono na swoim koncie kilka efektownych przedsięwzięć, wśród nich ogólnopolską kampanię społeczną "4U! – Uważaj! Uciekaj! Ukryj się! Udaremnij atak!"[5]. Celem akcji było dostarczenie wiedzy i zwiększenie świadomości społecznej w zakresie różnych typów zagrożeń i sytuacji niebezpiecznych (ze szczególnym naciskiem kładzionym na zagrożenia o charakterze terrorystycznym)[6], a także szerokie spektrum szkoleń z zakresu prewencji terrorystycznej (służby, kadry zarządcze, administracja publiczna instytucji) i bezpieczeństwa państwa w oparciu o innowacyjne programy, które wciąż są udoskonalane. Na uwagę zasługują również rekomendacje w zakresie profilaktyki w budynkach użyteczności publicznej szefa Agencji Bezpieczeństwa Wewnętrznego[7], poradnik prewencji terrorystycznej (zbiór wybranych rekomendacji, zaleceń i algorytmów zachowań w sytuacjach o charakterze terrorystycznym)[8] czy skorelowana z nim tematycznie platforma

[1] Por. B. Wiśniewska-Paź „Społeczne i edukacyjne konteksty bezpieczeństwa personalnego i strukturalnego. Wzajemne relacje, implikacje teoretyczne, wymiary praktyczne." Toruń 2019

[2] https://www.gov.pl/web/sluzby-specjalne/dwa-lata-centrum-prewencji-Terrorystycznej-abw https://tpcoe.gov.pl/cpt/wydarzenia/1796,CPT-ABW-ma-juz-3-lata.html

[3] Por. P. Kowal, A. Orzelska-Stączek "Inicjatywa Trójmorza: geneza, cele i funkcjonowanie /The Three Seas Initiative: origins, goals and functioning", ISP PAN, Warszawa 2019

[4] https://tpcoe.gov.pl/cpt/o-nas/1659,Centrum-Prewencji-Terrorystycznej-to-jednostka-Agencji-Bezpieczenstwa-Wewnetrzne.html

[5] https://4u.tpcoe.gov.pl

[6] Ibidem

[7] https://tpcoe.gov.pl/cpt/materialy/1649,Rekomendacje-w-zakresie-profilaktyki-antyterrorystycznej.html

[8] Por. „Poradnik prewencji terrorystycznej", Terrorism Prevention Centre of Excellence, Warszawa 2021

e-learningowa[9], o czym szerzej w dalszej części artykułu. W materiałach do pobrania na stronie można także znaleźć szereg przydatnych informacji na temat procesu radykalizacji, cyberbezpieczeństwa w kontekście niebezpieczeństw i zachowań, formularz przyjęcia informacji o zagrożeniu, czy zasad postępowania z niebezpieczną przesyłką[10]. Baza materiałów jest w trakcie tworzenia.

W końcu maja br. zostało podpisane porozumienie[11] pomiędzy Centrum Prewencji Terrorystycznej Agencji Bezpieczeństwa Wewnętrznego (www.tpcoe.gov.pl) a Centrum Studiów i Edukacji na rzecz Bezpieczeństwa Uniwersytetu Wrocławskiego (www.cseb.uni.wroc.pl) w zakresie współpracy naukowo-badawczej, projektowej, konferencyjno-seminaryjnej, szkoleniowej i eksperckiej. Oba centra są w trakcie wypracowywania najbliższych wspólnych przedsięwzięć projektowych, jednocześnie mając już na swoim koncie kilka przyczynkowych projektów. Sformalizowanie współpracy z pewnością przyczyni się do rozwinięcia bazy informacyjnej, projektowej, edukacyjnej i szkoleniowej w zakresie szeroko rozumianego bezpieczeństwa i kultury bezpieczeństwa, w tym edukacji i prewencji antyterrorystycznej. Cele działania obu centrów są spójne, odmienne są natomiast zakresy ich działania i *background* – w przypadku CSEB UWr – uniwersytecki, w przypadku CPT ABW – rządowy, co stanowi wartościową podstawę do uzupełniania się obu obszarów kompetencji w przedmiocie wspólnych działań.

EDUKACJA ANTYTERRORYSTYCZNA

Terroryzm jest aktualnie jednym z największych globalnych wyzwań, które obejmuje swoim zasięgiem bardzo szerokie spektrum zagrożeń dla współczesnego świata[12]. Mają one różny rozkład, typologie, przyczyny i ośrodki oddziaływania. Niebezpieczeństwa z nim związane ewoluują i są stanem permanentnym, stąd możliwość całkowitego wyeliminowania występowania tego rodzaju form zagrożeń jest praktycznie niemożliwa, zaś zakładanie w teorii takich scenariuszy najczęściej jest traktowane jako fikcja. Terroryzm stał się zatem stałym elementem rzeczywistości, z którym trzeba nauczyć się żyć, umieć interpretować otoczenie (symptomy, niepokojące sygnały), chronić siebie, innych i adekwatnie do sytuacji reagować. Ważna jest wiedza nie tylko na temat potencjału zagrożeń we własnym kraju, ale także innych państwach, zwłaszcza ościennych. Każdy powinien wiedzieć, gdzie szukać potrzebnych informacji przed wyjazdem, zwłaszcza do kraju innej strefy kulturowej[13]. To co jest konieczne do wypracowania tego rodzaju zachowań w przestrzeni społecznej to z jednej strony aktywność instytucji rządowych i organizacji międzynarodowych zmierzających do minimalizacji zagrożeń[14], z drugiej przygotowanie i wdrożenie koncepcji permanentnego procesu budowy, wsparcia i rozwoju kultury bezpieczeństwa adresowanej do różnych grup i kategorii społecznych. Głównie poprzez edukację realizowaną systemowo[15], która dostarczy szeroki wachlarz kompetencji w zakresie wiedzy (i konieczności jej stałego aktualizowania) oraz umiejętności praktycznych (zastosowania teorii w praktyce w sposób adekwatny do sytuacji). Ten aspekt jest wciąż marginalizowany lub realizowany fragmentarycznie. Wiele się o kulturze bezpieczeństwa mówi, widzi potrzebę jej istnienia, ale niewiele robi w tym kierunku.[16] Jeśli zaś już coś się w tym aspekcie zaczyna robić, to jest to wciąż za słabe jakościowo w stosunku do funkcji, które ma pełnić. Realizowane jest często w wąskim zakresie i okazyjnie bez

[9] https://tpcoe.gov.pl/cpt/wydarzenia/1807,CPT-ABW-otwiera-portal-e-learningowy.html

[10] https://tpcoe.gov.pl/cpt/materialy

[11] https://tpcoe.gov.pl/cpt/wydarzenia/1826,CPT-ABW-nawiazuje-wspolprace-z-Uniwersytetem-Wroclawskim.html; https://www.cseb.uni.wroc.pl/Aktualnosci/Porozumienie-o-wspolpracy-pomiedzy-Centrum-Studiow-i-Edukacji-na-rzecz-Bezpieczenstwa-UWr-oraz-Centrum-Prewencji-Terrorystycznej-Agencji-Bezpieczenstwa-Wewnetrznego-w-Warszawie

[12] Por. T. Aleksandrowicz „Kierunki zagrożeń terrorystycznych w pierwszej połowie XXI wieku. Próba prognozy" [w:] "Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej. Terroryzm – Strategie zwalczania – Edukacja antyterrorystyczna" t. I, red. B. Wiśniewska-Paź, J. Stelmach, Warszawa 2021, s.13-29.

[13] Por. B. Wiśniewska-Paź „Edukacja antyterrorystyczna – cele, strategie, aspekty wdrożeniowe" [w:] "Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej. Terroryzm – Strategie zwalczania – Edukacja antyterrorystyczna" t.I, red. B. Wiśniewska-Paź, J. Stelmach, Warszawa 2021,s.266-292.

[14] Por. B. Wiśniewska-Paź „Międzynarodowe struktury i instytucje zajmujące się zwalczaniem terroryzmu na świecie" [w:] "Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej. Terroryzm – Strategie zwalczania – Edukacja antyterrorystyczna" t. I, red. B. Wiśniewska-Paź, J. Stelmach, Warszawa 2021, s.80-97.

[15] Por. „Perspektywa systemowa" [w:] B. Wiśniewska-Paź „Społeczne i edukacyjne konteksty bezpieczeństwa personalnego i strukturalnego. Wzajemne relacje, implikacje teoretyczne, wymiary praktyczne." Toruń 2019, s.51-74.

[16] Por. „Kultura bezpieczeństwa – rola i znaczenie" [w:] B. Wiśniewska-Paź „Społeczne i edukacyjne konteksty bezpieczeństwa personalnego i strukturalnego. Wzajemne relacje, implikacje teoretyczne, wymiary praktyczne." Toruń 2019, s.171-178; por. także „Edukacja dla bezpieczeństwa. O kształtowaniu kultury bezpieczeństwa", red. A Skrabacz, K. Loranty, L. Konarski", Warszawa 2015.

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

wypracowanej koncepcji oddziaływania systemowego wraz z towarzyszącym temu przedsięwzięciu i prowadzonym w procesie ciągłym *outsourcingiem* badawczym (mapowanie zagrożeń, rekomendacje) oraz wdrożeniowym (wypracowywanie strategii, koncepcji edukacyjnych, wdrażanie ich, ewaluacja i aktualizowanie).

Kluczem do osiągniecia pożądanych efektów jest po pierwsze, permanentny charakter działań i procesów, po drugie, podejście holistyczne (kompleksowe) i systemowe (synergia teorii i praktyki, analiz i działań wdrożeniowych), po trzecie, przywiązywanie szczególnej dbałości do jakość koncepcji, działań i procesów[17]. Główne cele polityki antyterrorystycznej państwa są zawarte w Narodowym Programie Antyterrorystycznym na lata 2015-2019[18], który do dziś jest podstawowym dokumentem programowym dotyczącym zwalczania terroryzmu w Polsce. Jest w nim wskazana konieczność wzmocnienia polityki informacyjnej i edukacyjnej poprzez wypracowanie mechanizmów współpracy między różnymi instytucjami (m.in. administracji publicznej i mediami) w celu zainicjowania i wdrożenia wymiany informacji i ich przekazu społeczeństwu w kwestiach dotyczących sytuacji pośredniego lub bezpośredniego zagrożenia terrorystycznego, a także prowadzenia działalności profilaktycznej (w tym edukacyjnej).

Złożona struktura zjawisk o charakterze terrorystycznym implikuje konieczność realizowania procesu edukacji antyterrorystycznej w dwóch wspomnianych wymiarach: poznawczym (związanym z wiedzą na temat zagrożeń, ich symptomach i konsekwencjach) oraz praktycznym (związanym z kształtowaniem postaw i zachowań adekwatnych do sytuacji zagrożenia). Obu obszarów w żadnym wypadku nie należy traktować rozłącznie, podobnie jak do edukacji danej społeczności w ramach konkretnej instytucji nie powinno się podchodzić w sposób fragmentaryczny i ograniczać wyłącznie do szkolenia tylko np. kadry zarządczej lub wąskiej grupy/działu odpowiedzialnego za bezpieczeństwo danej instytucji[19]. Ważne jest również dostosowanie form i metod przekazu wiedzy oraz umiejętności praktycznych do grupy potencjalnych odbiorców z uwzględnieniem m.in. ich wieku, wykształcenia i innych zmiennych, nie tylko metryczkowych.

PLATFORMA E-LEARNINGOWA

Jednym z obiecujących kroków na tej drodze jest przygotowana przez Centrum Prewencji Terrorystycznej platforma e-learningowa[20], którą miałam okazję się bliżej poznać robiąc przy okazji wstępny projekt struktury narzędzia ewaluacyjnego, który docelowo będzie służył m.in. budowie rekomendacji dotyczących cyklicznej aktualizacji treści zamieszczonych na platformie i uzupełniania ich o aktualnie obowiązujące w postaci osobnych komponentów szkoleniowych i edukacyjnych. Świat nie stoi w miejscu. To co dziś jest zakresowo wystarczające, jutro może wymagać uzupełnienia lub zmiany. Platforma ruszyła na początku maja br.[21], jest współfinansowana ze środków Europejskiego Funduszu Społecznego w projekcie „Podnoszenie kompetencji służb bezpieczeństwa państwa, pracowników administracji publicznej i ośrodków naukowo-badawczych oraz rozwój ich współpracy w obszarze bezpieczeństwa narodowego" w ramach Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020[22].

Biorąc pod uwagę obecną sytuację związaną z pandemią i preferowanie od ponad półtora roku edukacji zdalnej przygotowana platforma jest bardzo profesjonalnym i rozwojowym narzędziem do przekazu podstawowej wiedzy w zakresie prewencji terrorystycznej. Obecnie z portalu e-learningowego korzystają przedstawiciele służb oraz kadra administracji publicznej. Udział w szkoleniu jest nieodpłatny, zgłaszany jest przez instytucje znajdujące się w grupie celowej zgodnie z zapotrzebowaniem przez osoby wyznaczone do kontaktów z Centrum (bliższe informacje dotyczące korzystania z platformy, wykaz instytucji z grupy celowej znajdują się na stronie portalu e-learningowego – www.learning.tpcoe.gov.pl). Na tej podstawie Centrum generuje indywidualne konta uczestnikom i przekazuje je zainteresowanym szkoleniem. W miesiąc od uruchomienia platformy z kursu skorzystało 12 tysięcy osób[23].

Kurs e-learningowy Centrum Prewencji Terrorystycznej ABW został przygotowany w oparciu

[17] Por. B. Wiśniewska-Paź „Społeczne i edukacyjne konteksty bezpieczeństwa personalnego i strukturalnego. Wzajemne relacje, implikacje teoretyczne, wymiary praktyczne." Toruń 2019.

[18] https://sip.lex.pl/akty-prawne/mp-monitor-polski/-narodowy-program-antyterrorystyczny-na-lata-2015-2019-18153802

[19] Por. B. Wiśniewska-Paź „Społeczne i edukacyjne konteksty bezpieczeństwa personalnego i strukturalnego. Wzajemne relacje, implikacje teoretyczne, wymiary praktyczne." Toruń 2019.

[20] https://learning.tpcoe.gov.pl

[21] https://tpcoe.gov.pl/cpt/wydarzenia/1807,CPT-ABW-otwiera-portal-e-learningowy.html

[22] Ibidem.

[23] https://tpcoe.gov.pl/cpt/wydarzenia/1837,12-tysiecy-uzytkownikow-portalu-e-learningowego-CPT-ABW.html

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

o wiedzę ekspercką funkcjonariuszy Centrum oraz wsparcie merytoryczne ze strony partnerskich służb specjalnych. Jego celem jest podniesienie świadomości w zakresie zagrożeń terrorystycznych służb i urzędników administracji publicznej.

Szkolenie składa się z pięciu modułów: **I. Radykalizacji, II. Rekomendowanych zachowań w przypadku zagrożenia o charakterze terrorystycznym**, **III. Ratownictwa IV. Cyberbezpieczeństwa** oraz **V. Komunikacji i Infrastruktury**.

W module **I. Radykalizacja,** w bardzo skondensowany sposób przedstawione są informacje czym jest radykalizacja oraz jak jej przeciwdziałać. W kolejnych odsłonach tego modułu użytkownik dowiaduje się jaka jest relacja między radykalizacją a terroryzmem, dlaczego ludzie się radykalizują (typologia przyczyn), jak rozpoznać radykalizację oraz jak jej przeciwdziałać.

W module **II. Rekomendowanie zachowania,** główne pytanie dotyczy sposobów reagowania w przypadku wystąpienia zdarzenia o charakterze terrorystycznym. W tym celu przedstawiona jest kolejno typologia zagrożeń, zasady postępowania w przypadku potencjalnie niebezpiecznego przedmiotu (np. pozostawionej walizki), podejrzanej przesyłki, ataku masowego zabójcy oraz sytuacji zakładniczej.

W module **III. Ratownictwo,** zostały przedstawione praktyczne porady udzielania pierwszej pomocy z zakresu BLS i podstaw TCCC. Można się dowiedzieć jak tamować krwawienie, prawidłowo zastosować opaskę uciskową, jak należy zabrać się za opatrywanie obrażeń klatki piersiowej, można również poszerzyć swój zakres wiedzy na temat rodzajów opatrunków i środków medycznych.

W module **IV. Cyberbezpieczeństwo** zostały zawarte tzw. dobre praktyki z korzystania z Internetu i szeroko rozumianej technologii, wyjaśnione czym jest cyberterroryzm i cyberprzestępczość, jakie są rodzaje ataków i oszustw, jakie są podstawowe zasady higieny pracy w Internecie, zaprezentowana została również specyfika wycieków danych i zasady udostępniania treści w sieci. Na zakończenie zostały przedstawione podstawy bezpiecznego korzystania z sieci Wi-Fi.

W ostatnim module **V. Komunikacja i Infrastruktura** użytkownik kursu ma możliwość zapoznać się z tym czym jest komunikacja strategiczna i jak ją prowadzić oraz jak przygotować się na potencjalne zagrożenie zanim nastąpi, w tym jak powinno wyglądać zabezpieczenie budynków, informacja o zagrożeniu, formy alarmowania oraz ewakuacja. W przypadku dwóch ostatnich kwestii – alarmowania i ewakuacji zostały przedstawione wciąż niestety aktualne problemy dotyczące alarmowania w instytucjach i różnice w zasadach ewakuacji w przypadku zagrożenia o charakterze terrorystycznym i innym zdarzeniu zagrażającym zdrowiu i życiu ludzi np. pożarze.[24]

Pakiet szkoleniowy zawiera 7 filmów oraz 40 animacji. Kurs jest interaktywny, co zdecydowanie podnosi poziom jego atrakcyjności oraz zachęca do przechodzenia kolejnych etapów. Każda część szkolenia kończy się testem. Popełniony błąd nie dyskwalifikuje uczestnika kursu, wręcz przeciwnie, system zachęca do powtórnego zastanowienia się w kwestii popełnionego błędu i finalnie udzielenia prawidłowej odpowiedzi. Kurs jest tak zaprojektowany, że do elementów wcześniejszych danego modułu można dowolną ilość razy wracać i w zależności od zapotrzebowania uzupełnić wiedzę. Grafika, czas oraz muzyka towarzysząca animacjom jest na bardzo profesjonalnym poziomie, dotyczy to zastosowanej kolorystyki, długości trwania animacji oraz wzmacniania akcentów, które powinny zostać zapamiętane.

Podobną rolę spełniają filmy i koncepcja ich przedstawiania, trochę na zasadzie puzzli, które w finalnym przekazie przedstawiają całą „układankę". Myślę, że w zależności od odbiorcy, na niektórych bardziej sugestywnie będą oddziaływać animacje, na innych filmy. Docelowo obie formy mają się w mojej ocenie uzupełniać i wzmacniać tym samym odbiór przekazywanych treści. Jak kurs będzie oceniony przez osoby, które go przeszły, dowiemy się niebawem. W tym celu przygotowywane są narzędzia badawcze (ewaluacyjne). To przedsięwzięcie jest w najbliższych planach do zrealizowania przez oba centra – CSEB UWr i CPT ABW.

Na portalu e-learningowym Centrum Prewencji Terrorystycznej znajdują się również filmy edukacyjne, ostatnio udostępnione dotyczą modułu szkoleniowego z zakresu cyberbezpieczeństwa[25]. Po ukończeniu szkolenia oraz pozytywnym rozwiązaniu testu uczestnik otrzymuje certyfikat.

[24] https://tpcoe.gov.pl/cpt/wydarzenia/1807,CPT-ABW-otwiera-portal-e-learningowy.html, https://learning.tpcoe.gov.pl

[25] https://tpcoe.gov.pl/cpt/materialy/1841,Cyberbezpieczenstwo.html?, fbclid=IwAR3u3yjMWsaw0vUVGsaTB5cwhCsdxsl_gQLGZlUn1Fpux7zykM3FjSEnL5w

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

PORADNIK PREWENCJI TERRORYSTYCZNEJ

W kontekście platformy e-learningowej CPT ABW na uwagę zasługuje także wydany w tym roku i uzupełniający merytorycznie kurs e-learningowy „Poradnik prewencji terrorystycznej”[26] przez tę samą instytucję (CPT ABW). Można z niego skorzystać przed przejściem kursu, będzie wówczas z pewnością łatwiejszy do zrozumienia i rozwiązania pośrednich testów. Poradnik zawiera wszystkie moduły, które są ujęte w kursie e-learningowym w postaci rozszerzonej, przedstawione w równie efektowy graficznie i syntetyczny sposób, który zachęca do przejrzenia, bliższego zapoznania się z wybranymi fragmentami lub całą książką. Co ważne, nie ma w nim informacji nieistotnych. Obie pomoce edukacyjne, kurs i poradnik, są tak pomyślane, że można z nich korzystać w dowolnej kolejności, w uzupełnieniu lub niezależnie od siebie. W założeniu pomysłodawców poradnik pełni rolę uzupełniającą wobec kursu i póki co nie wchodzi w skład pakietu szkoleniowego, choć są plany aby go włączyć.

Do poradnika dołączona jest zakładka z przedstawieniem idei i etapami kampanii społecznej 4U. Do każdego z etapów załączony jest osobny kod QR, po zeskanowaniu którego można przejść do pakietów informacyjnych i animacji na platformie CPT ABW.

Dotychczasowe działania podjęte przez Centrum Prewencji Terrorystycznej ABW uważam za doskonałe preludium do kolejnych etapów zmierzających przede wszystkim do podejmowania wyzwań i celów o charakterze systemowym, ewaluacji dotychczasowych narzędzi, pomocy dydaktycznych i kursów, aktualizowania i rozszerzania pakietów informacyjnych i edukacyjnych oraz mapowania specyfiki zagrożeń w określonych środowiskach w celu przygotowywania rekomendacji i na ich podstawie rozszerzonych pakietów informacyjno-szkoleniowych dopełnianych warsztatami praktycznymi.

Renegade/Sarex-21

Dowództwo Operacyjne Rodzajów Sił Zbrojnych

W dniach 17-21 maja 2021 r. zostało przeprowadzone ćwiczenie taktyczno-specjalne pk. Renegade/Sarex-21 z zakresu przeciwdziałania zagrożeniom terrorystycznym z powietrza oraz prowadzenia akcji poszukiwawczo-ratowniczych w obszarze lądowym i morskim.

W trakcie ćwiczenia przeprowadzone zostały cztery epizody. Pierwszy dotyczył uprowadzenia cywilnego statku powietrznego, jako możliwego środka ataku o charakterze terrorystycznym, stanowiącego zagrożenie dla bezpieczeństwa państwa.

RENEGADE

Lotniczy epizod ćwiczenia Renegade/Sarex-21 zakładał, że terroryści uprowadzili cywilny statek powietrzny, który stanowił zagrożenie dla bezpieczeństwa kraju.

Cywilny statek powietrzny wykonywał planowy lot nad terytorium Polski. Niespodziewanie zmienił trasę. 3 minuty po starcie nastąpiła nagła utrata łączności, a na transponderze samolotu został uruchomiony kod alarmowy. Polska Agencja Żeglugi Powietrznej przekazała natychmiastowy sygnał do Centrum Operacji Powietrznych-Dowództwa Komponentu Powietrznego o zagrożeniu w polskiej przestrzeni powietrznej. Uruchomione zostały procedury przeciwdziałania zagrożeniom terrorystycznym w powietrzu, podjęto decyzję o działaniu lotniczych sił i środków systemu Obrony Powietrznej oraz aktywacji wojskowych lotnisk interwencyjnych. Uruchomiono również system powszechnego ostrzegania i alarmowania o zagrożeniach z powietrza. Użyto syren alarmowych. Dźwięk alarmu słychać było w większych miastach na trasie przelotu porwanego statku powietrznego.

Aktywowana została narodowa para dyżurna samolotów F-16, której zadaniem było rozpoznanie i przechwycenie uprowadzonego statku powietrznego oraz doprowadzenie do lądowania na lotnisku interwencyjnym. Terroryści zdecydowali się na lądowanie w Świdwinie.

W międzyczasie nastąpiła również aktywacja i przemieszczenie na pokładzie C-130 Hercules żołnierzy Oddziału Specjalnego Żandarmerii Wojskowej, przygotowanych do prowadzenia działań kontrterrorystycznych.

[26] „Poradnik prewencji terrorystycznej”, Terrorism Prevention Centre of Excellence, Warszawa 2021

W wyniku przeprowadzonych negocjacji zatrzymano terrorystów, zneutralizowano zagrożenie i przystąpiono do działań dochodzeniowo-śledczych. Nie zabrakło również przećwiczenia procedur kontroli pasażerów, niebędących obywatelami UE znajdujących się na statku powietrznym.

W pasażerów wcielili się podchorążowie Akademii Wojsk Lądowych, natomiast w porywaczy żołnierze Żandarmerii Wojskowej. Cywilny statek powietrzny podgrywał samolot Boeing 737 z 1 Bazy Lotnictwa Transportowego. Natomiast narodową parę dyżurną w składzie dwóch samolotów F-16 wystawiła 31 Baza Lotnictwa Taktycznego. Ponadto, w epizodzie wzięli udział przedstawiciele Straży Granicznej i Policji.

Drugim z epizodów była operacja masowej ewakuacji (ang. MASSEVAC), w związku z kolizją dwóch okrętów z poszkodowanymi osobami na płonących i tonących jednostkach.

MASOWA EWAKUACJA

Morski epizod ćwiczenia Renegade/Sarex-21 zakładał, że na Bałtyku, w rejonie Łeby doszło do kolizji dwóch okrętów, a w jej wyniku, między innymi do rozerwania poszycia poniżej linii wody i pożaru.

Część poszkodowanych członków załóg znalazła się w wodzie, a jednostki zdryfowały na mieliznę. Służby ratownicze, po otrzymaniu sygnału o zdarzeniu, przystąpiły do działania zgodnie z procedurami. Poszkodowani zostali ewakuowani przez śmigłowce ratownicze Lotniczych Zespołów Poszukiwawczo-Ratowniczych z Gdyni i Darłowa, wydzielanych z Brygady Lotnictwa Marynarki Wojennej i jednostki pływające Morskiej Służby Poszukiwania i Ratownictwa i okręty Marynarki Wojennej, wydzielane z 3. Flotylli Okrętów. Rozbitkowie wymagający natychmiastowej hospitalizacji zostali przetransportowani drogą lotniczą bezpośrednio do 7 Szpitala Marynarki Wojennej w Gdańsku oraz Wojewódzkiego Szpitala Specjalistycznego w Słupsku. Pozostali poszkodowani zostali ewakuowani drogą powietrzną na lądowisko, stanowiące Punkt Przekazania i rejon koncentracji służb, oraz morską do portu w Łebie.

W akcji poszukiwania rozbitków i ich ewakuacji uczestniczyły: dyżurny okręt ratowniczy Marynarki Wojennej wraz z holownikiem, jednostki Morskiej Służby Poszukiwania i Ratownictwa, Morskiego Oddziału Straży Granicznej, a także samolot patrolowy z Brygady Lotnictwa Marynarki Wojennej. W ćwiczeniu uczestniczyli również żołnierze 7. Pomorskiej Brygady Obrony Terytorialnej, podchorążowie Akademii Marynarki Wojennej, Państwowa Straż Pożarna, Policja i służby medyczne. Osobnym elementem epizodu, prowadzonym po zakończeniu ewakuacji rozbitków, było ratowanie mienia, polegające na ściągnięciu jednostek z mielizny i odholowaniu do portu.

Na Bałtyku każdej doby przebywa od 2,5 do ponad 3 tysięcy jednostek, co sprawia, że akwen ten należy do jednych z najbardziej zatłoczonych na świecie. Konsekwencją tak intensywnego ruchu jest duże prawdopodobieństwo występowania incydentów zagrażających bezpieczeństwu użytkowników morza. Statystycznie, rocznie na Bałtyku dochodzi do około 120 różnego rodzaju wypadków. Stąd konieczność doskonalenia procedur i działania służb odpowiedzialnych za ratowanie zdrowia i życia na morzu w sytuacji wymuszającej przeprowadzenie tzw. masowej ewakuacji.

Kolejne dwa epizody związane były z przeprowadzeniem akcji poszukiwawczo-ratowniczych po zdarzeniach lotniczych (aplikacyjne rozbicie się statków powietrznych w terenach trudno dostępnych), mianowicie misja poszukiwawczo-ratownicza na obszarze lądowym oraz manewry ASAR.

MISJA POSZUKIWAWCZO-RATOWNICZA NA OBSZARZE LĄDOWYM

W trakcie realizacji lotu samolotu CASA C-295 dochodzi do sytuacji EMERGENCY w powietrzu, w wyniku której załoga samolotu zmuszona zostaje do podjęcia decyzji o awaryjnym lądowaniu w terenie przygodnym.

Dla celów ćwiczenia przyjęto, że część pasażerów opuściła statek powietrzny w powietrzu wykorzystując do ewakuacji posiadane na wyposażeniu spadochrony, jak również to, że w wyniku doznanych kontuzji po wylądowaniu nie byli w stanie się samodzielnie przemieszczać. W wyniku powyższego zdarzenia doszło również do pożaru w miejscu awaryjnego lądowania. Zadanie gaszenia pożaru z powietrza realizował również śmigłowiec Policji S-70 ze strażakami na pokładzie, przy wykorzystaniu zbiorników BAMBI BUCKET.

Służba ASAR, po otrzymaniu informacji o awaryjnym lądowaniu statku powietrznego, przystąpiła do działania zgodnie z obowiązującymi procedurami. W związku z tym, iż do zdarzenia doszło w terenie trudno dostępnym, z gęstym zalesieniem, z dużą ilością zbiorników wodnych, jak również przy założeniu, że działania poszukiwawcze trzeba będzie

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

realizować na bardzo dużym obszarze, do działań poszukiwawczo-ratowniczych na terenie należącym do nadleśnictwa Złocieniec zostało skierowanych szereg służb dedykowanych do realizacji zadań w ramach służby ASAR, jak również ją wspomagających.

Ze względu na specyfikę terenu, jak również rozległy obszar, poszukiwania rozbitków prowadzone były przez śmigłowiec ratowniczy Lotniczego Zespołu Poszukiwawczo-Ratowniczego (LZPR) ze Świdwina, statki powietrzne Straży Granicznej oraz Policji, jak również naziemne zespoły poszukiwawcze wydzielone z: Państwowej Straży Pożarnej i Ochotniczej Straży Pożarnej, Policji, 12. Wielkopolskiej i 14 Zachodniopomorskiej Brygady Obrony Terytorialnej, Polskiego Czerwonego Krzyża, OSP Wołczkowo oraz Stowarzyszenia Szukamy i Ratujemy. Działania trwały kilkanaście godzin.

Poszkodowani rozbitkowie wymagający hospitalizacji zostali przetransportowani drogą lotniczą przez śmigłowiec ratowniczy LZPR bezpośrednio do 107. Szpitala Wojskowego w Wałczu.

W związku z bardzo dużą liczbą operacji lotniczych realizowanych nad obszarem lądowym w FIR WARSZAWA, należy liczyć się z prawdopodobieństwem wystąpienia sytuacji, w której zagrożone będzie bezpieczeństwo załóg i pasażerów statków powietrznych wykonujących lot w naszej przestrzeni powietrznej. W celu odpowiedniego przygotowania się do powyższych sytuacji, istnieje konieczność doskonalenia procedur i działania służby ASAR oraz służb z nią współdziałających w realizacji wspólnych przedsięwzięć, mających na celu ratowanie zdrowia i życia ludzkiego.

MANEWRY ASAR

Zgodnie ze scenariuszem czwartego epizodu nastąpiło zdarzenie lotnicze, związane z aplikacyjnym rozbiciem się cywilnego statku powietrznego CESNA-172 z dwoma osobami na pokładzie, w terenie zalesionym, w rejonie Poligonu Jagodne.

Cztery Lotnicze Zespoły Poszukiwawczo-Ratownicze służby ASAR, pełniące doraźne dyżury na lotnisku w Mińsku Mazowiecki, wydzielone z 3SLTr, 25BKPow, BLMW i Lotnictwa Policji realizowały misję poszukiwawczo-ratowniczą z separacją czasową ich aktywacji, według tego samego scenariusza.

Po odnalezieniu i udzieleniu pomocy medycznej, poszkodowani zostali przetransportowani do Szpitalnego Oddziału Ratunkowego Wojskowego Instytutu Medycznego w Warszawie.

Charakter przedmiotowych manewrów pozwolił czterem Lotniczym Zespołom Poszukiwawczo-Ratowniczym z różnych związków taktycznych i lotnictwa Policji doskonalić swoje umiejętności w realizacji misji poszukiwawczo-ratowniczych oraz sprawdzić jednolitość procedur z obszaru działań lotnictwa, obsługi statków powietrznych i działań medycznych.

Ponadto, w ramach ćwiczenia doskonalono integrację służb, instytucji ratowniczych układu pozamilitarnego działających w systemie Państwowego Ratownictwa Medycznego i Krajowego Systemy Ratowniczo-Gaśniczego przy współdziałaniu z organami administracji samorządowej i wojewódzkimi centrami zarządzania kryzysowego.

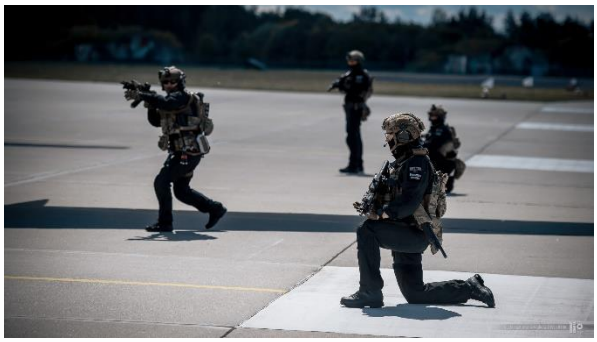
Działania z obszaru ratownictwa (lotniczego, morskiego, naziemnego, medycznego, specjalistycznego) są działaniami synergicznymi, pozwalają każdej ze służb, instytucji, organizacji pożytku publicznego na wypracowanie i sprawdzenie efektywnych procedur dla ratowania zdrowia i życia ludzkiego.

Głównym celem ćwiczenia było sprawdzenie zdolności Sił Zbrojnych RP i układu pozamilitarnego, jako elementów systemu bezpieczeństwa państwa, do przeciwdziałania sytuacjom kryzysowym właściwym dla systemu obrony powierzanej oraz ratownictwa lotniczego i morskiego. Organizatorem przedsięwzięcia było Dowództwo Operacyjne Rodzajów Sił Zbrojnych im. gen. Bronisława Kwiatkowskiego.

Przedsięwzięcie szkoleniowe rozgrywane było w przestrzeni powietrznej RP oraz na obszarach województw: zachodniopomorskiego, pomorskiego, lubelskiego i mazowieckiego.

W ćwiczeniu wzięły udział między innymi następujące podmioty odpowiedzialne za bezpieczeństwo w państwie oraz prowadzenie działań ratowniczych i ratunkowych: Dowództwo Operacyjne RSZ z podporządkowanymi centrami i ośrodkami, Dowództwo Generalne RSZ z podległymi jednostkami wojskowymi, Żandarmeria Wojskowa, Agencja Bezpieczeństwa Wewnętrznego, Wojska Obrony Terytorialnej, Polska Agencja Żeglugi Powietrznej, Policja, Straż Graniczna, Państwowa Straż Pożarna, Morska Służba Poszukiwania i Ratownictwa, Lotnicze Pogotowie Ratunkowe, Polski Czerwony Krzyż oraz podchorążowie uczelni wojskowych.

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




Zdjęcia: st. chor. szt. mar. Arkadiusz Dwulatek (DO RSZ)

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