POLSKIE
TOWARZYSTWO
BEZPIECZEŃSTWA
NARODOWEGO

ZAGROŻENIA O CHARAKTERZE TERRORYSTYCZNYM W RP W LATACH 2021-2022

PTBN
Polskie
Towarzystwo
Bezpieczeństwa
Narodowego

RAPORT PTBN
TOM IV (2023)

ISSN 2720-037X | ISBN 978-83-962605-2-9

ZAGROŻENIA O CHARAKTERZE TERRORYSTYCZNYM W RP W LATACH 2021-2022

Raport PTBN

Tom IV (2023)

Polskie Towarzystwo Bezpieczeństwa Narodowego

Warszawa • 2023

Raport PTBN, Tom IV (2023): „Zagrożenia o charakterze terrorystycznym w RP w latach 2021-2022”

Opracowany przez zespół w składzie:
dr Magdalena Adamczuk
dr Jarosław Cymerski
Krzysztof Izak
Maciej Kluczyński
dr Adam Krawczyk
dr Katarzyna Maniszewska
dr Daria Olender
dr Michał Piekarski
dr Anna Rożej-Adamowicz
dr Damian Szlachter
dr hab. Jarosław Tomasiewicz, prof. UŚ
dr Karolina Wojtasik

Treść Raportu PTBN zawiera wyłącznie prywatne poglądy autorów i nie mogą być one utożsamiane z instytucjami, w których autorzy są zatrudnieni.

Raport PTBN, Tom IV (2023): „Zagrożenia o charakterze terrorystycznym w RP w latach 2021-2022” został zamknięty 20 kwietnia 2023 r. Wersja online jest jego wersją pierwotną.

Autorem fotografii znajdującej się na okładce jest dr Tomasz Michalak.

Wersja online czasopisma jest dostępna na stronie www.PTBN.online

ISSN 2720-037X
ISBN 978-83-962605-2-9

Polskie Towarzystwo Bezpieczeństwa Narodowego
(KRS 0000583118)
ul. Odkryta 38A/8, 03-140 Warszawa
e-mail: zarzad@ptbn.online
www.PTBN.onLine

https://www.facebook.com/polskie.towarzystwo.bezpieczenstwa.narodowego/
https://twitter.com/PTBNonLine

ISBN 978-83-962605-2-9
9 788396 260529

Spis treści

Wstęp

Od opublikowania przez Polskie Towarzystwo Bezpieczeństwa Narodowego poprzedniego Raportu poświęconego terroryzmowi upłynęły dwa lata. Był to okres nacechowany gwałtownymi zwrotami i perturbacjami, by wspomnieć tylko wybuch pandemii COVID-19 oraz wojnę w Ukrainie. Szybkość i nieprzewidywalność zmian utrudnia adekwatną reakcję, dlatego nie można niestety powiedzieć, aby sytuacja w zakresie bezpieczeństwa wewnętrznego i międzynarodowego Polski uległa poprawie. Sygnalizowane w poprzednim raporcie zagrożenia się utrzymują, zaś destrukcyjna dla funkcjonowania państwa i społeczeństwa polaryzacja ideowo-polityczna nie zanikła, ani nie osłabła nawet w obliczu zewnętrznego zagrożenia. Zagrożenie terroryzmem „importowanym" (przede wszystkim dżihadystycznym) wprawdzie zeszło z czołówek mediów, ale jego potencjał nadal się utrzymuje, a w perspektywie długofalowej można się obawiać, że wzrośnie. Do występujących wcześniej zagrożeń doszły natomiast nowe. COVID-19 zdestabilizował nie tylko gospodarkę, ale też stan zdrowia psychicznego społeczeństwa, a będące tego pochodną niezadowolenie z restrykcji wzmocniło tendencje ekstremistyczne. Czas pandemii wykorzystali nasi adwersarze do testowania nowych metod i narzędzi walki poniżej progu wojny, których celem jest podważanie istniejącego ładu, kwestionowanie skuteczności instytucji międzynarodowych, pogłębianie chaosu, tworzenie podziałów i zwiększanie wpływów w określonych obszarach. Czas kryzysu sprzyja działaniom o charakterze hybrydowym, w tym w cyberprzestrzeni oraz w zakresie manipulacji informacją. Co więcej, pandemia potwierdziła powiązanie bezpieczeństwa wewnętrznego z zewnętrznym, które wynika z umiędzynarodowienia wielu sfer aktywności państwowej, gospodarczej i społecznej Zaostrzająca się sytuacja geopolityczna postawiła Polskę w obliczu nowego wyzwania jakim jest instrumentalizacja migracji. Po 24 lutego 2022 r. na pierwszy plan wysunęło się potencjalne zagrożenie aktami dywersji i sabotażu.

Nowa, bardziej złożona sytuacja wymusza rozszerzenie pola analiz również o instrumenty wojny hybrydowej, w tym zwłaszcza w domenie cyber. Za kluczowe w tym

kontekście uznane zostały z jednej strony cyberprzestrzeń, z drugiej obszar morski i przybrzeżny. Cyberprzestrzeń jest nowym, stosunkowo słabo rozpoznanym i szybko zmieniającym się teatrem działań, który umożliwia zarówno operacje propagandowo-psychologiczne, jak i wywiadowcze oraz sabotażowe. Wybrzeże morskie i wody przybrzeżne wydają się być najbardziej podatne na penetrację nieprzyjaciela, zarazem znaczenie tych obszarów dla gospodarki (choćby w kontekście importu surowców energetycznych lub wsparcia humanitarnego i wojskowego dla Ukrainy) trudno przecenić. Wymusza to szczególną troskę o obecną w tej części kraju infrastrukturę krytyczną – strategiczną dla transportu morskiego czy kolejowego oraz bezpieczeństwa energetycznego RP. Wysadzenie rurociągu Nord Stream II, działania rozpoznawcze wobec Baltic Pipe czy w okolicach terminala przeładunkowego ropy naftowej dowodzą tego dobitnie.

Raport składa się z trzech rozdziałów. Pierwszy opisuje zaistniałe i potencjalne zagrożenia w zakresie terroryzmu (i będącego jego zapleczem ekstremizmu), cyberbezpieczeństwa i bezpieczeństwa morskiego. Drugi analizuje wybrane elementy systemu antyterrorystycznego RP. Trzeci zawiera wnioski i zalecenia wynikające z porównania wyzwań i odpowiedzi na nie.

Raport został opracowany przez zespół ds. analiz zagrożeń o charakterze terrorystycznym i hybrydowym PTBN w oparciu o dostępne w przestrzeni publicznej materiały informacyjne, raporty analityczne, monografie i publikacje pokonferencyjne, strony internetowe wybranych instytucji państwowych, instytucji oraz organizacji UE i NATO, jak również szerokie spektrum krajowych aktów prawnych.

Celem niniejszego Raportu jest wywołanie konstruktywnej dyskusji nad kierunkiem rozwoju krajowego systemu antyterrorystycznego. Raport jest skierowany do badaczy zjawiska terroryzmu, dziennikarzy zajmujących się niniejszą problematyką, jak również do osób, które tworzyły polski system antyterrorystyczny lub pracują obecnie nad jego doskonaleniem i skutecznością. Szczególnym adresatem Raportu są przedstawiciele wszystkich instytucji i organów państwowych, które tworzą na co dzień „wspólnotę antyterrorystyczną RP".

Ideą Polskiego Towarzystwa Bezpieczeństwa Narodowego jest budowa „bezpieczeństwa ponad podziałami", dlatego zapraszamy wszystkich zainteresowanych do dyskusji o jednym z kluczowych podsystemów bezpieczeństwa narodowego, który jest inkubatorem przyszłych standardów w tym obszarze. Efekty tej dyskusji będą prezentowane w kolejnych aktualizacjach niniejszego opracowania.

1. Charakterystyka zagrożeń terrorystycznych dla RP w latach 2021-2022

1.1. Terroryzm w państwach europejskich

Raport Europol-u TE-SAT z 2022 r. wskazał znaczący spadek liczby aktów terroryzmu w Europie, zarówno dokonanych, nieudanych, jak i powstrzymanych przez organy ścigania krajów członkowskich UE w porównaniu do lat wcześniejszych. Na ten trend, jak się wydaje miała głównie wpływ pandemia i wprowadzone cyklicznie obostrzenia ograniczające łatwość przemieszczania się, jak również zmniejszenie się wpływu radykalizmu islamskiego po upadku Państwa Islamskiego. W 2019 r. dokonano lub próbowano dokonać[1] w Europie 55 zamachów, w 2020 – 57, w 2021 r. – 15. Spadek dotyczył głównie zamachów grup narodowowyzwoleńczych i separatystycznych (brak zamachów) i skrajnie lewicowych (jeden zamach). Raport uwypuklił regionalną działalność radykalnych organizacji lewicowych i anarchistycznych w Europie. Polskie grupy ekstremistów współpracowały ze swoimi odpowiednikami z Czech, Niemiec, Słowacji i Białorusi. Europol podaje następujące statystyki dla Polski: TE-SAT2020: 1 atak, 4 aresztowania w 2019 roku; TE-SAT2021: 9 aresztowań w 2020 roku a TE-SAT 2022 odnotowuje aresztowanie w 2021 roku w Polsce trzech osób powiązanych z organizacjami lub działaniem terrorystycznym o nieokreślonej ideologii.

Podobnie *Global Terrorism Index 2020* wskazuje na niskie zagrożenie terroryzmem w Polsce, która kwalifikowana jest na 114 miejscu (z indeksem 0.239, dla porównania miejsce pierwsze to Afganistan z wynikiem 9.592 w 10-stopniowej skali). Z kolei raport *Global Terrorism Index* 2022 wskazuje na brak w Polsce aktów przemocy kwalifikowanych jako działania terrorystyczne. W raporcie sklasyfikowano Polskę na ostatniej

[1] Podane statystyki pochodzą z raportów Europolu Te-Sat 2020, 2021 oraz 2022, które przedstawiają liczbę ataków dokonanych, nieudanych oraz udaremnionych przez służby. Dane przedstawione są bez Wielkiej Brytanii, która od TE-SAT 2021 nie jest uwzględniana w raporcie Europolu.

93 pozycji w rankingu wraz z takimi krajami UE jak Portugalia, Słowacja, Słowenia, Węgry, Estonia i Łotwa. Wyżej uplasowała się Litwa (pozycja 83), Republika Czeska i Dania (pozycja 86), Rumunia (78 pozycja), Szwecja (69 pozycja), Hiszpania (55 pozycja), Austria (52 pozycja), Niemcy (pozycja 33), Grecja (29 pozycja). Raport *Global Terrorism Index* 2023, który ukazał się w marcu 2023 roku i przedstawia dane za rok 2022 wskazuje na utrzymanie tego trendu: Polska ponownie jest zakwalifikowana do najbezpieczniejszych pod względem zagrożeń terrorystycznych państw świata plasując się kolejny raz na 93 miejscu.

Pandemia uwypukliła w EU polaryzację życia społecznego nasilając postawy ekstremistyczne. Według *Raportów TE-SAT 2022 oraz 2021* radykalne grupy wprowadziły nowe sposoby rekrutacji członków i stworzyły szerokie zaplecze zwolenników. Grupy te posługiwały się hasłami walki o „zachowanie wolności" i „ratowanie gospodarki" przesyłając również wezwanie do obywatelskiego nieposłuszeństwa czy wręcz fizycznego oporu wobec wprowadzonych obostrzeń ze względu na COVID-19. Często te hasła powiązane były z teoriami spiskowymi dotyczącymi technologii 5G czy ruchu QAnon. Takie działania zostały zauważone w całej Europie (również w Polsce), gdzie dochodziło do podpaleń czy aktów wandalizmu wobec infrastruktury telekomunikacyjnej.

Finansowanie grup ekstremistycznych w Polsce często odbywało się poprzez legalną działalność gospodarczą firm zajmujących się sprzedażą akcesoriów, ubiorów, muzyki itp. jak również poprzez internetowe zbiórki.

Służby podkreślają, że w wyniku obostrzeń i lockdownów, które zmniejszyły mobilność członków grup, ich komunikacja prawie całkowicie przeniosła się do Internetu. Również w Polsce ekstremiści za jego pomocą podtrzymywali krajowe i międzynarodowe relacje z grupami w innych państwach. *Raport TE-SAT 2021* wskazuje, że mimo ograniczeń w podróżowaniu oraz spotkaniach i koncertach kontakty pomiędzy polskim odłamem grupy Blood & Honour i odpowiednikami z innych państw były kontynuowane a nawet się wzmagały. Jedną z osi narracji łączących prawicowych ekstremistów z różnych państw Europy jest niechęć do Unii Europejskiej postrzeganej jako „wspólny wróg"

Jako zagrożenie dla bezpieczeństwa *Raport TE-SAT 2021* wskazał na coraz częstszy udział członków grup radykalnych w paramilitarnych obozach, warsztatach survivalowych, szkoleniach posługiwania się bronią palną oraz treningach walki wręcz. Raport odnotowuje istotny wzrost zainteresowania tego typu aktywnościami wśród ekstremistów prawicowych w Polsce.

1.2. Zagrożenia o charakterze hybrydowym i terrorystycznym w kontekście agresji Rosji na Ukrainę

Rozpoczęta w dniu 24 lutego 2022 r. agresja na Ukrainę jest czynnikiem intensyfikującym rosyjską kampanię hybrydową w RP. Przedmiotem tej kampanii jest przede wszystkim pomoc udzielana Ukrainie przez Polskę, w tym wsparcie dla uchodźców z Ukrainy, transfer pomocy wojskowej i humanitarnej oraz obecność w Polsce znacznych sił sojuszniczych. Wojna na Ukrainie wpływa również na wzrost ryzyka wystąpienia w Polsce zdarzenia o charakterze terrorystycznym lub sabotażowym inspirowanego przez Federację Rosyjską z możliwością wykorzystania zasobów państw trzecich. W dniu 28 lutego 2022 r. wprowadzony został stopień alarmowy BRAVO na terenie dwóch województw – podkarpackiego i lubelskiego, a w dniu 15 kwietnia 2022 r. przedłużono czas jego obowiązywania do 28 lutego 2023 r. oraz rozszerzono zasięg terytorialny na cały kraj. Od 6 października 2022 r. stan BRAVO obejmuje też polską infrastrukturę energetyczną poza granicami Polski, w tym platformy wiertnicze i inne obiekty zlokalizowane poza obrębem polskich wód terytorialnych.

Na Ukrainie Rosja nie osiągnęła środkami militarnymi swoich celów politycznych. Ujawnione słabości rosyjskich sił zbrojnych oraz dostawy uzbrojenia z Zachodu skutkują porażkami frontowymi. Poza działaniami o charakterze stricte militarnym Kreml kontynuuje kampanię hybrydową, która ma osłabić wolę walki w ukraińskim społeczeństwie, zaufanie we władze i demokratyczne instytucje państwowe. Te działania - poniżej progu wojny - skupiają się przede wszystkim na dezinformacji, cyberatakach, siłowych deportacjach i atakach na infrastrukturę krytyczną. Jest możliwe, że Rosja poszukując nowych sposobów skompensowania własnych deficytów w zakresie konwencjonalnych sił zbrojnych i nieskuteczności środków hybrydowych, będzie podejmować działania terrorystyczne i sabotażowe w krajach pełniących rolę frontowego zaplecza logistycznego Ukrainy, takich jak Polska czy Rumunia. Podobne działania miały już miejsce, przykładowo, w roku 2014 doszło do zamachów na składy amunicji w miejscowości Vrbětice w Republice Czeskiej.

Tego rodzaju ataki mogą mieć na celu zakłócenie procesów logistycznych (transportu pomocy wojskowej), wywarcie wpływu na polskie społeczeństwo oraz społeczeństwa państw zachodnich lub wywołanie zakłóceń w gospodarce i ustroju Polski, w takim stopniu, aby zmusić Polskę do zachowań zgodnych z interesem Rosji.

W szczególności możliwe są zamachy lub akty sabotażu wymierzone w następujące cele:

1. Ataki na infrastrukturę krytyczną, zwłaszcza energetyczną oraz transportową (kolejowa, morska, lotnicza, drogowa). Celem działań może być uniemożliwienie

jej wykorzystania (np. portów lotniczych i morskich, czy wyspecjalizowanych kolejowych centrów logistycznych) oraz wykazanie nieskuteczności jej ochrony oraz niezdolności państwa do poradzenia sobie z wywołanym przez atak kryzysem wewnętrznym lub międzynarodowym o charakterze politycznym, ekonomicznym czy ekologicznym (w przypadku działań sabotażowych lub terrorystycznych, które skutkują katastrofą ekologiczną jak np. atak na transport lub magazyn paliw).

2. Ataki na obiekty, sprzęt i personel wojskowy Polski oraz krajów sojuszniczych NATO przebywających czasowo na terytorium RP: zniszczenie ważnego i trudnego do zastąpienia sprzętu wojskowego, zabicie lub uprowadzenie żołnierzy, skażenia obszaru rozlokowania jednostek wojskowych. Celem takiego ataku byłoby wykazanie niezdolności sił zbrojnych do ochrony własnego personelu i instalacji. W przypadku ataku na żołnierzy państw sojuszniczych może być on powiązany z oddziaływaniem informacyjnym wymierzonym w społeczeństwa zarówno Polski, jak i tych państw. W Polsce adwersarz może dążyć do wywołania negatywnych nastrojów wobec obcych sił zbrojnych, zaś u Sojuszników wywołać niechęć do angażowania sił i środków w działania, które nie mają bezpośredniego wpływu na społeczeństwa tych państw.

3. Ataki na osobę powszechnie znaną lub cel symboliczny. Taki atak mógłby mieć na celu sprowokowanie reakcji społecznych, w szczególności pogłębienie polaryzacji politycznej. Dla wywołania wrażenia, że sprawcami ataku są osoby nie powiązane z Rosją, może mieć charakter prowokacji pod tzw. „fałszywą flagą".

W szczególności należy zwrócić uwagę na fakt, że powyższe działania będą najprawdopodobniej prowadzone przy wykorzystaniu zarówno metod terrorystycznych jak i narzędzi hybrydowych. Przykładowo, zamach wymierzony w infrastrukturę krytyczną energetyczną (np. terminal przeładunkowy, bazę paliw, port morski, platformę wydobywczą, sieć elektroenergetyczną, strategiczny kolejowy korytarz transportowy) może być wsparty przez akcję dezinformacyjną, sugerującą groźbę braku dostępności paliw na rynku. Zamach, który będzie wymierzony w infrastrukturę wojskową, może być wsparty przez demonstrację siły militarnej lub inne działania stwarzające wrażenie, że Polska jest w danym momencie szczególnie podatna na atak. Możliwe jest też wywoływanie paniki przy pomocy fałszywych alarmów bombowych (jak podczas egzaminów maturalnych w maju 2021 r.).

Ryzyko wystąpienia takich zagrożeń zwiększa fakt, że Rosja musi modyfikować charakter swoich działań. Szybka rezygnacja państw zachodnich z importu wschodnich surowców energetycznych sprawiła, że Rosja może próbować przerwać inne szlaki ich dostaw, nie tylko te bliskowschodnie, ale też bałtyckie. Wówczas pozwoliłoby to na

zastosowanie presji ekonomicznej i politycznej w postaci złożenia oferty dostaw gazu w zamian za polityczne ustępstwa.

W 2023 roku należy spodziewać się dalszej intensyfikacji rosyjskiej kampanii dezinformacyjnej przeciwko RP, której celem będzie dalsza polaryzacja społeczeństwa, podważenie zaufania w instytucje państwowe i przede wszystkim w demokratyczne procesy wyborcze".

1.3. Wykorzystanie metod o charakterze terrorystycznym przez rodzime środowiska radykalne

Mieszkaniec województwa lubelskiego Hubert C. w sierpniu 2021 r. doprowadził do podpalenia punktu szczepień na COVID-19 i siedziby Sanepidu w Zamościu. Rok wcześniej podpalił również dwa maszty sieci komórkowej w technologii 5G w swojej rodzinnej miejscowości Złojec. Hubert C. zbiegł w 2021 r. do Szwajcarii, został jednak zatrzymany kilka miesięcy później na terenie województwa podkarpackiego przez Policję. W procesie sądowym Hubert C. został opisany jako wyznawca teorii spiskowych zradykalizowany w wyniku materiałów pozyskiwanych w Internecie na temat rzekomej szkodliwości technologii 5G oraz propagandy ruchu przeciwko restrykcjom sanitarnym związanym z epidemią COVID-19.

Prokuratura Okręgowa w Zamościu zarzuciła Hubertowi C. podłożenie ognia i spowodowanie znacznych strat materialnych (łącznie na kwotę 370 tys. zł.), ale też działanie o charakterze terrorystycznym. W opinii prokuratury czyny te zostały dokonane w celu zastraszenia wielu osób. W sądzie podpalacz przyznał się do winy i wyraził skruchę dobrowolnie poddając się wyrokowi. Został uznany we wrześniu 2022 r. za winnego i skazany na karę 5 lat więzienia. Hubert C. został zwolniony z kosztów sądowych, ale musi dodatkowo pokryć straty finansowe poniesione przez Sanepid oraz lubelski Urząd Wojewódzki, a także przez operatora zaatakowanej sieci komórkowej.

1.4. Wybrane incydenty związane z działaniami zagranicznych organizacji terrorystycznych

W 2021 r. Rzecznik Ministra Koordynatora Służb Specjalnych Stanisław Żaryn stwierdził: „Ustalenia ABW wskazały […], że w Polsce lokowani są ludzie stanowiący zaplecze

logistyczne dla dżihadu. Od 2016 r. ABW kilkukrotnie zatrzymywała osoby: przygotowujące zamachy terrorystyczne, zajmujące się finansowaniem ISIS, szerzące propagandę dżihadystyczną, radykalizujące innych ludzi lub zbierające fundusze dla Państwa Islamskiego. Działania ABW nakierowane były również na identyfikowanie i wydalanie z Polski tych cudzoziemców, którzy brali czynny udział w działaniach bojowych ISIS lub wspierali je. Na wniosek ABW kilkudziesięciu cudzoziemców związanych z islamskim terroryzmem opuściło w ostatnich latach Polskę”[2].

a. Przypadek obywatela Afganistanu zaangażowanego w atak na polski patrol wojskowy w Ghazni w 2011 r.

W dniu 21 grudnia 2011 r. w miejscowości Rawza w afgańskiej prowincji Ghazni doszło do wybuchu improwizowanego ładunku wybuchowego (IED). W wyniku ataku zginęło pięciu żołnierzy z 20. Brygady Zmechanizowanej z Bartoszyc. Był to najtragiczniejszy w skutkach atak na patrol polskich żołnierzy z misji stabilizacyjnej w Afganistanie. Do zamachu przyznali się talibowie. W wyniku śledztwa prowadzonego przez SKW przy wsparciu SWW na początku 2012 r. władze afgańskie doprowadziły do zatrzymania 5 terrorystów współodpowiedzialnych za atak. Informacje przekazane afgańskim organom ścigania przyczyniły się do ich zatrzymania. Zebrane w sprawie informacje wskazywały, że głównym podejrzewanym o zorganizowanie zamachu został komendant talibów – Eid Mohammad, który ukrywał się na terenie Pakistanu. Ostatecznie został on zastrzelony w dniu 7 lutego 2020 r. przez afgańskie siły bezpieczeństwa (NDS) w trakcie próby zatrzymania.

Wśród zatrzymanych w 2012 r. osób zaangażowanych w przygotowanie ataku na polski patrol wojskowy wjeżdżający do m. Rawza znalazł się afgański tłumacz zatrudniony w bazie w Ghazni, który współpracował z talibami. Po wyjściu na wolność tłumacz starał się o ewakuację do Polski po przejęciu przez talibów władzy w Afganistanie w sierpniu 2021 r., co jednak zostało skutecznie zablokowane dzięki negatywnemu stanowisku SKW.

b. Przypadek Palestyńczyka w Olsztynie

W dniu 24 maja 2021 r. Straż Graniczna, działając na wniosek Agencji Bezpieczeństwa Wewnętrznego zatrzymała zradykalizowanego religijnie mężczyznę pochodzącego z Autonomii Palestyńskiej, wykazującego skłonność do przemocy wobec osób postronnych. Mężczyzna stwarzał bezpośrednie zagrożenie dla bezpieczeństwa wewnętrznego

[2] S. Żaryn, *Terroryzm aktualnym wyzwaniem*, „Biuletyn Analiz i Reagowania RCB”, nr 32, Warszawa 2021 r., s. 3.

RP, ponieważ posiadał umiejętności z zakresu chemii, technologii czy obsługi broni palnej oraz utrzymywał relacje z członkami organizacji terrorystycznych. Zgodnie z decyzją sądu Palestyńczyk trafił do strzeżonego ośrodka Straży Granicznej i stamtąd cudzoziemiec został wydalony z Polski.

c. Przypadek obywatela Gruzji

W lipcu 2022 r. ABW we współpracy ze Strażą Graniczną zatrzymała obywatela Gruzji Mamukę T. vel Abubakar T. w związku z podejrzeniem prowadzenia działalność o charakterze terrorystycznym na terenie Polski. Postawą prawną zatrzymania Gruzina była decyzja Ministra Spraw Wewnętrznych i Administracji o zobowiązaniu cudzoziemca do powrotu i zakazie wjazdu na teren strefy Schengen na okres 5 lat. Cudzoziemiec utrzymywał kontakty z osobami zaangażowanymi w aktywność terrorystyczną, które brały udział w działaniach zbrojnym na rzecz Państwa Islamskiego (ISIS). Abubakar T. zajmował się w Polsce nielegalną migrację mieszkańców krajów arabskich w celu ich przerzucenia do krajów Europy Zachodniej, jak również był członkiem grupy przestępczej handlującej narkotykami i dokonującej wymuszeń rozbójniczych na terenie RP. Abubakar T. został deportowany z Polski do Gruzji kilkanaście dni po zatrzymaniu.

d. Kryzys migracyjny na wschodniej granicy UE a zagrożenia o charakterze terrorystycznym dla RP

W kontekście kryzysu migracyjnego na wschodniej granicy UE wywołanego przez reżim Aleksandra Łukaszenki wobec Polski i Litwy, w dniu 27 września 2021 r. w trakcie konferencji prasowej Ministra Koordynatora Służb Specjalnych oraz Ministra Obrony Narodowej przedstawiono wyniki głębokiej weryfikacji tożsamości ponad 200 cudzoziemców przebywających w ośrodkach strzeżonych Straży Granicznej. Rzecznik Ministra Koordynatora Służb Specjalnych Stanisław Żaryn zaznaczył wówczas, że „informacje dotyczące co czwartego badanego wskazują na ich niebezpieczne powiązania i ich udział w praktykach niezgodnych z prawem. Ustalenia do tej pory poczynione pokazują, że co dziesiąta osoba ma możliwe powiązania z organizacjami terrorystycznymi, przestępczością kryminalną, przemytem ludzi, a także fałszowaniem dokumentacji”[3]. Dodatkowo 20 proc. zatrzymanych w Polsce nielegalnych imigrantów miało stałe związki z Federacją Rosyjską.

[3] S. Żaryn, *Napięta sytuacja na granicy*, „Polskie Radio 24”, 27.11.2021 r. w: https://polskieradio24.pl/5/1222/artykul/2815251,napieta-sytuacja-na-granicy-zaryn-wsrod-zatrzymanych-osoba-posiadajaca-kontakty-z-panstwem-islamskim (dostęp: 21.12.2022 r.)

Z danych udostępnionych w dniu 19 sierpnia 2021 r. w komunikacie PAP przez Stanisława Żaryna wynika, że na podstawie ustawy o działaniach antyterrorystycznych w pierwszym półroczu 2021 r. ABW 14 razy wpisała cudzoziemców na listę osób niepożądanych w Polsce Centrum Antyterrorystycznego (CAT) ABW. Oprócz tego jeden wniosek Szefa ABW dotyczył wydania decyzji o zobowiązaniu cudzoziemca do powrotu w związku z obawą, że może on prowadzić działalność terrorystyczną na terenie RP, a drugi cofnięcia statusu uchodźcy na terytorium Polski. Dla porównania w latach 2015-2019 na podstawie materiałów ABW wydalono z Polski 14 cudzoziemców stanowiących zagrożenie terrorystyczne.

W perspektywie długofalowej potencjał zagrożenia terrorystycznego z tego kierunku będzie zależał nie tylko od skuteczności służb, ale także od zdolności państwa i społeczeństwa polskiego do integracji imigrantów, aby przeciwdziałać ich radykalizacji.

Przypadek obywatela Tadżykistanu

W kwietniu 2021 r. obywatel Tadżykistanu Odilkhon S. przedostał się do Polski nielegalnym szlakiem migracyjnym zorganizowanym przez białoruskie służby. Następnie został zatrzymany przez Straż Graniczną i trafił do strzeżonego ośrodka dla cudzoziemców. Podejmowana w ośrodku aktywność zatrzymanego wskazywała na jego radykalizację religijną. ABW w ramach przeciwdziałania zagrożeniom o charakterze terrorystycznym ustaliła, że ww. mężczyzna jest sympatykiem Państwa Islamskiego. Odilkhon S. otrzymał decyzję komendanta placówki Straży Granicznej w Płaskiej o zobowiązaniu do powrotu do kraju pochodzenia oraz o zakazie ponownego wjazdu do Polski i państw strefy Schengen na okres 3 lat. **Mężczyzna** został uznany przez ABW za osobę zagrażającą bezpieczeństwu RP i deportowany w dniu 10 listopada 2021 r. z Polski.

Przypadek obywatela Iraku

W trakcie kryzysu imigranckiego na granicy polsko-białoruskiej do Polski trafił obywatel Iraku Husham M.H., któremu w trakcie pobytu w ośrodku dla cudzoziemców prowadzonym przez SG udowodniono kontakty z osobą mającą związki z terroryzmem. Osobą tą był specjalista od materiałów wybuchowych, członek Państwa Islamskiego, zatrzymany w 2021 r. na terenie jednego z krajów Unii Europejskiej. Husham M.H. został na tej podstawie wydalony z RP w 2022 r.

1.5. Zagrożenia o charakterze terrorystycznym wobec obywateli RP poza granicami kraju

23 maja 2021 r. doszło do wymuszenia lądowania na lotnisku w Mińsku samolotu linii Ryanair lecącego z Aten do Wilna (lot nr FR4978), na pokładzie którego znajdował się białoruski bloger opozycyjny Raman Pratasiewicz oraz 100 innych osób. Wśród uprowadzonych pasażerów znajdowali się również obywatele RP.

Z materiału dowodowego zebranego przez polskie organy ścigania oraz służby krajów prowadzące w tej sprawie swoje śledztwa (m. in. USA, Litwa, Grecja) oraz ICAO (*International Civil Aviation Organization*) wynika, że w czasie incydentu w sali operacyjnej wieży kontroli lotów w Mińsku przebywał funkcjonariusz białoruskiej cywilnej służby specjalnej (KGB), który w kluczowym momencie podejmował decyzje za kontrolera żeglugi powietrznej. To od funkcjonariusza KGB wychodziły instrukcje i decyzje dotyczące sprowadzenia statku powietrznego na lotnisko w Mińsku, eskortowanego przez wojskowe MIG-29, co miało być spowodowane groźbą ataku bombowego, rzekomo otrzymaną drogą elektroniczną od terrorystycznej organizacji Hamas (rzecznik Hamas zaprzeczył związkom organizacji z tą wiadomością).

Według polskich służb (Urząd Lotnictwa Cywilnego, ABW) cała sytuacja została sprowokowana przez stronę białoruską w celu uprowadzenia samolotu lot nr FR4978 i nosi ona znamion terroryzmu państwowego. W ocenie szefa linii lotniczej Ryanair Michaela O'Leary cała sprawa jest dywersją i „sponsorowanym przez państwo piractwem". Amerykański Departament Sprawiedliwości (sąd federalny w stanie New York) postawił czterem obywatelom Białorusi zarzuty bezprawnego przekierowania lotu pasażerskiego z obywatelami amerykańskimi w celu aresztowania białoruskiego dysydenta.

1.6. Radykalizacja jako potencjalne źródło zagrożenia terrorystycznego

a. Radykalizacja

Akty politycznie i/lub światopoglądowo motywowanej przemocy, stanowiące bezpośrednie zagrożenie dla bezpieczeństwa publicznego, są na ogół efektem końcowym długotrwałego procesu radykalizacji. Radykalizacja nie musi kulminować się w przemocy, jednak zawsze stanowi potencjalne zagrożenie wymagające monitorowania (zdarzają

się też spontaniczne, impulsywne akty przemocy, jednak ich znaczenie jest marginalne). Przemoc może być dziełem (a) jednostek indywidualnie zradykalizowanych, (b) jednostek zradykalizowanych w grupie, ale działających indywidualnie, (c) radykalnych grup, działających żywiołowo (np. demonstracje) lub (d) w sposób zorganizowany.

Radykalizacja nie jest działaniem jednorazowym, lecz procesem, który może przebiegać szybciej lub wolniej. Jednostka przechodzi przez poszczególne etapy tworzące pewną sekwencję. **Proces radykalizacji** polega na przyjęciu przez jednostkę lub grupę poglądów i postaw uznawanych za skrajne, to znaczy znacząco odbiegające od konsensu głównego nurtu, kwestionujące podstawy porządku społecznego. Radykalizacja może dokonywać się z grubsza rzecz biorąc na dwa sposoby: (1) poprzez przejmowanie od podstaw radykalnych poglądów przez jednostkę wcześniej apolityczną, (2) poprzez stopniową radykalizację wcześniejszych przekonań, przejawiającą się w eskalacji żądań, zmniejszeniu gotowości do kompromisu, skłonności rozwiązywania sporu metodami przymusu prawnego lub pozaprawnego (przemoc).

Ostatecznie może to prowadzić do działań przemocowych, zarówno w sferze symbolicznej, jak i fizycznej. Radykalizacja może dokonywać się pod wpływem grupy (środowiska, organizacji), do której jednostka należy lub utrzymuje kontakt, jak też indywidualnie, gdy osoba radykalizująca się sama inicjuje ten proces, bez interakcji z innymi ekstremistami (samoradykalizacja).

Przyczynami radykalizacji mogą być: (a) pogorszenie statusu jednostki, (b) strach przed pogorszeniem statusu, (c) brak poprawy statusu w stopniu zgodnym z aspiracjami. Dotyczy to zarówno statusu materialnego (dochód rozporządzalny, co istotne – w kontekście rozwarstwienia majątkowego) jak niematerialnego: swobód (w tym poczucia sprawczości, kontroli nad własnym życiem, wpływu na otoczenie) i prestiżu (w tym kwestii tożsamościowych).

Brak satysfakcji w którymkolwiek z tych aspektów prowadzi do poczucia krzywdy, wykluczenia i niesprawiedliwości. Z badań (m.in. prowadzonych w ramach programu Dialogue about Radicalisation and Equality) wynika, że kluczową kwestią nie jest obiektywny status jednostki, ale jej subiektywne odczucie (zwłaszcza w sferze niematerialnej). Jest to szczególnie istotne w przypadku najmłodszych roczników (tzw. zoomers), przywiązujących ogromną wagę do indywidualnego dobrostanu, który może zostać naruszony nie tylko szeroko rozumianą agresją (działaniem), ale też brakiem uwagi czy szacunku (zaniechaniem działania). W rezultacie radykalizację może wywołać nie tylko niesprawiedliwość systemowa (stan prawny, funkcjonowanie instytucji publicznych), ale też ideowa (symbole ważne dla tożsamości jednostki,

w tym język) oraz kontekstowa (najróżniejsze czynniki środowiskowe i sytuacyjne, tworzące otoczenie codziennego życia jednostki). W wielu teoriach radykalizacji wspomina się też moment, gdy jednostka znajduje „winnego" swojego stanu i to w stosunku do tej osoby/grupy/instytucji kieruje działania przemocowe. Zagrożenie dla swego statusu jednostka może dostrzegać zarówno w czynnikach wewnętrznych jak i zewnętrznych.

Radykalizacja następuje w pewnym otoczeniu zewnętrznym, które może jej sprzyjać lub przeciwdziałać. **Warunki** towarzyszące radykalizacji możemy podzielić na trzy grupy: makrostrukturalne (sytuacja polityczna i ekonomiczna w kraju), mikrostrukturalne (bezpośrednie otoczenie jednostki: grupy rodzinne, towarzyskie, sąsiedzkie, zawodowe) i indywidualne (cechy jednostkowe: osobowość, doświadczenia).

Na wszystkich tych poziomach w 2021 r. zaobserwować można było pogorszenie stanu/zwiększenie potencjału radykalizacji w społeczeństwie. Głównym czynnikiem o charakterze makrostrukturalnym pozostawała pandemia COVID-19, która po letnim okresie uspokojenia jesienią nabrała nowej dynamiki. Pomimo dobrej sytuacji gospodarczej pandemia wciąż zagrażała funkcjonowaniu niektórych dziedzin gospodarki, zwłaszcza drobnego biznesu i sfery usług; z kolei przyśpieszająca inflacja uderzała przede wszystkim w dochody pracowników sfery budżetowej. Sytuację międzynarodową Polski w największym stopniu determinował kryzys migracyjny sprokurowany przez władze białoruskie, gdy w drugiej połowie roku doszło do zorganizowanych naruszeń granicy państwowej i unijnej na bezprecedensową skalę. Co charakterystyczne, nawet pandemia i kryzys migracyjny nie doprowadziły do wypracowania konsensusu, gdyż obie strony konfliktu politycznego zainteresowane były tylko realizowaniem własnych celów (przede wszystkim – osłabieniem przeciwnika). Niemożność wypracowania wspólnego, kompromisowego stanowiska nawet w fundamentalnej sprawie zagrożenia zewnętrznego, kontrastująca choćby ze zgodą narodową wobec kryzysu migracyjnego na Litwie, jest bardzo niepokojąca.

Na poziomie mikrostrukturalnym obserwować można było kontynuację wcześniejszych trendów: rozpadowi (czy przynajmniej osłabieniu) dotychczasowych więzi międzyludzkich towarzyszyło poszukiwanie i formowanie nowych więzi na bazie zbieżności politycznej i światopoglądowej, czemu sprzyjało przeniesienie aktywności do Internetu w czasie lockdownu w poprzednim roku. Internet zapewnia poczucie anonimowości i bezkarności, oferuje ogrom niemożliwych do zweryfikowania informacji, w których każdy odnajdzie potwierdzenie swoich przekonań; pozwala odnaleźć ludzi o podobnych poglądach, a co za tym idzie – środowisko dające różne rodzaje wsparcia, poczucie uczestnictwa i duchowe przywództwo. Media społecznościowe

swymi algorytmami ułatwiają formowanie „baniek filtrujących" (tworzących swoistą barierę informacyjną, uniemożliwiającą dostęp alternatywnych informacji do zamkniętego środowiska), które nieraz stają się tzw. echo-chambers, wzmacniającymi przekaz ekstremistów.

Zaryzykować można twierdzenie, że również na poziomie indywidualnym dostrzec można zwiększoną podatność na radykalizację. Zazwyczaj najbardziej narażone na uleganie ekstremizmowi są osoby młode, budujące własną tożsamość poprzez rewizję dotychczasowych wartości („młodzieńczy bunt"). Obserwowanym przez psychologów skutkiem pandemii jest destabilizacja psychiki wielu osób (także dorosłych) spowodowana wytrąceniem z dotychczasowego trybu życia oraz obawami o zdrowie i życie, przejawiająca się w rozdrażnieniu, nadpobudliwości, skłonności do paranoi (wiary w teorie spiskowe).

Radykalizacja jest procesem mentalnym, wewnętrznym, jednak zaobserwować można różne jej **przejawy**. Najłatwiej zauważyć je w Internecie. O ile złośliwe przedstawianie przeciwnika, tendencyjne dobieranie faktów, zastępowanie argumentów merytorycznych demagogicznymi należy uznać za naturalny, powszechnie występujący element propagandy politycznej, to symptomami radykalizacji są niewątpliwie: (1) używanie nacechowanych emocjonalnie (np. wulgarnych) obelg; (2) dehumanizacja przeciwnika (również poprzez np. wyzwiska, deformację nazw i nazwisk); (3) aprobata przemocy, a tym bardziej nawoływanie do niej. Nawet pobieżny przegląd polskiego Internetu pozwala zauważyć, że wszystkie te zjawiska stały się powszechne w mediach społecznościowych, komentarzach internetowych, a nawet niektórych, na razie niszowych portalach i blogach. Radykalizacja może być również obserwowana w warstwie ikonograficznej (awatary, nakładki), a także – w sposób najbardziej wymierny – w częstotliwości odwiedzin na ekstremistycznych stronach czy liczbie polubień profili i postów na Facebooku, Twitterze, Instagramie czy Youtube. Radykalizację dostrzec można również w przestrzeni publicznej, gdy kojarzone z ekstremizmem symbole, obrazki czy slogany pojawiają się na odzieży, samochodach, murach itp.

Wymienione powyżej przejawy radykalizacji mogą stanowić zagrożenie dla bezpieczeństwa publicznego, nakręcając spiralę agresji oraz – jak dowodzi w swoich badaniach francuski socjolog Gilles Kepel – mogą bezpośrednio prowadzić do czynów, w tym ataków terrorystycznych. Zwłaszcza przynależność do radykalnej grupy (także wirtualnej) sprzyja działaniom przemocowym, gdyż przyczyniają się one do wzmocnienia więzi grupowych (działania zespołowe) a jednostce zapewniają akceptację (działania indywidualne). Napisanie hasła lub narysowanie symbolu na elewacji cudzego budynku można już uznać za przejaw przemocy symbolicznej, zniszczenie

symbolu lub nośnika propagandy (np. plakat) przeciwnika manifestuje gotowość do działań destrukcyjnych. Dotyczy to nie tylko symboli stricte politycznych, ale – w związku z konfliktem światopoglądowym – także historycznych i religijnych (chrześcijańskich, judaistycznych, muzułmańskich). Obiektem agresji mogą stać się również budynki o takim charakterze (podpalenia kościoła w Lublinie w lutym 2021 r., katedry w Opolu 19 grudnia 2021 r.).

Kolejnym krokiem staje się przemoc werbalna i fizyczna skierowana bezpośrednio wobec przeciwników politycznych (a czasem przypadkowych przedstawicieli znienawidzonych zbiorowości – tu jednak trudno czasem ją odróżnić od przestępczości pospolitej). Przemoc przeciw ludziom ma dotychczas na ogół charakter rozproszony, spontaniczny i chaotyczny. Najczęstszym jej przejawem są ataki słowne. Najbardziej niepokojącą ich formę stanowią pogróżki (czasem przyjmujące postać „wyroków śmierci"), przy czym podkreślić należy, że zagrożenie nie staje się mniejsze w sytuacji, gdy sprawcami są osoby niezrównoważone. Pocieszającym symptomem jest fakt, że w odróżnieniu od poprzedniego roku, w 2021 udało się uniknąć poważniejszych aktów przemocy w czasie masowych demonstracji ulicznych.

O ile w latach 90. XX w. i na początku XXI w. główne przyczyny radykalizacji miały charakter ekonomiczny (pauperyzacja dużych grup społecznych będąca skutkiem transformacji ustrojowej), a w latach 2014-17 radykalizację wywoływał strach przed czynnikami zewnętrznymi (w tym: agresywna polityka Federacji Rosyjskiej, terroryzm islamski kojarzony z pozaeuropejską imigracją), to w 2021 r. motorem radykalizacji stały się inne czynniki: (1) wewnętrzna polaryzacja polityczna, (2) pandemia i związane z nią restrykcje. Stwierdzić trzeba, że procesy radykalizacji sygnalizowane w poprzednim Raporcie w roku 2021 uległy pogłębieniu.

W przypadku polaryzacji konflikt rozgrywa się nie tylko między zwaśnionymi ugrupowaniami politycznymi. Poprawa statusu niektórych grup odbierana jest przez inne jako zagrożenie własnego statusu; dotyczy to zarówno sfery materialnej (biedni/bogaci) jak niematerialnej (tradycjonaliści/progresiści). W rezultacie wrogością obdarzani są nie tylko politycy, ale całe grupy społeczne (zawodowe, światopoglądowe, wiekowe, terytorialne itd.) kojarzone z poparciem dla przeciwnika. Niechęć do rządu, do rządzącej orientacji politycznej przenoszona jest na inne instytucje państwowe, zwłaszcza na Policję. Zjawiska te mogą zwiększyć deficyt zaufania społecznego do poziomu anarchizującego państwo, paraliżującego funkcjonowanie jego aparatu. Coraz bardziej realny staje się scenariusz, że bez względu na rzeczywisty wynik następnych wyborów strona przegrana nie uzna ich legalności. Nietrudno dostrzec, że sytuacja taka może zostać z łatwością wykorzystana przez przeciwników zewnętrznych.

b. Radykalizm polityczno-społeczny w Polsce w latach 2021-2022

Polaryzacja prowadzi do sytuacji, w której brak jest jakichkolwiek instytucji, symboli czy wartości mogących łączyć całe społeczeństwo lub przynajmniej jego znaczącą większość. Każda ze stron konfliktu ma własne media oraz naukowe i moralne autorytety, co pozwala im funkcjonować w układach zamkniętych. Strony konfliktu są wręcz zainteresowane podsycaniem radykalizacji, gdyż utrzymuje to wysoki poziom mobilizacji własnych zwolenników, a zarazem pozwala przerzucać odpowiedzialność za konflikt na przeciwnika. Przemocowe zachowania własnych ekstremistów są przemilczane, bagatelizowane (na ogół opisywane przy użyciu innego języka niż takie same czyny przeciwników), a nawet usprawiedliwiane („nie pochwalam, ale rozumiem"), choć – co trzeba zaznaczyć – wciąż nie pochwalane. Główne obozy polityczne stały się zakładnikami własnych ekstremistów, którzy są niezbędni dla zmajoryzowania przeciwnika. Rezultatem była rosnąca w 2021 r. liczba incydentów z użyciem przemocy (np. ataki typu wandalskiego na biura poselskie).

Ekstremiści jako siła odśrodkowa stają się jednak niesterowalni, co zaczyna być zagrożeniem dla spójności głównych sił politycznych. Skłonność do stosowania przemocy zaczyna być przenoszona nawet do własnego środowiska (vide starcia między różnymi grupami lewicowych ekstremistów w marcu 2021 r. w Poznaniu (Kolektyw PyRa vs Rozbrat) – lub w Warszawie na ul. Wilczej w grudniu 2021 r. (squat Syrena i kolektyw Stop Bzdurom vs squat Przychodnia). Zjawisko „sztafety ekstremizmów" (pojawiania się coraz radykalniejszych frakcji) prowadzi do fragmentaryzacji sceny politycznej, swego rodzaju „rozmnażania przez podział i pączkowanie". Doszło do odrodzenia wygasłych, zdawałoby się, form ekstremizmu, jak panslawistyczny antysemicki nacjonalizm czy stalinowski wariant komunizmu. Przetrwały one w przestrzeni wirtualnej, podtrzymywane niekiedy poprzez trolling, by w sprzyjających warunkach zebrać zwolenników i wyjść w przestrzeń fizyczną (wcześniej podobne zjawisko można było dostrzec w przypadku amerykańskiej Alt-Right).

Dalsze pogłębianie tych trendów może doprowadzić do „bałkanizacji" polskiej sceny politycznej, zapewniając ekstremistom niewspółmiernie dużą rolę. Nazwać można to „efektem centryfugi", gdy erozji politycznego centrum towarzyszy wzrost znaczenia ekstremistów, punkt ciężkości sceny politycznej przesuwa się na jej obrzeża. W warunkach skrajnej polaryzacji ekstremiści marginalizują, a nawet eliminują umiarkowanych we własnym obozie (historycy mówią o tym, że „rewolucja pożera własne dzieci").

Specyficzny charakter ma ruch protestu wobec restrykcji pandemicznych, potocznie zwany ruchem antyszczepionkowym lub (bardziej poprawnie) koronasceptycznym.

Jest to czołowy przedstawiciel rosnącego w ostatnich latach segmentu ekstremizmu, jaki stanowią wyznawcy teorii spiskowych i/lub paranaukowych. Z ruchem koronasceptycznym łączy się ściśle – poprzez pseudonaukową teorię „pól torsyjnych" – ruch anty5G, podnoszący zagrożenia związane z rozwojem nowych technologii. Również jego agitacja prowadzić może do stosowania przemocy (na ogół sabotażu). Ze względu na amorficzną strukturę tych środowisk, aktywnych głównie w Internecie, stanowią one dogodne środowisko do prowadzenia operacji dezinformacyjnych i destabilizacyjnych (choć Raport PTBN „Zagrożenia informacyjne dla infrastruktury krytycznej na przykładzie technologii 5G" z 2022 r. zaznacza, że „Uzyskane dane nie są również wystarczające do stwierdzenia tego czy zjawisko miało charakter nieautentycznej ingerencji w przestrzeń informacyjną np. przez podmiot zagraniczny, działający na zlecenie obcych służb specjalnych").

Ruch „antyszczepionkowy" ma charakter ogólnoświatowy, ale zauważalny głównie w krajach szeroko pojętego Zachodu, związany z radykalnymi organizacjami prawicowymi (choć czasem angażują się weń też ekstremiści lewicowi). Działalność koronasceptyków polega nie tylko na dezinformacji, rozsyłaniu fake newsów w sieci, ale także na aktach przemocy, wandalizmie, groźbach wobec polityków i lekarzy, manifestacjach i pikietach. Wraz ze wzrostem aktów kryminalnych tych grup w państwach europejskich sugeruje się uznanie ich za organizacje przestępcze a nawet terrorystyczne. Następuje również proces upolitycznienia postulatów ruchu antyszczepionkowego, przez skrajne odłamy sceny politycznej. W Polsce to zjawisko, choć związane jest z radykalną prawicą, w zasadzie pozostaje w opozycji wobec obozu rządzącego, kontestując nawet najłagodniejsze przejawy polityki antycovidowej, a nawet samą realność pandemii.

Działalność radykalnych ugrupowań „antyszczepionkowych" w Polsce w 2021 r. gwałtownie wzrosła. Postulaty przez nie głoszone dotyczyły głównie: zniesienia obostrzeń lub ich niewprowadzania (lockdownu, noszenia maseczek, dystansu społecznego, funkcjonowanie tzw. „paszportu covidowego") oraz niestosowania szczepionek przeciw Covid-19 lub niewprowadzania ich obowiązkowości. Niekiedy łączą się z tym hasła antysemickie i panslawistyczne. Organizacje antyszczepionkowe działają w oparciu o strategię oporu niekierowanego: to luźna siec lokalnych grup pozbawiona jednolitego przywództwa. Większość jego uczestników nie stosuje przemocy, ale kolportuje w Internecie fake newsy dotyczące pandemii oraz zaprzecza dorobkowi współczesnej medycyny, tworząc atmosferę ideologicznego wsparcia dla ekstremistów i głosicieli teorii spiskowych.

Radykalna część ruchu koronasceptycznego stosuje jednak manifestacje siły (np. antyszczepionkowcy w paramilitarnych uniformach zorganizowali 4 sierpnia 2021 r.

manifestację zniechęcającą do szczepień na rynku w Poznaniu), przemoc werbalną (groźby wobec pracowników służby zdrowia i instytucji państwowych), a nawet fizyczną (podpalenia, dewastacje). Agresja zaczyna się od mowy nienawiści na portalach internetowych czy nawoływania do działań antypaństwowych, a kończy na aktach przemocy fizycznej. W grudniu 2021 r. do polityków różnych opcji politycznych deklarujących poparcie obostrzeń związanych z pandemią wysyłano listy z pogróżkami i oskarżeniami o zdradę stanu. Były one podpisane przez Suwerena Narodu Polskiego, Polski Trybunał Narodowy i Komitet Ścigania Zbrodni Przeciwko Narodowi Polskiemu. „Wyroki śmierci" i groźby pozbawienia życia otrzymali prezydenci m.in. Białegostoku, Gdańska, Wałbrzycha, Wrocławia. Antyszczepionkowcy grozili śmiercią szefowi PSL i rzecznikowi ministerstwa zdrowia na ulicach Karpacza w trakcie XXX Forum Ekonomicznego. Prawdopodobnie koronasceptycy odpowiedzialni są również za kilkadziesiąt alarmów bombowych w szkołach i urzędach na terenie całej Polski. 8 sierpnia 2021 r. została wysłana drogą mailową groźba wysadzenia Term Maltańskich i aquaparku w Poznaniu (ewakuowano 1800 osób), ze względu na otwarcie kas dla zaszczepionych co miało rozładować kolejki przed wstępem do obiektu.

W lipcu 2021 r. w Grodzisku Mazowieckim antyszczepionkowcy próbowali siłą wedrzeć się do punktu szczepień. Gdy to im się nie udało ze względu na działania ochrony, wywiązała się awantura, w której dwie osoby zostały ranne. Napastnicy krzyczeli „Mordercy, ludobójcy!". Nastąpiła próba zablokowania radiowozu, zaatakowano karetkę. Dwie osoby zostały zatrzymane pod zarzutami naruszenie nietykalności cielesnej funkcjonariusza oraz znieważenia i kierowania gróźb karanych wobec policjantów. W sierpniu 2021 r. grupa 16 osób zaatakowała w Gdyni „szczepieniobus": został on okrążony a wobec służby medycznej użyto wyzwisk takich jak „mordercy" czy „dzieci doktora Mengele". W tym samym miesiącu członkowie Ogólnopolskiego Stowarzyszenia Wiedzy o Szczepieniach STOP NOP zakłócili w Poznaniu piknik laktacyjny zorganizowany w Szpitalu Ginekologiczno-Położniczym, gdyż miał tam zostać otwarty punkt szczepień. Grupa około 30 osób z transparentami i megafonami uczestniczyło w zgromadzeniu, po czym kilka osób wdarło się na teren szpitala i jego zabudowań. Piknik został zakończony przedwcześnie. Grupa członków Bydgoskiego Kamractwa Rodaków wtargnęła 26 lipca w Aleksandrowie Kujawskim do Domu Dziecka domagając się zaprzestania szczepień podopiecznych ośrodka („kamraci" stanęli „w obronie praw ojca", którego dwójka dzieci przebywała w ośrodku).

Inną kategorię stanowią przypadki spontanicznej przemocy indywidualnej – wyzwisk, gróźb a nawet pobić osób domagających się założenia maseczki: w kwietniu 2020 r. w supermarkecie w Lesznie, w sierpniu 2020 r. przed supermarketem w Gdańsku i w Bydgoszczy, we wrześniu 2020 r. atak nożem w sklepie w Łodzi, w październiku

2020 r. pobicie motorniczej Tramwajów Warszawskich, w listopadzie 2020 r. w Łodzi, w styczniu 2021 r. napaści w supermarkecie w Warszawie i trolejbusie w Gdyni, w marcu 2021 r. pobicie strażnika na Jasnej Górze, w maju 2021 r. pobicie kierowcy autobusu linii Grodziec-Opole, w czerwcu 2021 r. pobicie pasażera w autobusie w Bydgoszczy, w listopadzie 2021 r. pobicie pracownicy agencji pocztowej w Zabrzu, w grudniu 2021 r. pobicie policjanta i strażnika miejskiego w Zamościu oraz pracownika apteki w Zgorzelcu.

Sytuacja uległa istotnej zmianie w 2022 r. Zakończenie restrykcji związanych z pandemią zmniejszyło dynamikę ruchu antyszczepionkowego, przy którym pozostał tylko najbardziej zdeterminowany rdzeń aktywistów. Zarazem wybuch wojny na Ukrainie doprowadził do konsolidacji zdecydowanej większości społeczeństwa na platformie antyrosyjskiej. Nie pojawiły się przy tym nowe gwałtowne ogniska konfliktu społecznego porównywalne z wyrokiem Trybunału Konstytucyjnego w sprawie aborcji w październiku 2020 r. Zjawiska te osłabiły potencjał ekstremizmu politycznego.

Ekstremizm jednak nie zniknął. Przede wszystkim nie zanikły – nawet w obliczu wojny – antagonizmy międzypartyjne. Przejawem ich utrzymywania się w 2022 r. są (niegroźne na ogół) ataki na biura poselskie i ich pracowników. Działania ekstremistów na ogół ograniczają się do wzajemnych konfrontacji i sporadycznych aktów sabotażu (lub raczej wandalizmu – jak niszczenie banerów deweloperskich w Łodzi w lutym 2022 r. czy bankomatu i biletomatu we Wrocławiu w grudniu 2021 r.). Niekiedy jednak związek ekstremizmu ze stosowaniem przemocy prowadzi do apolitycznych zbrodni (przypadek sympatyka antify Mikołaja J. z Inowrocławia; znane są też związki grup neonazistowskich z przestępczością zorganizowaną).

Zagrożenie ekstremizmem może znacząco zwiększyć się wraz z pogarszaniem sytuacji gospodarczej, zwłaszcza jeśli obniżenie stopy życiowej zostanie skojarzone z pomocą dla Ukrainy i napływem uchodźców z tego kraju. Na tej płaszczyźnie możliwa jest konsolidacja i dynamizacja opozycji antysystemowej.

1.7. Zagrożenia bezpieczeństwa cybernetycznego

Zagrożenia o charakterze cybernetycznym, w tym również cyberterrorystycznym mogą dzisiaj sięgnąć niemal każdej jednostki organizacyjnej i każdego państwa czy organizacji międzynarodowej. Biorąc pod uwagę zagrożenia atakami cyberterrorystycznymi można zidentyfikować najwyższą podatność poniższych systemów:

- systemy wojskowe,
- systemy przedsiębiorstw,
- systemy należące do obiektów infrastruktury krytycznej – tzn. bankowo-finansowe, energetyczne, telekomunikacyjne, dostarczania wody, transportu, służb do działań w sytuacjach wyjątkowych, zasobów przechowujących informacje ważne dla bezpieczeństwa państwa.

Europejska Agencja ds. Cyberbezpieczeństwa – ENISA opracowała kolejną wersję raportu o zagrożeniach dla cyberbezpieczeństwa. Analiza dotyczy okresu między kwietniem 2020 a lipcem 2021 r. i została opracowana na podstawie otwartych źródeł (artykuły medialne, opinie ekspertów, analizy incydentów, raporty), a także na podstawie wywiadów z członkami grupy roboczej ENISA ds. cyberzagrożeń. W raporcie wyróżniono 9 najpoważniejszych zagrożeń dla systemów teleinformatycznych: ransomware (ataki z użyciem złośliwego oprogramowania połączone z blokowanie danych z żądaniem okupu, ataki wykorzystujące złośliwe oprogramowanie do zaszyfrowania danych z żądaniem okupu, z możliwością eksfiltracji danych); malware (złośliwe oprogramowanie, m.in.. wykradające dane czy ustanawiające stały dostęp adwersarza do zainfekowanych stacji roboczych); kradzież kryptowalut; zagrożenia związane z pocztą elektroniczną (phishing, spearpshishing, eksfiltracja korespondencji); zagrożenia dla dostępności i integralności danych (np. ataki typu DDoS); dezinformacja/celowe wprowadzanie w błąd; ataki na łańcuchy dostaw; inne (błędy ludzkie, nieprawidłowe konfiguracje systemów, wypadki mające wpływ na systemy informatyczne). W analizowanym okresie zaobserwowano następujące trendy:

1. Oprogramowanie typu ransomware jest najpoważniejszym zagrożeniem w raportowanym okresie.

2. Rośnie liczba cyberataków (przede wszystkim ransomware) na infrastrukturę krytyczną (przede wszystkim placówki służby zdrowia, służby ratunkowe oraz przedsiębiorstwa z systemów transportu i energii).

3. Przeprowadzanie cyberataków stało się usługą, na którą jest popyt, co powoduje, że ten rodzaj działalności staje się dochodowy, rośnie więc podaż i powstają podmioty oferujące tego typu usługi. Ponadto hakerzy stale podnoszą swoje kwalifikacje, stosują nowe lub nietypowe języki programowania.

4. Upowszechniają się kryptowaluty, które są środkiem płatniczym w nielegalnych transakcjach związanych ze zleceniem ataków bądź płaceniem hakerowi okupu; zarazem zwiększyła się liczba ataków typu cryptojacking polegających na wykorzystywaniu

komputera nieświadomej ofiary do generowania kryptowalut. Liczba infekcji związanych z cryptojackingiem osiągnęła rekordowo wysoki poziom w pierwszym kwartale 2021 r. w porównaniu z ostatnimi latami.

5. Wątki związane z pandemią COVID-19 są dominującą przynętą w przypadku ataków na skrzynki e-mailowe. Ponadto, w latach 2020 i 2021 zaobserwowano wzrost liczby niezłośliwych incydentów niewynikających z działań złośliwych, ponieważ pandemia COVID-19 stała się mnożnikiem błędów ludzkich i błędnych konfiguracji systemu do tego stopnia, że większość naruszeń w 2020 r. była spowodowana takimi właśnie błędami. Cyberataki skierowane na łańcuchy dostaw mogą mieć katastrofalne skutki, dlatego ENISA opracowała osobny raport dotyczący tej kategorii zagrożeń.

Kluczowym dokumentem obrazującym stan cyberbezpieczeństwa w Polsce jest *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku* opracowany przez Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV.

W roku 2021 Zespół CSIRT GOV odnotował 762.175 zgłoszeń dotyczących potencjalnego wystąpienia incydentu teleinformatycznego, z czego 26.899 zgłoszeń zakwalifikowano jako faktyczne incydenty.

Tabela 1. Liczba zgłoszonych incydentów

ROK	ZGŁOSZONE INCYDENTY	FAKTYCZNE INCYDENTY
2021	762.175	26.899
2020	246.107	23.309
2019	226.914	12.405
2018	31.865	6.236
2017	28.281	5.819

Źródło: opracowanie własne na podstawie danych z Raportów z 2020 i 2021 r.

Wysoka ilość zgłoszeń w latach 2019-2021 jest wynikiem wejścia w życie przepisów ustawy o krajowym systemie cyberbezpieczeństwa, nakładającej obowiązek raportowania incydentów, z drugiej strony globalna tendencja wskazuje na coroczny przyrost tego typu zdarzeń. Ważnym czynnikiem było rozpoczęcie pandemii COVID-19 i przejście wielu przedsiębiorstw w zdalny tryb pracy. Największa liczba faktycznych

incydentów w 2020 r. (7.957) została zarejestrowana w II kwartale 2020 r., czyli zbiegła się z początkiem tzw. lockdownu. Choć ograniczenia związane z pandemią już się skończyły, to wiele firm na stałe przeszło w zdalny lub hybrydowy tryb pracy. Z kolei trzykrotny wzrost liczby zgłoszeń w 2021 r. w stosunku do roku 2020 wynika z dużej wykrywalności zdarzeń przez ciągle aktualizowany system ARAKIS GOV.

Gdy przyjrzeć się rodzajom ataków, to w roku 2021 najwięcej incydentów zostało sklasyfikowanych wśród trzech następujących kategorii: „wirus" (24.171 incydentów), „podatność" (1.148), „socjotechnika" (904). Kategoria „podatność" definiowana jest jako: „słabość systemu teleinformatycznego, błędy konfiguracyjne oraz brak odpowiedniej polityki bezpieczeństwa, związanej z aktualizacją oraz weryfikacją poprawnie wdrożonych rozwiązań teleinformatycznych" (*Raport*… s. 17). Incydenty z kategorii „socjotechnika" to kampanie phishingowe, podszywanie się oraz ataki z zakresu tzw. inżynierii społecznej, czyli wykorzystanie różnych form manipulacji w celu nakłonienia użytkownika do określonego działania. Najczęściej mają na celu wyłudzenie poufnych informacji, zainfekowanie komputera złośliwym oprogramowaniem bądź nakłonienie użytkownika do określonych działań, np. ujawnienie loginu i hasła, dokonanie przelewu, udzielenie dostępu do systemu teleinformatycznego. W tej kategorii najwięcej incydentów dotyczyło podszywania się pod witryny internetowe wykorzystujące wizerunek podmiotu, często mających na celu wyłudzenie środków finansowych bądź danych logowania.

Najczęściej występującą formą ataków phishingowych były maile, których nadawcy podszywali się pod dział pomocy (helpdesk), administratorów IT, bądź wykorzystywali logotypy instytucji administracji publicznej lub operatorów IK, aby dodatkowo uwiarygodnić korespondencję. Wiadomość była tak sformułowana, by zachęcić odbiorcę do otworzenia zawartego w niej linka i wprowadzenia danych logowania do poczty elektronicznej. Najczęściej właściciel adresu informowany był o problemach technicznych, alarmie, zapełnieniu skrzynki mailowej czy niezbędnej aktualizacji, w każdym z tych przypadków koniecznym było natychmiastowe zalogowanie się do poczty. Celem tych kampanii było pozyskanie danych uwierzytelniających do skrzynek administracji publicznej (login, hasło) i przejęcie zawartych w nich informacji, a także uzyskanie możliwości wysyłania z nich korespondencji. Skutki mogły być poważne, jak w przypadku przejęcia przez hakerów konta e-mailowego szefa Kancelarii Prezesa Rady Ministrów Michała Dworczyka w czerwcu 2021 r.

W 2020 r. w atakach phishingowych wykorzystywano ponadto elementy systemu identyfikacji wizualnej firm kurierskich (np. Poczta Polska, InPost) oraz operatorów telekomunikacyjnych (np. Orange i Play), w 2021 proceder podszywania się pod operatora

Play trwał nadal. Nadawcy korespondencji podszywali się pod te podmioty i wysyłali maile z informacją o niezapłaconej fakturze, oczekującej przesyłce, konieczności dokonania dopłaty za usługi kurierskie/pocztowe. Celem tych ataków była próba infekcji złośliwym oprogramowaniem lub pozyskanie danych autoryzacyjnych do serwisów bankowości elektronicznej i wykradanie środków finansowych.

Epidemia COVID-19, niepewność, strach, a także konieczność szybkiego przeorganizowania biur i przejścia na pracę zdalną były czynnikami wykorzystywanymi przez cyberprzestępców. Do ataków wykorzystywano interaktywną mapę rozprzestrzeniania się wirusa, fikcyjne maile od Światowej Organizacji Zdrowia (WHO), wiadomości z ofertami firm oferujących środki ochrony osobistej (maseczki, kombinezony) czy fikcyjne zbiórki pieniędzy. Celem takich ataków było zainfekowanie systemu lub wykradzenie danych uwierzytelniających. W 2021 r. nadal wykorzystywano motyw pandemii COVID-19, w kampaniach phishingowych wykorzystywano podmioty takie jak Główny Inspektorat Sanitarny i firmę Orlen S.A., pojawiła się też kampania phishingowa polegająca na przesyłaniu wiadomości pomiędzy organy administracji publicznej oraz operatorów IK. Mail pochodził z adresu vddoming@sct.gob.mx., a celem było wykradzenie danych logowania.

W 2020 r. wśród najczęściej atakowanych sektorów na pierwszym miejscu znalazły się incydenty teleinformatyczne dotyczące urzędów państwowych – 8.356 incydentów. Ponadto incydenty odnotowano w systemach teleinformatycznych infrastruktury krytycznej (2.626 przypadków) oraz instytucji publicznych (2.518). Co ważne, w 2020 r. nastąpił znaczący wzrost liczby incydentów w urzędach państwowych (o 118%), u operatorów infrastruktury krytycznej (o 283%) oraz służbach i wojsku (311%) w stosunku do roku 2019. Rok 2021 charakteryzował się zwiększoną liczbą cyberataków na systemy teleinformatyczne operatorów IK (9.196 zarejestrowanych incydentów); tym samym niezbędne dla funkcjonowania państwa i społeczeństwa zakłady, obiekty i usługi stały się najczęściej atakowanymi podmiotami. Na drugim miejscu pod względem liczby ataków znalazły się systemy instytucji (7.203 zgłoszenia), na kolejnym – urzędów państwowych 5.563 incydenty. Pozostałe kategorie podmiotów to: ministerstwa (3.056), służby i wojsko (1.237), pozostałe (644).

ARAKIS-GOV jest systemem wczesnego ostrzegania o zagrożeniach występujących na styku sieci wewnętrznej z Internetem. W 2021 r. w sieciach teleinformatycznych podmiotów uczestniczących w projekcie ARAKIS 3.0 GOV odnotowano 1.758.708.908 przepływów, co przełożyło się na 3-366-360 alarmów wygenerowanych przez system. Wśród zanotowanych alarmów 1.170.136 miało priorytet „pilny", tzn. wymagało natychmiastowej reakcji na zagrożenie ze strony administratorów, ponieważ niosło duże ryzyko przełamania zabezpieczeń.

System umożliwia klasyfikację alarmów. W 2020 r. 32,35% wszystkich alarmów stanowiły alarmy typu 1 („komunikacja ze złośliwych adresów") i wynikały z prób nawiązywania komunikacji z adresami IP lub domenami uznanymi za złośliwe bądź mogącymi stanowić zagrożenie. Najwięcej, bo 49,26 % alarmów to typ 2 („skanowanie"); najwięcej tego rodzaju incydentów zostało zanotowanych w instytucjach zdefiniowanych jako infrastruktura krytyczna (31,81%). Alarmy typu 3 – „wykryte znane ataki", stanowiły 4,94% zgłoszeń, typu 4 -„wykryte nieopisane ataki" 10,04%, a najniższe wartości zanotowano w ramach typu 5 („infekcje wewnętrzne", identyfikowane na podstawie niepożądanej komunikacji z elementami sieci objętymi systemem ARAKIS 3.0 GOV) i wyniosły 0,21 %.

Najwięcej przepływów wygenerowano z Federacji Rosyjskiej (25% przepływów) oraz USA (15% przepływów); 12% przepływów pochodziło z adresów należących do Polski. Na dalszych miejscach pojawiły się Chiny, Wielka Brytania, Francja, Niemcy ze wskazaniami na poziomie 5-7 %.

W zestawieniu cyberzagrożeń nie można pominąć kampanii mających na celu dezinformację czy celowe wprowadzanie w błąd. Cyfryzacja prasy i ciągły wzrost popularności mediów społecznościowych powodują, że coraz więcej osób czerpie wiedzę i informacje z Internetu, co sprzyja kampaniom dezinformacyjnym i rozprzestrzenianiu się tzw. fake newsów. Kampanie, których celem jest rozprzestrzenianie fałszywych informacji, są częścią ataków hybrydowych i wspierają inne zagrożenia, wywołując nieufność i zamieszanie, spadek zaufania do instytucji demokratycznych i dezintegrację społeczeństw. Niepokoić może relatywnie wysoka liczba ataków wykorzystujących socjotechnikę, ponieważ najczęściej adresowane są one do szeregowych pracowników, którzy posiadają niewielką wiedzę na temat cyberbezpieczeństwa i rzadko są szkoleni w zakresie metod przeprowadzania cyberataków i odporności na nie. Podnoszenie świadomości pracowników (przede wszystkim pracowników IK, bo ten sektor atakowany jest najczęściej) powinno być priorytetem w zakresie szkoleń.

Istotnym elementem zapewnienia bezpieczeństwa systemów i sieci teleinformatycznych organizacji jest również stała aktualizacja oprogramowania elementów wstawionych do sieci Internet. Eksploitacja podatności oprogramowania może nieść za sobą znaczące skutki, takie jak: eksfiltracja danych z systemów, infekcja ransomware czy wykorzystanie skompromitowanego systemu do dalszych ataków. Podatność biblioteki Log4j, wykryta w 2021 r., została uznana za jedną z najbardziej krytycznych podatności w ostatnim czasie, a konsekwencją jej wykorzystania mogło być zdalne wykonanie kodu z uprawnieniami podatnej aplikacji. Podatności Microsoft Exchange, również

zidentyfikowane w 2021 r., mogły skutkować kompromitacją zaatakowanych serwerów. Wskazane jest, aby administratorzy IT stale podnosili swoje kompetencje i poszerzali wiedzę w zakresie wykorzystywanego w organizacji oprogramowania.

1.8. Charakterystyka zagrożeń na morzach i oceanach

a. Zagrożenia terroryzmem obywateli polskich na międzynarodowych akwenach morskich

Historia pokazuje, że Polacy jako członkowie załogi oraz pasażerowie doświadczyli już terroryzmu. Nie można także zapominać o nieudanych próbach uprowadzenia, gdy polskie załogi umiejętnie przeczekały lub skutecznie odparły piracką agresję, m.in. MV *ESL Australia* (20 maja 2020 r.) i MV *Port Gdynia* (21 grudnia 2020 r.). Ostatni tego typu incydent miał miejsce 13 grudnia 2021 r. na wodach Zatoki Gwinejskiej, gdzie doszło do uprowadzenia 7 osób z załogi kontenerowca MV *Tonsberg*, w tym obywatela RP. 17 stycznia 2022 r. uwolniono Polaka i towarzyszących mu członków załogi.

Warto w tym miejscu zaznaczyć, że najnowsze dane International Maritime Bureau wskazują na znaczny spadek porwań dla okupu (ze 135 w roku 2020 do 57 w roku 2021). Mimo to według amerykańskiego Office of Naval Intelligence tylko od stycznia do lutego 2022 r. odnotowano 7 incydentów w Zatoce Gwinejskiej oraz 11 Azji w Południowo-Wschodniej.

b. Charakterystyka zagrożeń na polskich obszarach morskich

Bezpieczeństwu RP zagraża również terroryzm morski. Zarówno przeciwdziałanie mu, jak i zwalczanie jego skutków, nie powinny być traktowane mniej poważnie w stosunku do innych bezpośrednich zagrożeń. Proces globalizacji dynamizuje rozwój międzynarodowego handlu morskiego, wymusza wzrost liczby szlaków morskich, a przede wszystkim wzrost częstotliwości kursów statków przewożących towary, czemu zagraża morska przestępczość. Rosnące zapotrzebowanie energetyczne zwiększa liczbę platform wydobywczych, których obiekty i instalacje są szczególnie wrażliwe na akty terroryzmu. Naturalną konsekwencją prężnego przyrostu ruchu pasażerskiego, sukcesywnego zwiększania obrotów i powierzchni portów jest znaczny wzrost przepływu osób w tym rejonie. Ponadto specyfiką polskich portów morskich jest ich zespolenie urbanistyczne z aglomeracjami miejskimi, co wymaga doskonalenia procedur ochronnych na wypadek zagrożenia dla bezpieczeństwa. Porty morskie, stocznie, obiekty administracji państwowej i samorządowej oraz miejsca znacznych skupisk ludzi (dworce,

ciągi komunikacyjne, centra handlowe) – wszystko tworzy niejako całość. Usytuowanie istotnych dla RP obiektów portowych stanowi bezapelacyjnie czynnik ułatwiający działania potencjalnym terrorystom.

Obiektami morskiej infrastruktury krytycznej mogą być porty, miejsca bazowania, terminale gazowe, terminale pasażerskie, rurociągi, platformy wiertnicze, kable podmorskie i inne konstrukcje hydrotechniczne. Należy mieć na uwadze, że ingerencja w ich sprawne funkcjonowanie niesie za sobą widmo załamania sytemu transportu towarów istotnych z punktu widzenia funkcjonowania państwa bądź np. katastrofy ekologicznej, a w rezultacie strat ekonomicznych. Nie można zapominać też o zachwianiu pozycji RP na arenie międzynarodowej. Stąd też obiekty morskiej infrastruktury krytycznej wymagają należytej uwagi, nadzoru i kontroli.

Wyzwaniem w obszarze bezpieczeństwa morskiego RP pozostaje rozbudowa infrastruktury logistycznej umożliwiającej zwiększanie zdolności w zakresie wsparcia przez Państwo – Gospodarza (*Host Nation Support*, HNS) oraz wysuniętą morską obecność NATO w rejonie Morza Bałtyckiego i rozszerzającą przestrzeń do pogłębiania współpracy NATO z UE.

Polskie porty cechuje duży potencjał. Korzystne nadmorskie położenie geograficzne Polski na skrzyżowaniach istotnych korytarzy transportowych rodzi wiele wyzwań i szans, niosąc jednak za sobą również zagrożenia. Sprawna, bezpieczna i atrakcyjna infrastruktura portowa ma zasadnicze znaczenie dla kryterium konkurencyjności obiektu. Dynamiczny rozwój, rozbudowa i modernizacja dotyczą nie tylko nabrzeży przeładunkowych, torów podejściowych, baz czy choćby terminali, ale i poprawy dostępności drogowo-kolejowej do poszczególnych obiektów (drogi samochodowe, linie kolejowe, drogi wodne śródlądowe). W *Strategii Zrównoważonego Rozwoju Transportu do 2030 roku* zaakcentowano kluczową rolę portów morskich jako węzłowych punktów wpływających na sprawność i wydajność krajowego układu transportowego, natomiast poprawa dostępu do portów (zarówno od strony lądu, jak i od strony morza) jawi się jako jeden z podstawowych celów operacyjnych przywołanej *Strategii*. Modernizacja i rozbudowa morskiej infrastruktury transportowej (zarówno liniowej, jak i punktowej) musi spełniać normy krajowe i unijne, również w zakresie ochrony środowiska morskiego i nadmorskiego. Niemniej istotny, kiedy mówimy o morskiej infrastrukturze krytycznej, pozostaje morski system łączności, który wymaga sprawowania szczególnej pieczy w obliczu współczesnych zagrożeń w cyberprzestrzeni. Inwestycje ześrodkowane wokół morskich portów o podstawowym znaczeniu dla gospodarki narodowej mają wspomóc osiągnięciu przez nie wszystkie statusu hubów, tj. portów komasacyjno-rozdzielczych.

Na liście głównych portów morskich o fundamentalnym znaczeniu dla gospodarki narodowej znajdują się: port Gdańsk, port Gdynia, port Szczecin i port Świnoujście. Obiekty te wraz z całą infrastrukturą rozlokowane są w ciągu głównych europejskich szlaków transportowych i w strategii rozwoju transportu UE, stanowiąc istotne ogniwa Transeuropejskiej Sieci Transportowej (ang. *Trans-European Transport Networks* – TEN-T).

Z uwagi na zajmowaną powierzchnię oraz zróżnicowanie terenu Port Gdańsk jest podzielony na dwa kluczowe obszary: port wewnętrzny (ciągnący się wzdłuż Martwej Wisły oraz kanału portowego) oraz port zewnętrzny (umiejscowiony na wodach Zatoki Gdańskiej). W Gdańsku znajduje się jedyny w Polsce morski terminal przeładunkowy ropy naftowej oraz jeden z największych terminali przeładunku produktów jej rafinacji. W 2021 r. przeładował 17 898 mln ton ropy naftowej i paliw (o ponad 6% więcej niż w rekordowym 2019 r.). Co istotne, w kwestii dywersyfikacji surowców energetycznych ok. 2/3 dostaw ropy naftowej do Polski odbywa się drogą morską, w większości z kierunków innych niż wschodni. Baza przeładunku paliw płynnych Naftoport dysponuje możliwościami odbioru – w sytuacji kryzysowej – nawet 60 mln ton ropy rocznie.

Z kolei port w Gdyni notuje rekordowe wzrosty obrotu towarów ro-ro, czemu sprzyja usytuowanie w jednym z Korytarzy Sieci Bazowej TEN-T – Bałtyk-Adriatyk, którego przedłużeniem jest łącząca Gdynię ze Szwecją Autostrada Morska Gdynia-Karlskrona. Dalszy dynamiczny rozwój portu implikuje konieczność budowy nowych terminali głębokowodnych. Do 2030 r. planuje się budowę 4 nowych nabrzeży i przebudowę już istniejących oraz stworzenie rezerwy pod budowę terminala LNG-FSRU i rozbudowę terminala przeładunku paliw płynnych. Program budowy pływającego terminalu regazyfikacyjnego skroplonego gazu ziemnego (ang. *Floating Storage Regasification Unit* – FSRU) zakłada usytuowanie w Zatoce Gdańskiej instalacji nie tylko zdolnej do wyładunku, procesowego składowania i regazyfikacji LNG, ale także do świadczenia innych dodatkowych usług, m.in. umożliwiających efektywny przesył gazu z rejonu Trójmiasta do całej Polski. To kolejny w ostatnim czasie, obok budowy gazociągu Baltic Pipe, projekt z zakresu dywersyfikacji dostaw gazu.

Niemniej istotnym kompleksem o znaczeniu strategicznym w tej materii pozostaje usytuowany na polskim wybrzeżu zachodnim gazoport w Świnoujściu. Bezapelacyjnym atutem portu w Świnoujściu jest jego usytuowanie – to najdalej wysunięty w kierunku zachodnim port polski, przez który prowadzi najkrótsza droga łącząca Europę Środkowo-Wschodnią ze Skandynawią. Ulokowany w tym rejonie port zewnętrzny z terminalem LNG to inwestycja kluczowa z punktu widzenia bezpieczeństwa energetycznego RP (dywersyfikacja dostaw gazu). Pierwsza dostawa komercyjna skroplonego gazu ziemnego miała miejsce w czerwcu 2016 r. Od tego czasu odnotowano ponad 150 dostaw, w rezultacie

czego do Polski dotarło droga morską 27,2 mln m^3 LNG, zaś łączny wolumen LNG po procesie regazyfikacji przekroczył 16 mld m^3. Do 2030 r. przewiduje się budowę 3 nowych nabrzeży. Z kolei w pobliskich Policach Grupa Azoty kontynuuje budowę kompleksu petrochemicznego, który wespół z terminalem LNG w Świnoujściu i przesyłem gazu przez rurociąg podmorski na należącym do Norwegii szelfie Morza Północnego będzie stanowił potężne zaplecze do odbioru i transportu surowców drogą morską przez Bałtyk. Rurociąg Baltic Pipe będzie bramą dostępową do terminalu LNG dla Szwecji i Danii, co pozwoli tym skandynawskim krajom na dywersyfikację źródeł dostaw gazu spoza Europy.

Z uwagi na nasze położenie geopolityczne problem przestępczości morskiej jest niezwykle istotny. Rozwinięta turystyka nadmorska oraz gazoport czy naftoport czynią nasz kraj potencjalnym celem terrorystów. Atak terrorystyczny na wspomniane porty pozwoliłby terrorystom zdobyć rozgłos. Segmentem szczególnie wrażliwym jest infrastruktura krytyczna systemu energetycznego. Skuteczny atak na jej obiekty stwarza możliwość windowania cen surowców energetycznych jak również wywołania znacznej katastrofy ekologicznej przez wyciek ropy lub materiałów ropopochodnych. Gazoport w Świnoujściu plasuje się jako atrakcyjny cel ataku terrorystycznego lub dywersyjnego z uwagi na to, iż stanowi on infrastrukturę krytyczną o znaczeniu europejskim, a zarazem system transportu LNG stwarza dogodne warunki do spektakularnego aktu terroru.

Poza dotychczas znanymi elementami morskiej infrastruktury krytycznej pojawiły się innowacyjne zespoły morskich elektrowni wiatrowych z infrastrukturą towarzyszącą. W pierwszej fazie rozwoju morskiej energetyki wiatrowej znalazły się projekty MFW Bałtyk I, II i III. Na Morzu Bałtyckim panują bardzo dobre warunki wietrzne, czyniąc z nich stabilne źródła energii odnawialnej.

c. Zagrożenia terrorystyczne na obszarach morskich

Zagrożenia czasu pokoju

Zagrożenia te powodowane są przede wszystkim poprzez działalność podmiotów niepaństwowych, nie wspieranych przez żadne państwo. Mogą to być działania podejmowane z powodów ideologicznych lub z chęci uzyskania korzyści majątkowej. Należy pamiętać, że z uwagi na specyfikę funkcjonowania gospodarki morskiej czyn w zamiarze kryminalny może być dokonany w sposób uzasadniający podejrzenie popełnienia czynu o charakterze terrorystycznym (art. 115 § 20 Kodeksu Karnego). W szczególności dotyczy to modus operandi sprawców oraz wykorzystywanych przez nich narzędzi i środków technicznych.

W przypadku działań podejmowanych przez osoby lub grupy nie posiadające wsparcia państwowego, zagrożenia dla morskiej infrastruktury krytycznej oraz żeglugi warunkowane są przez dostępne im zasoby finansowe, uzbrojenie i wyposażenie oraz umiejętności wykorzystania go, a także zdolności organizacyjne i pozyskiwania informacji. Możliwe jest pozyskanie przez takich aktorów improwizowanych urządzeń wybuchowych, broni strzeleckiej oraz dostępnych na cywilnym rynku pojazdów oraz jednostek pływających i dostępnego dla użytkowników cywilnych wyposażenia do prac podwodnych czy bezzałogowych statków powietrznych. Istotną barierą w przypadku sprzętu podwodnego, w tym bezzałogowych pojazdów podwodnych, jest koszt ich nabycia.

W związku z powyższym możliwe jest przeprowadzenie przez aktorów niepaństwowych ataków na cele, do których sprawcy mają najłatwiejszy dostęp. Mając na uwadze polskie obszary morskie są to przede wszystkim obiekty położone na lądzie (porty) oraz jednostki żeglugi pasażerskiej i rekreacyjnej. Inną sytuacją jest *insider attack* – a więc zagrożenie powodowane przez osobę zatrudnioną w danym obiekcie, działającą samodzielnie lub w porozumieniu z innymi osobami (dobrowolnie lub pod przymusem).

Sprawcy tego typu ataków mogą kierować się motywami ideologicznymi, w szczególności związanymi z prowadzoną przez Polskę polityką zagraniczną. Możliwe jest także prowadzenie działań przez organizacje radykalnych ekologistów, w szczególności ataki na wydobycie i transport surowców energetycznych. Mogą wystąpić także incydenty związane z próbą przeniknięcia sprawców na terytorium Polski lub jego opuszczenia (ucieczki).

Można wskazać w tym kontekście kilka możliwych scenariuszy ataku na żeglugę jak również morską infrastrukturę krytyczną.

Pierwszym jest dokonanie tradycyjnego zamachu z użyciem urządzenia wybuchowego, broni palnej lub innych niebezpiecznych narzędzi na terenie obiektu portowego. Może mieć on formę ataku bombowego, ataku „aktywnego strzelca" lub wzięcia zakładników; poza miejscem wystąpienia nie będzie się różnić od innych tego rodzaju zdarzeń na terenie obiektów infrastruktury krytycznej. Należy jedynie pamiętać o specyfice poszczególnych obiektów, z uwagi na przeładowywane w portach towary, w tym ładunki niebezpieczne oraz możliwości przedostania się sprawcy na pokład zacumowanej w porcie jednostki pływającej.

Drugim jest dokonanie zamachu – zarówno bombowego jak również wzięcia zakładników, lub ataku z użyciem niebezpiecznego narzędzia na pokładzie jednostki pływającej lub na pokładzie instalacji znajdującej się na morzu (np. platforma wiertnicza). W szczególności prawdopodobnym jest scenariusz przejęcia kontroli nad jednostką

pływającą w celu spełnienia żądań stawianych przez sprawców (ustępstw politycznych, wypłacenia okupu). W polskich obszarach morskich możliwym celem takich ataków mogą być jednostki pasażerskie (zwłaszcza promy morskie) a poza Bałtykiem – jednostki handlowe na akwenach zagrożonych działalnością grup przestępczych.

Trzecim możliwym scenariuszem jest atakowanie obiektów portowych lub jednostek pływających za pomocą bezzałogowych statków powietrznych. Mogą one w szczególności posłużyć do przeniesienia niewielkich urządzeń wybuchowych. Prawdopodobne jest użycie komercyjnie dostępnych urządzeń, co przekłada się na łatwość użycia ale przynosi relatywnie niewielkie szkody (zob. *Bezpieczeństwo infrastruktury krytycznej wobec zagrożeń ze strony platform bezzałogowych*, „Raport PTBN", Tom II.2).

Czwarty scenariusz to użycie jednostki pływającej jako środka ataku terrorystycznego. W szczególności może to być łatwo dostępna jednostka pływająca (np. łódź motorowa) przenosząca urządzenie wybuchowe. Atak może mieć charakter samobójczy lub zostać dokonany z pomocą jednostki zdalnie sterowanej lub zaopatrzonej w urządzenia samosterujące. Mając na uwadze dostępność środków technicznych, możliwe (choć mniej prawdopodobne) jest wykorzystanie zakupionego lub skonstruowanego samodzielnie bezzałogowego pojazdu podwodnego. Ponadto jednostka nawodna pozwala na umieszczenie na niej ładunku wybuchowego o większej masie, a więc większej zdolności rażenia.

Należy odnotować, że działania terrorystyczne wymierzone w infrastrukturę portową czy żeglugę są relatywnie rzadkie. Dane *Global Terrorism Database* zawierają informacje o 394 atakach na cele morskie w przedziale 1971-2019 z czego w Europie i Ameryce Północnej jedynie 33. Wpływ na to ma prawdopodobnie stopień trudności związany z atakami na cele morskie i porty, jak również możliwy jest wpływ zjawiska *sea blindness,* a więc niedostrzegania znaczenia gospodarki morskiej w świadomości społecznej. Dla porównania atak na cel taki jak międzynarodowy port lotniczy jest dla terrorystów łatwiejszy (o czym świadczy większa częstotliwość ataków) jak również bardziej medialny. Nie bez znaczenia jest także dużo większy udział przewozów pasażerskich w transporcie lotniczym, a więc więcej jest zarówno potencjalnych świadków jak również ofiar takiego ataku.

Zagrożenia czasu kryzysu realizowane w ramach zagrożeń hybrydowych

Zagrożenia hybrydowe zostały zdefiniowane na użytek niniejszego opracowania jako działania aktorów państwowych, podejmowane w celu osiągnięcia swoich celów politycznych, gospodarczych i wojskowych poprzez destabilizację środowiska bezpieczeństwa

osiąganą poprzez połączone jawne i niejawne wykorzystanie różnych środków nacisku, w tym militarnych, gospodarczych i informacyjnych, także wykorzystując lub pozorując działalność innych podmiotów, w tym aktorów niepaństwowych. Hybrydowość zagrożenia oznacza, że prawdopodobne jest użycie różnych środków, z różnych domen (m.in. politycznej, wojskowej, ekonomicznej i społecznej) i w zróżnicowanym stopniu natężenia. Do najczęściej stosowanych w ostatnim latach narzędzi hybrydowych zalicza się działania dezinformacyjne, cyberataki, ingerencję w procesy wyborcze, szantaż ekonomiczny i uzależnienie od dostaw surowców.

W kontekście bezpieczeństwa polskich obszarów morskich oraz infrastruktury krytycznej za najbardziej prawdopodobne zagrożenie hybrydowe należy uznać działania Rosji, dążącej do wywarcia wpływu na Polskę oraz inne państwa Europy Środkowej. Prawdopodobnym celem będzie wykazanie nieskuteczności polskich organów państwowych do przeciwdziałania i reagowania na zagrożenia, a w ślad za tym skomplikowanie sytuacji międzynarodowej Polski, osłabienie solidarności sojuszniczej oraz wymuszenie spełnienia rosyjskich żądań politycznych, gospodarczych i wojskowych. Powodowane w ten sposób sytuacje będą miały na celu także wykazanie rzekomej skuteczności i sprawczości Rosji jako aktora zdolnego zapewnić bezpieczeństwo zamiast Polski oraz organizacji takich jak NATO i UE lub przynajmniej wymuszenie podjęcia negocjacji z Rosją. Jest to zagrożenie szczególnie prawdopodobne w kontekście rosyjskiej agresji na Ukrainę.

Scenariusze możliwych kryzysów muszą uwzględniać istniejące i możliwe podatności Polski, także w domenie morskiej.

Wykorzystanie środków hybrydowych w domenie morskiej może przybrać postać jednego z kilku scenariuszy.

1. Zakwestionowanie zdolności Polski do zapewnienia bezpieczeństwa w wyłącznej strefie ekonomicznej. Scenariusz ten zakłada stworzenie sytuacji, w której bezpieczeństwo żeglugi znajdujących się w wyłącznej strefie ekonomicznej RP rurociągów i kabli podmorskich oraz innych instalacji – np. energetycznych i wydobywczych – zostaje zagrożone w formie faktycznego incydentu, np. zdarzenia o charakterze terrorystycznym lub sabotażu czy też groźby takiego zdarzenia. Towarzyszyłaby temu intensywna akcja informacyjna, mająca na celu np. przekonanie opinii publicznej o rzekomych lub prawdziwych skutkach np. katastrofy morskiej. Należy zwrócić uwagę, że ten scenariusz nie zakłada bezpośredniego oddziaływania na Polskę, ale jedynie udowodnienie jej nieskuteczności. Przykładowo, wykreowane zagrożenie mogłoby godzić np. w żeglugę handlową obsługującą porty rosyjskie. Wariantem tego

scenariusza jest wykreowanie sytuacji kryzysowej w sposób sugerujący, że doszło do zagrożenia dla żeglugi i instalacji w innych obszarach Bałtyku, ale mającego źródło na obszarach kontrolowanych przez Polskę, np. rzekome dokonanie sabotażu na gazociągu poza polską wyłączną strefą ekonomiczną przy pomocy jednostki, która wcześniej zawinęła do portu polskiego. Należy odnotować, że scenariusz ten, choć poza polskimi obszarami morskimi zmaterializował się w postaci wysadzenia we wrześniu 2022 r. gazociągów Nord Stream i Nord Stream II.

W tych scenariuszach przekaz kierowany byłby zarówno do społeczeństwa polskiego jak również do szerszej widowni, w tym społeczeństw innych państw europejskich. Działania Rosji prowadziłyby do stworzenia warunków pozwalających na szeroką aktywność rosyjskich sił morskich pod pozorem „operacji antyterrorystycznej".

2. Zablokowanie możliwości korzystania przez Polskę z transportu morskiego. Ten scenariusz zakłada już bezpośrednie działanie mające na celu utrudnienie lub uniemożliwienie żeglugi handlowej na polskich obszarach morskich oraz akwenach dla Polski strategicznie ważnych. W szczególności dotyczy to importu surowców energetycznych oraz transportu innych, ważnych dla gospodarki polskiej ładunków. Może to zostać osiągnięte poprzez działania zarówno kinetyczne jak niekinetyczne. Zablokowanie lub utrudnienie transportu morskiego oznacza zwiększenie podatności Polski na inne formy presji, w tym gospodarczej. Możliwe jest także, podobnie jak w scenariuszu poprzednim, doprowadzenie do sytuacji, w której Rosja rozpocznie jednostronną operację na obszarze Bałtyku pod pozorem „ochrony bezpieczeństwa żeglugi".

3. Atak na infrastrukturę, w tym infrastrukturę krytyczną położoną na obszarach morskich. Ten scenariusz zakłada działania przeciwko instalacjom zlokalizowanym na polskich wodach terytorialnych lub w wyłącznej strefie ekonomicznej, takim jak platformy wydobywcze, morskie farmy wiatrowe, rurociągi i kable podmorskie. Celem działania sprawców byłoby uniemożliwienie korzystania z nich w celu zwiększenie podatności Polski na inne formy presji (zwłaszcza gospodarczej), jak również wywołanie strachu przed kryzysem gospodarczym lub katastrofą ekologiczną. Do tej kategorii zaliczyć należy działania wymierzone w pływające instalacje przeładunkowe gazu ziemnego (FSRU – taka instalacja ma znaleźć się w Zatoce Gdańskiej).

4. Atak na obiekty brzegowe, w tym obiekty infrastruktury krytycznej. Mogą to być instalacje związane bezpośrednio z gospodarką morską, takie jak porty lub też obiekty położone w pobliżu wybrzeża, na przykład instalacje przemysłowe lub energetyczne.

W każdym z tych scenariuszy, należy uwzględnić możliwość wykorzystania szerokiego spektrum środków. Mogą to być środki typowe dla ruchów protestu, organizacji terrorystycznych lub wojsk specjalnych przeciwnika. Możliwe jest także celowe atakowanie jednostek pływających, obiektów, instalacji wykorzystywanych przez służby państwowe. Należy w tym uwzględnić ryzyko wykorzystania jednostek pływających jako narzędzi ataku lub transportu.

W szczególności prawdopodobnymi metodami działania są:

- blokady w formie biernego oporu upozorowane na protesty organizacji społecznych i ekologicznych, zarówno na morzu (z użyciem cywilnych jednostek rekreacyjnych) jak na lądzie i w powietrzu, mające na celu ograniczenie swobody żeglugi i pracy instalacji przeładunkowych;
- akty polegające się na przedostaniu się osób na teren instalacji lub pokłady jednostek pływających, upozorowane na akty protestu, mające wykazać podatność penetrowanych celów na akty dywersji;
- uporczywe nękanie statków i instalacji brzegowych przy pomocy bezzałogowych statków powietrznych lub załogowych i bezzałogowych jednostek pływających (w tym tzw. „wypychanie kadłubem”);
- upozorowanie lub celowe dokonanie awarii jednostki pływającej, np. samozatopienie statku handlowego w celu zablokowania szlaku żeglugowego;
- upozorowanie zderzenia na morzu załogowej lub bezzałogowej jednostki pływającej z inną jednostką pływającą lub platformą wiertniczą;
- umieszczenie urządzenia wybuchowego na terenie obiektu brzegowego lub jednostki pływającej poprzez wniesienie go lub wwiezienie na pokładzie pojazdu;
- niszczenie i uszkadzanie pomocy nawigacyjnych i środków obserwacji technicznej, także należących do służb państwowych;
- wykorzystanie środków dywersji podwodnej w celu umieszczenia urządzenia wybuchowego na podwodnej części kadłuba statku, platformy wydobywczej, turbiny wiatrowej lub przerwania ciągłości innej instalacji ułożonej na dnie morza np. rurociągu lub kabla podmorskiego. Może to nastąpić przy wykorzystaniu płetwonurków lub/i pojazdów bezzałogowych, w tym jednorazowego użytku;
- napad ogniowy z wykorzystanie środków rażenia takich jak bezzałogowe statki powietrzne lub uzbrojenie rakietowe w celu zaatakowania statków lub innych obiektów, np. portowych lub celów brzegowych. Ich nosicielami mogą być w szczególności jednostki pływające;
- atak z wejściem na obiekt w celu zniszczenia lub przejęcia kontroli nad jednostką pływającą lub innym celem (np. platformą wiertniczą), w tym mający na celu doprowadzenie do sytuacji zakładniczej;

- wywołanie katastrofy ekologicznej przez uwolnienie wskutek sabotażu substancji chemicznych (ropa z tankowców, sarin na dnie Zatoki Gdańskiej);
- ataki cybernetyczne i informacyjne, w tym mające na celu zakłócenie pracy systemów nawigacyjnych i wspomagających żeglugę (jak GPS i AIS) oraz systemów sterowania jednostkami pływającymi (w tym bezzałogowymi) i pracami instalacji brzegowych.

Zagrożenia czasu wojny

W razie zaistnienia otwartego konfliktu zbrojnego, także na skutek eskalacji działań hybrydowych, w tym cyberataku, zarówno żegluga jak również infrastruktura może stać się celem ataków prowadzonych przez siły zbrojne przeciwnika, w tym przez siły nawodne, podwodne, lotnicze, rakietowe, pododdziały wojsk specjalnych oraz siły lądowe, w tym desanty morskie. Przeciwdziałanie im wymaga więc użycia własnych sił konwencjonalnych, przede wszystkim sił i środków Marynarki Wojennej. Oprócz nich istotną rolę, zwłaszcza w zakresie działań przeciwdywersyjnych, mogą odegrać także siły i środki przeznaczone do prowadzenia działań kontrterrorystycznych, w szczególności w zakresie wykrywania oraz zwalczania grup dywersyjno–rozpoznawczych. Należy przy tym zauważyć, że z uwagi na swoją specyfikę wojska specjalne przeciwnika mogą zostać skrycie rozmieszczone i przygotowane do użycia przed rozpoczęciem walk i użyte w pierwszych chwilach konfliktu zbrojnego.

1.9. Percepcja zagrożenia o charakterze terrorystycznym w UE i RP

a. Percepcja zagrożenia o charakterze terrorystycznym w UE

24 stycznia 2023 r. Polskie Towarzystwo Bezpieczeństwa Narodowego brało udział w badaniu ankietowym członków EU PSA (antyterrorystycznej inicjatywy ochrony przestrzeni publicznych i infrastruktury krytycznej Komisji Europejskiej – DG HOME) oraz przedstawicieli wspierających ten projekt instytucji UE z udziałem partnerów strategicznych z USA[4]. Badanie zrealizowano na podstawie zestandaryzowanego kwestionariusza ankiety na próbie 55 osób. Respondenci reprezentowali: EU PSA (83,64%),

[4] Szczegółowe dane z badań wraz z komentarzem zostaną opublikowane w: Karolina Wojtasik, Wyniki badania na temat percepcji zagrożeń o charakterze terrorystycznym wśród uczestników EU PSA, Analizy PTBN, nr 1 (2023), Warszawa 2023.

instytucje UE wspierające ww. inicjatywę (10,91%) oraz partnera strategicznego projektu EU PSA – Stany Zjednoczone (5,45%).

Eksperci ds. zagrożeń terrorystycznych zaangażowani w EU PSA lub wspierający te inicjatywę Komisji Europejskiej jako najbardziej potencjalne cele ataku terrorystycznego na terenie UE wskazywali infrastrukturę krytyczną (63,63% wszystkich odpowiedzi), systemy transportu publicznego (60%) oraz symboliczne obiekty turystyczne (34,55%).

Jeśli chodzi o narzędzia, które dziś stanowią największe wyzwanie dla służb, organów i instytucji mających zapewniać bezpieczeństwo fizyczne osób i obiektów mogących być celem ataków terrorystycznych w UE, respondenci wskazywali pojazdy bezzałogowe (powietrzne, lądowe, wodne) – 49,09% odpowiedzi.

Ponad 80% respondentów uważa, że w perspektywie 3-letniej działalność terrorystyczna będzie wykorzystywana w ramach scenariuszy zagrożeń hybrydowych podejmowanych na terytorium UE przez obce państwo.

Jeśli chodzi o typy obiektów, które w perspektywie 3-letniej będą na terenie UE charakteryzować się najwyższym poziomem zagrożenia atakiem terrorystycznym, respondenci najczęściej wskazywali: infrastrukturę krytyczną sektora energetycznego (suma wszystkich wskazań: 70,91%), system transportu publicznego (58,19%) oraz siedziby konstytucyjnych organów państwowych i miejsca kultu religijnego (po 27,22%).

Respondenci wskazali, że systemem IK, który w perspektywie 3-letniej powinien być traktowany priorytetowo w kwestii budowy odporności na zagrożenia hybrydowe, jest system energetyczny.

W przypadku pytania o obszar przeciwdziałania aktywności o charakterze terrorystycznym, który wymaga dziś priorytetowego traktowania przez UE, zdania ekspertów były podzielone – trzy kategorie (wykrywanie i blokowanie propagandy terrorystycznej oraz materiałów instruktażowych publikowanych on-line; przeciwdziałanie finansowaniu terroryzmu; inicjatywy edukacyjne z zakresu budowania kultury bezpieczeństwa obiektów podatnych na ataki terrorystyczne) uzyskały identyczną liczbę wskazań po 21,82%.

Jako przedsięwzięcia najbardziej zwiększające poziom odporności na zamachy terrorystyczne w obiektach chronionych respondenci wskazali: standaryzację bezpieczeństwa fizycznego (52,72% wszystkich wskazań), rozwój inicjatyw profilaktyki

antyterrorystycznej w ramach kultury bezpieczeństwa obiektu (54,54%) oraz stosowanie testów kontroli bezpieczeństwa przez zewnętrze podmioty nadzoru (47,28%). 45,45% respondentów uważa, że sprawcami obecnych ataków na systemy infrastruktury krytycznej są cyberprzestępcy powiązani z aktorem państwowym.

Inne aspekty zagrożeń o charakterze terrorystycznym w krajach UE przedstawiają niepublikowane wyniki badań przeprowadzonych przez dr. Jarosława Cymerskiego w zakresie kierunków zmian funkcjonowania formacji chroniącej osoby i obiekty ustawowo podlegających ochronie. W obliczu dynamicznie zmieniającego się środowiska zagrożeń postawiono pytanie dotyczące kształtowania się poziomu zagrożenia terroryzmem w Europie. Badana grupa ekspertów udzielająca odpowiedzi w formie wywiadu eksperckiego zwróciła uwagę na szereg aspektów zmienności omawianego środowiska z jednoczesnym akcentem na wzrost poziomu zagrożeń o charakterze terrorystycznym w krajach członkowskich. 77% respondentów uznało, że należy liczyć się ze wzrostem poziomu zagrożeń o charakterze terrorystycznych a jedynie 8 % respondentów wskazało na obniżenie poziomu zagrożenia terroryzmem w krajach UE.

W kwestii źródła zamachów terrorystycznych największa grupa 54% respondentów uważa, że zagrożenia spowodowane będą niekontrolowaną imigracją do Unii Europejskiej, postępującym procesem destabilizacji politycznej i ekonomicznej w krajach UE oraz konfliktami państwowymi (co zdaje się wpisywać się realia obecnej sytuacji w krajach europejskich będącej m.in. konsekwencją wojny ukraińsko-rosyjskiej). 15% respondentów odpowiedziało, że należy liczyć się z prawdopodobieństwem występowania zamachów inspirowanych przez Federacje Rosyjską. Taka sama grupa wskazała na prawdopodobieństwo zamachów przeprowadzonych przez organizacje separatystyczne. Po 8% respondentów odpowiedziało, że należy liczyć się z prawdopodobieństwem występowania zamachów przeprowadzonych przez organizacje skrajnie lewicowe i zwolenników „białej supremacji".

W charakter prowadzonego konfliktu wojennego wpisują się również zagrożenia infrastruktury krytycznej powstałe w wyniku przeprowadzanych ataków cybernetycznych – 23% respondentów odpowiedziało, że należy liczyć się z prawdopodobieństwem występowania zagrożeń spowodowanych atakami cybernetycznymi na systemu infrastruktury krytycznej w krajach Unii Europejskiej. Z kolei 15% przewiduje możliwość występowania zagrożeń spowodowanych wykorzystaniem broni masowego rażenia. Przyjąć więc można, że percepcja zagrożeń o charakterze terrorystycznym została potwierdzona w szeregu badań prowadzonych zarówno przez instytucje ds. bezpieczeństwa jak indywidualnych badaczy.

b. Percepcja zagrożenia o charakterze terrorystycznym w RP – uczestnicy systemu AT

W 2022 r. na łamach periodyku naukowego „Terroryzm – studia, analizy, prewencja" wydawanego przez ABW opublikowano wyniki pierwszego w Polsce badania ankietowego dotyczące percepcji zjawiska terroryzmu oraz przewidywanych, najbardziej prawdopodobnych kierunków rozwoju tego typu zagrożeń w RP. Respondentami byli przedstawiciele służb i instytucji należących do wspólnoty antyterrorystycznej RP (76%) oraz przedstawiciele środowiska akademickiego, jak również analitycy zajmujący się studiami nad terroryzmem. Oto najbardziej istotne kwestie z punktu widzenia oceny zagrożenia o charakterze terrorystycznym w RP:

- Według 53,19% respondentów ISIS (Daesh) to organizacja stanowiącą największe zagrożenie bezpieczeństwa RP, służby specjalne Federacji Rosyjskiej zajęły drugie miejsce z wynikiem 17,02%, na trzecim miejscu znalazła się sieć Atomwaffen z wynikiem 14,89%.
- Respondenci wskazali następujące typy obiektów jako najbardziej prawdopodobny cel zamachów terrorystycznych w UE: infrastruktura krytyczna – 39,36%, otwarte przestrzenie publiczne 32,98%, – infrastruktura turystyczna i obiekty sportowe 14,89%.
- Według 47,87% respondentów w latach 2022-2025 Polska będzie krajem atrakcyjnym dla terrorystów międzynarodowych planujących swoją aktywność w UE, z kolei 19,15% respondentów było przeciwnego zdania.
- W opinii 90,43% respondentów uznało, że w latach 2022-2025 należy spodziewać się aktywności terrorystycznej prowadzonej w ramach działań hybrydowych podejmowanych w RP przez państwa trzecie.
- Wśród obiektów umiejscowionych w RP, których poziom zagrożenia atakiem terrorystycznym w latach 2022-2025 został oceniany przez respondentów jako najwyższy, respondenci wskazali m.in. obiekty energetycznej infrastruktury krytycznej – 36,17%, system transportu publicznego – 34,04%, bazy wojskowe wykorzystywane w ramach wschodniej flanki NATO – 19,15%.

1.10. Perspektywy rozwoju zagrożeń o charakterze terrorystycznym na terytorium RP

Sytuacja społeczno-polityczna w ostatnich latach stała się nieprzewidywalna, dlatego wszelkie próby prognozowania obarczone są dużym ryzykiem. Rośnie prawdopodobieństwo pojawienia się „czarnych łabędzi" – nieoczekiwanych wydarzeń, które zmieniają

dynamikę procesów. Zakładając jednak, że w najbliższym czasie takie wydarzenia nie zaistnieją można próbować wytyczyć kierunki zagrożeń na podstawie długofalowych trendów.

W przypadku zagrożeń pochodzenia wewnętrznego oprzeć można się na teorii, według której przemoc polityczna (w tym terrorystyczna) jest efektem procesu radykalizacji. O ile radykalizacja jednostkowa jest trudna do zdiagnozowania i wykrycia, o tyle radykalizacja masowa przyjmuje postać zjawisk społecznych takich jak ruchy protestu. W przypadku Polski zaliczyć można tu:

- pogłębianie się polaryzacji politycznej i światopoglądowej,
- wzrost niechęci do imigrantów,
- napięcia na tle socjalnym (w przypadku pogarszania się sytuacji gospodarczej),
- radykalizację ruchu ekologicznego,
- radykalizację zwolenników teorii spiskowych (np. Wielki Reset).

Najbardziej prawdopodobnie są indywidualne, w dużym stopniu żywiołowe akty przemocy, których celem będą w pierwszej kolejności symbole i mienie (np. budynki), rzadziej ludzie (zarówno rozpoznawalne postaci jak przypadkowe osoby należące do „wrogiej" grupy). Możliwe są także – zwłaszcza w przypadku radykalnych obrońców środowiska czy zwolenników teorii spiskowych – akty sabotażu skierowane przeciw infrastrukturze gospodarczej. W miarę radykalizacji ruchów protestu rozwijać się będą grupy przygotowujące się do stosowania przemocy (treningi fizyczne, zwłaszcza sztuk walki) i stosujące przemoc w sposób zorganizowany (choć raczej ograniczające się do starć ulicznych). Nie można wykluczyć, że na marginesie tych ruchów samodzielnie zradykalizowane jednostki będą próbowały przeprowadzić mordercze zamachy terrorystyczne.

Zagrożenia pochodzenia zewnętrznego mogą mieć dwojakie źródła. Pierwszym jest nasilona w ostatnich latach imigracja, która potencjalnie może stać się podłożem nawrotu terroryzmu dżihadystycznego ale też zaognienia polsko-ukraińskich resentymentów historycznych (backlash); możliwe jest również przenoszenie na terytorium Polski zagranicznych antagonizmów narodowościowych (np. turecko-kurdyjskiego). Drugie źródło to ingerencja podmiotów państwowych (w zasadzie Federacji Rosyjskiej); ze względu na słabe zaplecze społeczne przyjmować będzie prawdopodobnie postać zakamuflowanej inspiracji innych (wymienionych powyżej) ruchów.

2. Elementy systemu antyterrorystycznego RP

2.1. System bezpieczeństwa cyberprzestrzeni RP a zagrożenia o charakterze terrorystycznym

a. Unijne i krajowe uwarunkowania prawne w zakresie cyberterroryzmu

W polskim jak też europejskim ustawodawstwie brak jest jednolitej definicji cyberterroryzmu. Ogólnie można przyjąć, że ataki cyberterrorystyczne dzielą się na dwie kategorie. Pierwsza obejmująca działania zmierzające do zniszczenia wytypowanego celu lub destabilizacji systemu skutkujące fizycznym zniszczeniem np. obiektów infrastruktury krytycznej kraju. Druga obejmuje użycie technologii informacyjnych i komunikacyjnych np. do ataków typu Dos i DDoS lub wirusowych, a także nieautoryzowany dostęp do systemów rządowych czy korporacyjnych (ważne węzły informacyjne, teleinformatyczne oraz telekomunikacyjne), mające na celu wywołanie określonego skutku czy reakcji. Jest to więc bezprawny atak lub groźba ataku na komputery, sieci lub systemy informacyjne, będący rezultatem działań podmiotów niepaństwowych bądź obcych służb specjalnych, w celu zastraszenia albo wymuszenia ustępstwa na rządzie lub wywołania niepewności i strachu w społeczeństwie.

Inną kwestią jest kwalifikacja czynów polegających na wykorzystywaniu przestrzeni wirtualnej do działań prowadzących do radykalizacji (szerzenia propagandy terrorystycznej), rekrutacji do organizacji czy komunikowania się zwolenników i członków ugrupowania terrorystycznego. W tym obszarze prowadzone są prace legislacyjne zarówno na poziomie UE jak i poszczególnych krajów członkowskich mające na celu stałą aktualizację regulacji wobec coraz bardziej wyrafinowanych metod działalności terrorystycznej.

Dokumenty UE odnoszące się do cyberterroryzmu

UE opracowuje w zakresie cyberprzestrzeni wytyczne polityczne i zalecenia, jak np.:

- *Zalecenie Komisji (UE) 2017/1584 z dnia 13 września 2017 r. w sprawie skoordynowanego reagowania na incydenty i kryzysy cybernetyczne na dużą skalę*. Określono w nim cele i sposoby współpracy między państwami członkowskimi a instytucjami UE w zakresie reagowania na transgraniczne incydenty cybernetyczne lub kryzysy na dużą skalę. Wyjaśniono w nim, w jaki sposób istniejące mechanizmy zarządzania kryzysowego mogą być w pełni wykorzystywane przez istniejące podmioty cyberbezpieczeństwa na szczeblu UE.
- *Zalecenie Komisji (UE) 2021/1086 z dnia 23 czerwca 2021 r. w sprawie utworzenia wspólnej jednostki ds. cyberprzestrzeni*. Dokument stanowi ważny krok w kierunku ukończenia europejskich ram zarządzania kryzysowego w dziedzinie cyberbezpieczeństwa. Jest to konkretny rezultat strategii UE w zakresie cyberbezpieczeństwa i strategii UE w zakresie unii bezpieczeństwa, przyczyniający się do bezpiecznej gospodarki cyfrowej i społeczeństwa cyfrowego. Wspólna jednostka ds. cyberprzestrzeni będzie działać jako platforma zapewniająca skoordynowaną reakcję UE na cyberincydenty i cyberkryzysy na dużą skalę, a także oferująca pomoc w usuwaniu skutków tych ataków. Aby osiągnąć ten cel w zaleceniu zdefiniowano również procedurę, cele pośrednie i harmonogram, które państwa członkowskie i właściwe instytucje, organy i agencje UE powinny stosować, mając na uwadze stworzenie i rozwój platformy.

16 grudnia 2020 r. Komisja Europejska zaprezentowała nowy pakiet cyberbezpieczeństwa, w skład którego weszła m.in. *Strategia UE w zakresie cyberbezpieczeństwa* skoncentrowana na budowaniu wspólnych zdolności reagowania na poważne cyberataki oraz współpracy z partnerami w celu zapewnienia międzynarodowego bezpieczeństwa i stabilności w cyberprzestrzeni, a także wzmocnieniu odporności Europy na cyberprzestępstwa. Strategia składa się z inicjatyw w obszarach: (1) odporność, technologiczna suwerenność i przywództwo, (2) budowanie zdolności operacyjnych do zapobiegania, odstraszania i reagowania na incydenty w cyberprzestrzeni, (3) rozwój globalnej i otwartej cyberprzestrzeni poprzez zacieśnienie współpracy międzynarodowej.

Dodatkowo Komisja przedstawiła wnioski legislacyjne dotyczące zarówno cyberodporności, jak i fizycznej odporności podmiotów krytycznych i krytycznych sieci: *Dyrektywę w sprawie bezpieczeństwa sieci i systemów informatycznych* (dyrektywa NIS 2") oraz *Dyrektywę Parlamentu Europejskiego i Rady w sprawie odporności podmiotów*

krytycznych. Proponowane regulacje mają na celu zwiększenie poziomu bezpieczeństwa podmiotów wchodzących w skład infrastruktury krytycznej państw członkowskich Unii Europejskiej i ich odporności począwszy od cyberataków i cyberterorryzmu po przestępczość czy klęski żywiołowe. Propozycja regulacji ma formę dyrektywy, aby umożliwić uwzględnienie krajowych specyfik, współzależności sektorowych oraz transgranicznych. Nowe unijne ramy dotyczące odporności infrastruktury krytycznej zawierają m.in. opis obowiązków właściwych organów, w tym wskazywanie podmiotów krytycznych.

Dodatkowo 22 marca 2021 r. Rada UE przyjęła konkluzje w sprawie strategii cyberbezpieczeństwa, podkreślając, że cyberbezpieczeństwo ma zasadnicze znaczenie dla budowania odpornej, ekologicznej i cyfrowej Europy, a głównym celem działań UE w tym obszarze jest dążenie do autonomii strategicznej przy jednoczesnym zachowaniu otwartej gospodarki poprzez zwiększenie zdolności dokonywania samodzielnych wyborów w obszarze cyberbezpieczeństwa. Do 18 maja 2022 r. Rada przedłużyła obowiązywanie ram sankcji za cyberataki zagrażające UE lub jej państwom członkowskim. Dzięki temu UE może nadal nakładać ukierunkowane sankcje na osoby lub podmioty biorące udział w cyberatakach, które powodują istotne szkody i są zewnętrznym zagrożeniem dla UE lub jej państw członkowskich. Sankcje można stosować także w odpowiedzi na cyberataki wymierzone przeciwko państwom trzecim lub organizacjom międzynarodowym, jeżeli uzna się to za konieczne do osiągnięcia celów wspólnej polityki zagranicznej i bezpieczeństwa.

Innym aspektem cyberbezpieczeństwa zajmuje się *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/784 z dnia 29 kwietnia 2021 r. w sprawie przeciwdziałania rozpowszechnianiu w Internecie treści o charakterze terrorystycznym*. Podstawowym celem przepisów ujętych we wskazanym rozporządzeniu jest ograniczenie używania sieci do radykalizacji, rekrutacji, podżegania do przemocy oraz umożliwienie szybkiego usuwania treści terrorystycznych, a także stworzenie wspólnych ram prawnych dla wszystkich państw członkowskich poprzez wprowadzenie mechanizmu wydawania i weryfikowania nakazów usunięcia lub uniemożliwienia dostępu do treści o charakterze terrorystycznym. Przepisy mają zastosowanie do dostawców usług hostingowych oferujących usługi w UE, niezależnie od miejsca znajdowania się siedziby głównej danego podmiotu. Właściwe organy w państwach członkowskich będą miały uprawnienia do wydawania usługodawcom nakazów usunięcia treści o charakterze terrorystycznym lub zablokowania dostępu do treści w ciągu jednej godziny. Pełne wdrożenie postanowień wskazanego rozporządzenia nastąpiło w Polsce 7 czerwca 2022 r.

Krajowe dokumenty i regulacje odnoszące się do cyberterroryzmu

Na poziomie strategicznym w Rzeczypospolitej Polskiej cyberbezpieczeństwa dotyczą następujące dokumenty:

- *Strategia Cyberbezpieczeństwa RP na lata 2019-2024* została zaakceptowana przez Radę Ministrów w dniu 22 października 2019 r. (z mocą od 31 października 2019 r.) zastępując *Krajowe Ramy Polityki Cyberbezpieczeństwa RP na lata 2017-2022*.
- *Doktryna Cyberbezpieczeństwa RP*, będąca jedynie dokumentem o charakterze koncepcyjnym i niemającym mocy prawnej, opracowana została w 2015 r. w Biurze Bezpieczeństwa Narodowego i zaakceptowana przez Radę Bezpieczeństwa Narodowego. Jest to dokument wykonawczy w stosunku do *Strategii Bezpieczeństwa Narodowego RP* określający cele w dziedzinie cyberbezpieczeństwa, a także rekomendacje jakie powinny być realizowane w ramach budowy systemu cyberbezpieczeństwa państwa. Zawiera postulaty m.in. takie jak: wprowadzenie określonych rozwiązań formalno-prawnych, stworzenie mechanizmów współpracy sektora publicznego i prywatnego, zwiększenie inwestycji w narodowe rozwiązania w dziedzinie cyberbezpieczeństwa oraz wykorzystanie potencjału obywatelskiego na rzecz ochrony państwa w cyberprzestrzeni.
- *Strategia Bezpieczeństwa Narodowego*. Głównym celem wskazanym w SBN dla obszaru cyberbezpieczeństwa jest podniesienie poziomu odporności na zagrożenia oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym i prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich zasobów informacyjnych.

W polskim systemie regulacji prawnych podstawowym obszarem zwalczania terroryzmu jest prawo karne oraz administracyjne, w których zostały zawarte mechanizmy prawne mające na celu zapobieganie cyberterroryzmowi, a także zwalczanie jego skutków. Nie ma jednego dokumentu, który regulowałby obszar cyberataków, a przepisy dotyczące cyberterroryzmu są regulowane sektorowo lub wycinkowo, według zadań różnych podmiotów, w wyniku czego pozostają rozproszone w wielu aktach prawnych.

Ustawa o działaniach antyterrorystycznych nie odnosi się bezpośrednio do zwalczania zjawiska cyberterroryzmu i ochrony cyberprzestrzeni, jednak w ramach artykułów zmieniających inne ustawy zawarto w niej zapisy dotyczące odpowiedzialności ABW w zakresie rozpoznawania zagrożeń w cyberprzestrzeni, zapobiegania im oraz zwalczania. Dodatkowo ustawa ta znowelizowała *Ustawę o ABW oraz AW* poprzez rozszerzenie zadań ABW o przepis wskazujący na szczegółowe rozwiązania dotyczące ochrony cyberprzestrzeni w ramach jej ustawowych działań zawartych w art. 5 ust. 1 ustawy. ABW stała

się właściwa w zakresie rozpoznawania zagrożeń godzących w bezpieczeństwo istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemów sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej (o których mowa w art. 5b ust. 7 p. 1 *Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*), a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej. Przepis ten po raz pierwszy w polskim systemie prawnym wskazywał podmiot odpowiedzialny za określony zakres bezpieczeństwa teleinformatycznego państwa.

W związku z tym w art. 32a *Ustawy o ABW i AW* powierzono ABW przeprowadzanie oceny bezpieczeństwa wskazanych systemów teleinformatycznych lub sieci teleinformatycznych (tzw. testów penetracyjnych) oraz analizę zdarzeń naruszających bezpieczeństwo systemów teleinformatycznych skutkujące wydawaniem podmiotom, o których mowa w art. 32d ust. 3, rekomendacji zmierzających do podniesienia poziomu bezpieczeństwa systemów teleinformatycznych. Przedmiotowa kwestia została szczegółowo uregulowana w *Rozporządzeniu Rady Ministrów z dnia 19 lipca 2016 r. w sprawie przeprowadzania oceny bezpieczeństwa związanej z zapobieganiem zdarzeniom o charakterze terrorystycznym*. Przytoczony akt wykonawczy oprócz określenia warunków i trybu przeprowadzania oceny bezpieczeństwa, a także czynności niezbędnych do przeprowadzania oceny bezpieczeństwa, wyznacza wzór porozumienia zawierającego ramowe warunki przeprowadzenia oceny.

W celu zapobiegania, wykrywania, przeciwdziałania przestępstwom o charakterze terrorystycznym oraz ścigania ich sprawców wprowadzona została mocą art. 32c *Ustawy o ABW oraz AW* możliwość stosowania tzw. „blokady dostępności". Sąd Okręgowy, na pisemny wniosek Szefa ABW złożony po uzyskaniu pisemnej zgody prokuratora generalnego, w drodze postanowienia może zarządzić zablokowanie przez usługodawcę świadczącego usługi drogą elektroniczną dostępności w systemie teleinformatycznym.

Inną niezwykle ważną kwestią jest uregulowanie na poziomie ustawowym możliwości wystąpienia zdarzenia o charakterze terrorystycznym, którego celem byłyby systemy teleinformatyczne istotne z punktu widzenia funkcjonowania państwa. W tym zakresie *Ustawa o działaniach antyterrorystycznych* (art. 15) wprowadziła powszechnie obowiązujący, jednolity i dostosowany do wymogów NATO czterostopniowy system stopni alarmowych, w tym również stopni alarmowych dotyczących cyberprzestrzeni RP (stopnie alarmowe CRP). Dodatkowo wprowadzono na podstawie art. 17 ustawy mechanizm powoływania przez szefa ABW sztabu koordynacyjnego w przypadku wprowadzenia stopnia alarmowego dotyczącego zdarzeń na terytorium RP oraz stopnia alarmowego CRP.

Ustawa o Krajowym Systemie Cyberbezpieczeństwa (dalej KSC), będąca wypełnieniem zobowiązania wdrożenia do polskiego porządku prawnego dyrektywy 2016/1148, ma na celu kompleksowe uregulowanie obszaru cyberbezpieczeństwa poprzez określenie organizacji oraz sposobu funkcjonowania krajowego systemu cyberbezpieczeństwa, sposobu sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy oraz zakresu i trybu stanowienia Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej.

b. Rola i zadania podmiotów odpowiedzialnych za przeciwdziałanie cyberterroryzmowi

Zapewnienie bezpieczeństwa cyberprzestrzeni RP ze szczególnym uwzględnieniem zagrożenia, jakim jest szeroko rozumiany cyberterroryzm, powinno odbywać się zarówno poprzez rozwój zdolności defensywnych jak i ofensywnych. Niemniej istotna jest także współpraca i koordynacja działań instytucji i służb państwowych z podmiotami sektora prywatnego (np. telekomunikacyjnego, energetycznego, finansowego, transportowego). Nie ulega wątpliwości, że rozpoznawanie cyberterroryzmu, a także przestępstw dokonywanych w cyberprzestrzeni, zapobieganie im oraz ściganie sprawców wymaga systemowego podejścia w wymiarze prawnym, organizacyjnym i technicznym.

Podstawowymi ogniwami systemu są tzw. CERT (Computer Emergency Response Team) powołane przez przedsiębiorców oraz inne zespoły ds. naruszeń w sieci. Należą do nich:

- **CSIRT (Computer Security Incident Response Team) GOV**, który funkcjonuje w ramach Departamentu Bezpieczeństwa Teleinformatycznego ABW i jest właściwy w zakresie incydentów związanych ze zdarzeniami o charakterze terrorystycznym, o których mowa w art. 2 p. 7 *Ustawy o działaniach antyterrorystycznych* z 10 czerwca 2016 r.
- **CSIRT NASK** prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy. CSIRT NASK wraz z CSIRT GOV obsługują system ARAKIS-GOV, będący systemem wczesnego ostrzegania o zagrożeniach w sieci Internet.
- **CSIRT MON** prowadzony przez Ministerstwo Obrony Narodowej jest właściwy w zakresie incydentów związanych ze zdarzeniami o charakterze terrorystycznym. CSIRT MON zobowiązany jest do koordynacji incydentów zgłaszanych przez podmioty podległe Ministrowi Obrony Narodowej lub przez niego nadzorowane.

Do powyższych zespołów CSIRT raportowane są incydenty (w tym incydenty mogące mieć znamiona cyberterroryzmu) wpływające na działalność operatorów usług kluczowych (incydenty poważne) i dostawców usług cyfrowych (incydenty istotne), a także

incydenty w podmiotach publicznych, a przede wszystkim incydenty krytyczne skutkujące znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi.

Każdy z zespołów CSIRT odpowiedzialny jest za koordynację incydentów zgłaszanych przez przyporządkowane zgodnie z ustawą podmioty. Na mocy KSC w sytuacji wystąpienia poważnego incydentu czy cyberataku wymagającego współpracy na poziomie ogólnokrajowym możliwa jest koordynacja działania wszystkich CSIRT-ów w Polsce (również sektorowych zespołów cyberbezpieczeństwa).

Zespoły CSIRT mają możliwość badania urządzeń lub oprogramowania w celu identyfikacji podatności, które wykorzystywane mogą być do zagrożenia integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych mających wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa. Na podstawie tych badań CSIRT mogą składać rekomendacje w celu usunięcia podatności urządzeń lub oprogramowania stosowanego przez podmioty krajowego systemu cyberbezpieczeństwa.

Zespół do spraw Incydentów Krytycznych jest organem pomocniczym w sprawach obsługi incydentów krytycznych zgłoszonych CSIRT MON, CSIRT NASK lub CSIRT GOV i koordynującym działania podejmowane przez te zespoły oraz Rządowe Centrum Bezpieczeństwa (art. 36 ustawy o KSC). W jego skład wchodzą przedstawiciele CSIRT MON, CSIRT NASK, Szefa ABW realizującego zadania w ramach CSIRT GOV oraz RCB.

Zapowiedziana nowelizacja ustawy o KSC wprowadza nowe rozwiązania dotyczące m.in.:

- zadań zespołów SOC (Security Operations Center) działających na rzecz operatorów usług kluczowych (do KSC wprowadzono pojęcie operacyjnych centrów bezpieczeństwa SOC, które zastąpią poprzednie struktury odpowiedzialne za cyberbezpieczeństwo operatora usług kluczowych),
- centrów wymiany informacji i analiz o cyberbezpieczeństwie ISAC, centrum wymiany i analizy informacji na temat podatności, zagrożeń i incydentów funkcjonujące w celu wspierania podmiotów KSC,
- utworzenia zespołów CSIRT sektorowych działający na poziomie sektora lub podsektora wspierających operatorów usług kluczowych w obsłudze incydentów (**CSIRT Telco** – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na rzecz przedsiębiorców komunikacji elektronicznej).

W celu skuteczniejszej koordynacji współpracy pomiędzy podmiotami krajowego systemu cyberbezpieczeństwa i efektywniejszej odpowiedzi na pojawiające się nowe zagrożenia powołano Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa oraz Kolegium do Spraw Cyberbezpieczeństwa.

Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa jest odpowiedzialny za koordynowanie na poziomie krajowym realizacji zadań dotyczących cyberbezpieczeństwa w RP. Do jego kompetencji należy również analiza i ocena funkcjonowania KSC na podstawie zagregowanych danych i wskaźników opracowanych przy udziale organów administracji państwowej, organów właściwych i zespołów CSIRT, jak również nadzór nad procesem zarządzania ryzykiem KSC z wykorzystaniem zagregowanych danych i wskaźników opracowanych przy udziale organów właściwych i zespołów CSIRT.

Kolegium do Spraw Cyberbezpieczeństwa jest organem opiniodawczo-doradczym w sprawach planowania, nadzorowania i koordynowania działalności zespołów CSIRT, sektorowych zespołów cyberbezpieczeństwa oraz organów właściwych. Na czele Kolegium stoi Prezes Rady Ministrów. Po otrzymaniu rekomendacji Kolegium, Prezes Rady Ministrów może wydać wiążące wytyczne w celu koordynacji działań w zakresie cyberbezpieczeństwa

Inne podmioty zaangażowane w przeciwdziałanie i zwalczanie różnego rodzaju przestępstw i zdarzeń w cyberprzestrzeni mogących być kwalifikowane jako cyberterrorystyczne oraz zajmujące się ochroną narodowych technologii kryptologicznych, to m.in. Biuro do Walki z Cyberprzestępczością KGP (na bazie którego od stycznia 2022 r. tworzone jest Centralne Biura Zwalczania Cyberprzestępczości) oraz Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni.

Dotychczasowe **Biuro do Walki z Cyberprzestępczością** realizuje zadania związane z tworzeniem warunków do efektywnego wykrywania sprawców przestępstw popełnionych przy użyciu nowoczesnych technologii teleinformatycznych. Do zadań Biura należy w szczególności nadzorowanie, koordynowanie i wspieranie ukierunkowanych na zwalczanie cyberprzestępczości działań prowadzonych przez komendy wojewódzkie (i stołeczną) Policji w zakresie czynności operacyjno-rozpoznawczych oraz współdziałanie z Centralnym Biurem Śledczym Policji w tym zakresie. Nowo powołane Centralne Biuro Zwalczania Cyberprzestępczości CBZC zgodnie z ustawą z 17 grudnia 2021 r. stanowi jednostkę organizacyjną Policji właściwą w sprawach zwalczania cyberprzestępczości, odpowiedzialną za realizację na obszarze całego kraju zadań w zakresie rozpoznawania, zapobiegania i zwalczania przestępstw popełnionych

przy użyciu technologii teleinformatycznych oraz wspierania w niezbędnym zakresie pozostałych jednostek organizacyjnych Policji w rozpoznawaniu, zapobieganiu i zwalczaniu przestępstw. Funkcjonariuszom CBZC będzie przysługiwać w pełni możliwość prowadzenia działań operacyjno-rozpoznawczych, dochodzeniowo-śledczych oraz administracyjno-porządkowych wynikających z ustawy o Policji.

Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni powołane zostało 1 czerwca 2013 r. przez Ministerstwo Obrony Narodowej na podstawie *Zarządzenia Nr 10/MON* z dnia 29 kwietnia 2013 r. jako Narodowe Centrum Kryptologii. Od 5 marca 2019 r. nosi obecną nazwę. Do jego zadań należy monitoring, analiza i aktywne reagowanie w przypadku incydentów naruszających bezpieczeństwo sieci i jej użytkowników. W tym celu m.in. prowadzi badania dotyczące metod wykrywania incydentów w cyberprzestrzeni (w tym do analizy złośliwego oprogramowania) oraz ochrony informacji (w tym kryptograficzne).

2.2. Bezpieczeństwo antyterrorystyczne obszarów morskich RP

Bezpieczeństwo polskich obszarów morskich określają zapisy kilku aktów prawnych. W szczególności są to ustawy: *z dnia 21 marca 1991 r. o obszarach morskich Rzeczypospolitej Polskiej i administracji morskiej, z dnia 18 sierpnia 2011 r. o bezpieczeństwie morskim, z dnia 4 września 2008 r. o ochronie żeglugi i portów morskich, z dnia 12 października 1990 r. o ochronie granicy państwowej, z dnia 12 października 1990 r. o Straży Granicznej, z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*.

Przepisy tych ustaw regulują funkcjonowanie i uprawnienia szeregu organów państwowych, które posiadają zarówno zróżnicowane kompetencje jak i zasoby. Zróżnicowanie dotyczy także możliwych obszarów działania poszczególnych służb. O ile przepisy dotyczące obszarów morskich oraz zakresu działania Straży Granicznej pozwalają na podjęcie działań w ramach kompetencji tych organów na obszarze wód wewnętrznych, wód terytorialnych oraz wyłącznej strefy ekonomicznej, to *Ustawa o działaniach antyterrorystycznych* zawęża zakres działań do polskiej strefy odpowiedzialności SAR (Search and Rescue), która nie jest tożsama z wyłączną strefą ekonomiczną i obejmuje inne obszary południowego Bałtyku.

W przypadku instytucji cywilnych upoważnienia administracji rządowej związane z korzystaniem z morza posiadają **terenowe organy administracji morskiej**. Na mocy

Ustawy o ochronie żeglugi dyrektor właściwego urzędu morskiego ma prawo wydawać statkom wiążące polecenia (np. zajęcia określonej pozycji lub zakazać wyjścia z portu) w celu zapobieżenia lub ograniczenia zagrożenia ochrony żeglugi i portów. Z kolei **Morska Służba Poszukiwania i Ratownictwa** jest służbą właściwą w zakresie ochrony życia ludzkiego na morzu i dysponuje w tym celu wyszkolonym personelem i sprzętem w postaci statków ratowniczych i środków brzegowych. **Straż Graniczna** ustawowo upoważniona jest do nadzoru nad eksploatacją polskich obszarów morskich oraz przestrzeganiem przez statki przepisów obowiązujących na tych obszarach i posiada uprawnienia do zatrzymywania i kontroli jednostek pływających w granicach wyznaczonych przepisami ustaw oraz użycia środków przymusu, w tym broni palnej, także wobec jednostek pływających. Posiada wyspecjalizowany oddział morski (**Morski Oddział Straży Granicznej**) wyposażony w jednostki pływające różnych typów, w tym statki patrolowe typu SKS-40, a w jego składzie znajduje się także pododdział specjalny przygotowany do działania na pokładach jednostek pływających. W skład tej służby wchodzi także komponent lotniczy wyposażony w śmigłowce i samoloty patrolowe. Wreszcie Policja oraz inne służby wykonują na wybrzeżu i polskich obszarach morskich (zwłaszcza wodach wewnętrznych i morzu terytorialnym) swoje ustawowe zadania, przy czym należy zauważyć, że ich zakres jest uzależniony od zasobów sprzętowych. **Policja** posiada w tym zakresie ograniczone możliwości, dysponując jedynie łodziami motorowymi o małej dzielności morskiej. Ponadto w jej składzie funkcjonuje służba kontrterrorystyczna a część pododdziałów przygotowana jest do działania w środowisku wodnym (w tym morskim).

Z kolei zdolności Sił Zbrojnych Rzeczypospolitej Polskiej do działania w środowisku morskim skoncentrowane są przede wszystkim w dwóch związkach taktycznych **Marynarki Wojennej**: **3. Flotylli Okrętów** i **8. Flotylli Obrony Wybrzeża.** Te zasoby uzupełniają siły innych komponentów (w tym **Wojsk Specjalnych**) oraz lotnictwa (zwłaszcza lotnictwa morskiego: **Brygada Lotnictwa Marynarki Wojennej**). Siły Zbrojne posiadają zdolności w zakresie rozpoznania i obserwacji sytuacji na polskich obszarach morskich, rażenia celów nawodnych, zwalczania okrętów podwodnych oraz rozpoznania i neutralizacji zagrożenia minowego. Szczegółowe zdolności zależne są od możliwości sił okrętowych, brzegowych i lotniczych. Siły Zbrojne wspierają także działania ratownicze, zwłaszcza przy pomocy samolotów patrolowych i śmigłowców poszukiwawczo-ratowniczych.

Mając na uwadze uwarunkowania działań antyterrorystycznych i kontrterrorystycznych należy zauważyć, że najważniejszymi zasobami w zakresie przeciwdziałania i reagowania na zagrożenia terrorystyczne dysponują Straż Graniczna oraz Siły Zbrojne, przede wszystkim Marynarka Wojenna. To te formacje posiadają takie zasoby

jak Zautomatyzowany System Radarowego Nadzoru Straży Granicznej czy punkty obserwacyjne Marynarki Wojennej.

Co więcej, to wojsko lub Straż Graniczna mogą podjąć działania na obszarach morskich wykorzystując jednostki pływające oraz statki powietrzne. W szczególności jednostki pływające w postaci statków Straży Granicznej oraz okrętów Marynarki Wojennej pozwalają na długotrwałe przebywanie na obszarach morskich, co pozwala potencjalnie na pozyskiwanie informacji o zagrożeniach oraz zapobieganie im poprzez działania prewencyjne – nawet przez sam fakt aktywnego patrolowania danego akwenu. Zdolności tej nie zapewniają komponenty brzegowe. Jednostka pływająca jest bowiem z uwagi na swoją specyfikę platformą dla urządzeń rozpoznawczych (sensorów) oraz uzbrojenia (efektorów). Należy przy tym także pamiętać, że jednostki pływające pozwalają na użycie sił jednostek kontrterrorystycznych, które należy przetransportować w rejon prowadzonych działań. Długotrwały przerzut przy pomocy tylko łodzi specjalnych jest utrudniony z uwagi na ich konstrukcję i parametry. Z kolei zdolności statków powietrznych pozwalają na szybką reakcję na zaistniałe zdarzenie, w tym na przerzut osób i sprzętu, jednak przy znacznie krótszym czasie, w którym śmigłowiec lub samolot mogą przebywać w nakazanym obszarze. Dla statków powietrznych jest to okres maksymalnie kilku godzin, podczas gdy dla jednostek pływających mogą to być tygodnie. Wreszcie komponent lądowy w postaci brzegowych sił rakietowych MW może być użyty tylko w przypadku, gdyby zaszła konieczność zniszczenia (zatopienia) jednostki pływającej. Niepokoją w tym zakresie trwające od lat ograniczenia jakościowe i ilościowe zdolności sił okrętowych Marynarki Wojennej. Wpływa to negatywnie na zdolność do reagowania na sytuacje kryzysowe na polskich obszarach morskich.

Istotnym problemem jest również fakt, że zgodnie z *Ustawą o działaniach antyterrorystycznych*, kierującym działaniami antyterrorystycznymi jest funkcjonariusz Policji (chyba, że do zdarzenia doszłoby na obszarze lub obiekcie wojskowym – wówczas działaniami kieruje żołnierz Żandarmerii Wojskowej). O ile jest to zasadne podczas działań na lądzie, gdzie byłby to przedstawiciel formacji zapewniającej zasadnicze środki niezbędne do rozwiązania sytuacji kryzysowej, to w przypadku obszarów morskich zasoby te będą zapewniane przez inne służby, dysponujące własnymi systemami dowodzenia i działające w sposób odmienny od środowiska lądowego.

2.3. Polski system przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu

a. Związek między terroryzmem a przestępczością finansową

Finansowanie organizacji terrorystycznych dokonywane jest m.in. przez finansowanie społecznościowe czy działalność organizacji typu *non-profit*, jak również przy wykorzystaniu systemu handlowego. Grupy przestępcze i organizacje terrorystyczne wykorzystują go do prania pieniędzy i transferu wartości pieniężnych pochodzących z popełnionych czynów zabronionych prawem wykorzystując do tego transakcje handlowe (ang. *Trade Based Money Laundering*) – zarówno fikcyjne, jak i prawdziwe, lecz dokonywane na podstawie fałszywych lub błędnie wypełnionych dokumentów przewozowych i celnych.

Najbardziej rozpowszechniona technika prania pieniędzy przy wykorzystaniu transakcji handlowych polega na podawaniu fałszywych wartości towarów będących przedmiotem transakcji bądź ich wolumenu poprzez:

- zaniżanie lub zawyżanie rzeczywistej wartości towaru na fakturach VAT – w pierwszym przypadku mechanizm ów pozwala na przeniesienie wartości finansowych od eksportera do importera, który dokona zapłaty za towar po niższej cenie niż wynosi jego wartość handlowa na wolnym rynku (importer zyskuje możliwość odsprzedaży towaru z większym zyskiem), w drugim zaś na przeniesienie wartości finansowych od importera do eksportera, poprzez dokonanie płatności powyżej rzeczywistej wartości towaru;
- wielokrotne wystawianie faktur dla tego samego towaru;
- zawyżanie lub zaniżenie wolumenu towarów wysłanych w stosunku do wolumenu towarów figurującej na dokumentach przewozowych;
- podawanie na fakturach VAT i dokumentach przewozowych lub celnych niezgodnego z prawdą opisu towarów co do jego rodzaju lub jakości;
- w skrajnych przypadkach dokonywanie tylko i wyłącznie obrotu dokumentacją przewozową lub celną bez dokonywania faktycznego obrotu towarowego.

b. Ochrona interesów finansowych państwa

Organy ochrony interesów finansowych państwa stanowią ważny element systemu antyterrorystycznego RP, przede wszystkim w obszarze przeciwdziałania nielegalnemu wykorzystaniu obrotu towarowego oraz przepływów finansowych mających służyć

wspieraniu działalności organizacji terrorystycznych. Śledzenie i analiza transakcji handlowych oraz finansowych jest nieodzowne w celu wykrycia ewentualnych powiązań między organizacjami terrorystycznymi, grupami przestępczymi i prywatnymi osobami działającymi na ich rzecz. Jednak wykrycie pozyskiwania przez organizacje terrorystyczne środków finansowych np. pod przykryciem legalnie funkcjonujących podmiotów gospodarczych lub organizacji pozarządowych stanowi dla właściwych organów i służb szczególne wyzwanie.

Organami informacji finansowej w polskim systemie prawnym są: minister właściwy ds. finansów publicznych oraz **Generalny Inspektor Informacji Finansowej** (dalej: Generalny Inspektor, GIIF). Generalny Inspektor w zakresie przeciwdziałania finansowaniu terroryzmu współpracuje z Szefem ABW. GIIF we współpracy z Centrum Antyterrorystycznym ABW poddaje analizie powiązania z osobami lub podmiotami z krajów o podwyższonym ryzyku terrorystycznym i identyfikuje związki tych osób z organizacjami terrorystycznymi. W 2021 r. wprowadzono sześcioletnią kadencję pełnienia funkcji GIIF, która może być pełniona maksymalnie dwukrotnie, oraz zakaz przynależności Generalnego Inspektora do partii politycznej.

Międzyresortowy **Komitet Bezpieczeństwa Finansowego**, który pełnił funkcje opiniodawczą i doradczą w zakresie stosowania szczególnych środków ograniczających przeciwko osobom, grupom i podmiotom, został zastąpiony Komitetem Bezpieczeństwa Finansowego pełniącym funkcje opiniodawczą i doradczą w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu. Tym samym została wzmocniona pozycja Generalnego Inspektora poprzez rozszerzenie zakresu merytorycznego odpowiedzialności Komitetu, rozszerzenie jego składu oraz uczynienie go wiodącym organem odpowiedzialnym za obszar bezpieczeństwa finansowego w zakresie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu.

Zgodnie z opublikowaną w połowie 2019 r. przez GIIF *Krajową oceną ryzyka prania pieniędzy oraz finansowania terroryzmu* zagrożenie finansowania terroryzmu na terytorium RP, podobnie jak samo zagrożenie terrorystyczne, jest obecnie niskie. Pojawia się jednak zastrzeżenie, że Polska może być uznawana za kraj atrakcyjny dla budowania zaplecza logistycznego i finansowego przez organizacje terrorystyczne. Największy poziom prawdopodobieństwa w zakresie finansowania terroryzmu został przypisany fizycznemu przewozowi przez granice wartości majątkowych przy wykorzystaniu osób fizycznych. Relatywnie wysoko oszacowano również ten poziom dla wykorzystania usług kurierskich i pocztowych do przewozu przez granice pieniędzy pochodzących z nielegalnych źródeł. Oprócz tego wskazano ryzyka dla takich obszarów, jak: waluty wirtualne, usługi telekomunikacyjne powiązane z płatnościami mobilnymi, finansowanie

społecznościowe, usługi płatnicze (oferowane przez inne podmioty niż banki), działalność organizacji typu *non-profit*, ubezpieczenia oraz bankowość.

c. Strategia przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu

19 kwietnia 2021 r. Rada Ministrów przyjęła *Strategię przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu*. Dokument zawiera trzy sekcje: (1) Rozwój krajowego systemu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, (2) Plan działań oraz (3) Monitorowanie realizacji planu działań.

Zwiększenie efektywności polskiego systemu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu wymaga podjęcia działań w czterech obszarach, tj.: (1) uzupełnienia regulacji prawnych, (2) rozwoju szkoleń (zarówno pracowników jednostki analityki finansowej, jak również jednostek współpracujących oraz instytucji obowiązanych), (3) wymiany informacji przy wykorzystaniu dokumentów elektronicznych i systemów teleinformatycznych, a także (4) generowania danych statystycznych umożliwiających obiektywną ocenę skuteczności krajowego systemu AML/CFT (Anti-Money Laundering/Counter Financing of Terrorism).

W Strategii przedstawiono następujące priorytety rozwoju krajowego systemu AML/CFT:

1. **Zwiększenie skuteczności** działania jednostki analityki finansowej i jednostek współpracujących w zakresie **analizy informacji** poprzez wykorzystanie podejścia opartego na ryzyku.

2. **Dostosowanie katalogu instytucji obowiązanych i ich obowiązków** do pojawiających się zagrożeń oraz potrzeb informacyjnych.

3. **Harmonizacja i usprawnienie zasad nadzoru i kontroli** nad instytucjami obowiązanymi.

4. **Optymalizacja** trybu, zakresu i jakości **wymiany informacji** oraz dostępu do informacji.

5. Zorganizowanie **skutecznego systemu szkoleń** oraz wymiany wiedzy i doświadczeń.

6. Określenie **jednolitych zasad generowania informacji**, w szczególności danych statystycznych potrzebnych do przeprowadzania oceny skuteczności krajowego systemu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu i jej elementów.

Realizację działań przewidzianych w *Strategii* rozłożono na lata 2021–2023, aby była ona powiązana z *Krajową oceną ryzyka prania pieniędzy oraz finansowania terroryzmu*, która powinna być aktualizowana nie rzadziej niż raz na 2 lata.

d. Raport MONEYVAL Rady Europy

Założenia *Strategii* pokrywają się z kluczowymi wnioskami będącymi rezultatem piątej rundy ewaluacyjnej w zakresie zgodności polskiego systemu przeciwdziałania praniu pieniędzy oraz finansowania terroryzmu z zaleceniami FATF (Financial Action Task Force) przeprowadzonej przez Komitet MONEYVAL Rady Europy. Raport został przyjęty podczas 62. sesji plenarnej Komitetu MONEYVAL 16 grudnia 2021 r. Na podstawie przeprowadzonej ewaluacji stwierdzono, że Polska musi poprawić ramy regulacyjne i zwiększyć środki przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, zaś wśród elementów wymagających poprawy wskazano m.in.:

- konieczność wykorzystania w szerszym zakresie analiz GIIF podczas prowadzonych postępowań prokuratorskich;
- wzmocnienie mechanizmów kontroli środków pieniężnych na granicy poprzez zapewnienie podstawy prawnej do zatrzymania, ograniczenia lub zajęcia podejrzanego mienia;
- podjęcie działań w celu zdefiniowania finansowania terroryzmu jako odrębnego przestępstwa, a nie jako przestępstwa pochodnego wobec terroryzmu;
- wsparcie dochodzeń w sprawach finansowania terroryzmu dodatkowymi wytycznymi i procedurami;
- prowadzenie śledztw finansowych nie tylko w sprawach związanych z finansowaniem terroryzmu, ale także w przypadkach podejrzenia co do legalności lub przeznaczenia środków finansowych;
- uwzględnienie podatności organizacji non-profit na ryzyko finansowania terroryzmu;
- stosowanie konfiskaty środków pochodzących z prania pieniędzy i finansowania terroryzmu jako celu polityki organów ścigania;
- konieczność opracowania przez właściwe organy jednorodnej praktyki w celu usprawnienia śledzenia aktywów.

Ze względu na niedociągnięcia Polska została objęta rozszerzonym monitorowaniem ze strony Komitetu MONEYVAL procesu wdrażania zaleceń ewaluacyjnych.

2.4. Wybrane zmiany organizacyjno-prawne wspólnoty AT w RP

a. Międzyresortowy Zespół do Spraw Zagrożeń Terrorystycznych (MZdZT)

8 kwietnia 2021 r. weszło w życie *Zarządzenie Nr 37 Prezesa Rady Ministrów zmieniające zarządzenie w sprawie utworzenia Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych*, w którym wprowadzono następujące zmiany:

1) **§ 2 otrzymuje brzmienie:**

„§ 2. 1. Zespół zapewnia współdziałanie administracji rządowej w zakresie przygotowania do zapobiegania zdarzeniom o charakterze terrorystycznym, przejmowania nad nimi kontroli w drodze zaplanowanych przedsięwzięć oraz do reagowania na nie.

2. Do podstawowych zadań Zespołu należy:

1) monitorowanie zagrożeń o charakterze terrorystycznym, ich analiza i ocena, a także przedstawianie opinii i wniosków Radzie Ministrów;

2) opracowywanie projektów standardów i procedur w zakresie reagowania w przypadku wystąpienia zdarzeń o charakterze terrorystycznym;

3) inicjowanie, koordynowanie i monitorowanie działań podejmowanych przez właściwe organy administracji rządowej w zakresie przygotowania do zapobiegania zdarzeniom o charakterze terrorystycznym, przejmowania nad nimi kontroli w drodze zaplanowanych przedsięwzięć oraz do reagowania na nie;

4) opracowywanie propozycji zmierzających do usprawnienia metod i form zapobiegania zdarzeniom o charakterze terrorystycznym, przygotowania do przejmowania kontroli nad tymi zdarzeniami i reagowania w przypadku wystąpienia takich zdarzeń oraz występowanie z wnioskiem do właściwych organów o podjęcie w tym zakresie prac legislacyjnych.”;

2) w § 4:

a) po ust. 2 dodaje się ust. 2a w brzmieniu:

„2a. Zespół rozpatruje sprawy na posiedzeniach albo w drodze korespondencyjnego uzgadniania stanowisk, w tym za pomocą środków komunikacji elektronicznej.”,

b) ust. 3 otrzymuje brzmienie:

„3. Posiedzenia Zespołu zwołuje przewodniczący z własnej inicjatywy lub na wniosek jednego z członków Zespołu.”.

Następnie 13 października 2021 r. Prezes Rady Ministrów podpisał *Wytyczne w sprawie koordynacji wymiany informacji o zagrożeniach terrorystycznych*, których projekt opracowano w ramach MZdZT. W 2022 r. w ramach Zespołu dokonano również aktualizacji *Decyzji nr 41 Przewodniczącego MZdZT z dnia 2 listopada 2020 r. w sprawie powołania zespołu zadaniowego – Stałej Grupy Eksperckiej* (doprecyzowanie roli SGE oraz umożliwienie korespondencyjnego uzgadniania stanowisk, poza trybem stałych posiedzeń). Dodatkowo w tym samym roku uchwałą nr 1/2022 MZdZT zdjęto klauzule niejawności z *Uchwały nr 2/2019 z dnia 27 sierpnia 2019 r. dot. współdziałania w sprawie oceny wiarygodności informacji o podłożeniu urządzenia wybuchowego*, jak również dokonano aktualizacji jednostek organizacyjnych Policji współpracujących w tym obszarze m.in. poprzez dodanie Centralnego Biura Zwalczania Cyberprzestępczości.

b. Legislacja antyterrorystyczna

W 2021 r. dokonano śladowej nowelizacji *Ustawy o działaniach antyterrorystycznych* z 2016 r. w wyniku wejścia w życie *Ustawy z dnia 30 marca 2021 r. o zmianie ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu oraz niektórych innych ustaw* (w art. 5.1 zaktualizowano skład instytucji biorących udział w koordynacji czynności analityczno-informacyjnych realizowanych przez Szefa ABW).

W 2022 r. dodano do *Ustawy o działaniach antyterrorystycznych* punkt 13a. w brzmieniu:

„Art. 13a. 1. Prezes Rady Ministrów, mając na względzie możliwość wystąpienia zdarzenia o charakterze terrorystycznym albo zagrożenia dla bezpieczeństwa i porządku publicznego, może, w drodze zarządzenia, ograniczyć publiczny dostęp do wykazów, rejestrów, baz danych i systemów teleinformatycznych zawierających dane lokalizacyjne infrastruktury technicznej.

2. W zarządzeniu, o którym mowa w ust. 1, wskazuje się wykazy, rejestry, bazy danych oraz systemy teleinformatyczne, do których ograniczony zostaje dostęp publiczny, oraz okres tego ograniczenia.

3. Dysponenci wykazów, rejestrów, baz danych i systemów teleinformatycznych wskazanych w zarządzeniu, o którym mowa w ust. 1, ograniczają do nich publiczny dostęp zgodnie z tym zarządzeniem niezwłocznie."

W 2023 r. planowana jest nowelizacja *Ustawy o działaniach antyterrorystycznych* oraz *Ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*, stanowiąca wdrożenie do polskiego porządku prawnego mechanizmu blokowania w Internecie treści propagujących terroryzm na mocy *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/784 z 29 kwietnia 2021 r. w sprawie zapobiegania rozpowszechnianiu w Internecie treści o charakterze terrorystycznym*.

Wnioski (#ZaleceniaAT)

W Raporcie PTBN, Tom I (2020): „Zagrożenia o charakterze terrorystycznym a system antyterrorystyczny w RP", wydanym w marcu 2021 r. zdefiniowaliśmy siedem wyzwań, przed jakimi stoi Polska w kontekście budowy odporności społecznej na zagrożenia terrorystyczne oraz doskonalenia systemu antyterrorystycznego RP. W raporcie tym zaproponowaliśmy również możliwe warianty rozwiązań. #ZaleceniaAT z 2021 r. dotyczyły takich zagadnień jak:

1. wspieranie badań nad ekstremizmem politycznym oraz radykalizacją mniejszości religijnych oraz budowanie pomostów między instytucjami odpowiedzialnymi za koordynacje poziomu strategicznego systemu AT w RP (MZds.ZT) a osobami realizującymi tego typu projekty badawcze;

2. penalizacja posiadania materiałów/treści potrzebnych do popełnienie przestępstwa o charakterze terrorystycznym (z wyłączeniem działalności naukowej i edukacyjnej) oraz działania edukacyjne i informacyjne wskazujące na negatywne konsekwencje takich zachowań;

3. uchwalenie Narodowego Programu Edukacji Antyterrorystycznej w celu podnoszenie świadomości i kształtowanie właściwych mechanizmów reagowania na zagrożenia o charakterze terrorystycznym, którego koordynacją w ramach całego systemu AT w RP zajęłaby się istniejąca instytucja państwowa właściwa w zakresie profilaktyki terrorystycznej;

4. opracowanie metodyki audytu bezpieczeństwa antyterrorystycznego (podatność na fizyczne incydenty o charakterze terrorystycznym) dla siedzib konstytucyjnych organów państwa, obiektów strategicznych z uwagi na bezpieczeństwo i obronność kraju oraz wybranych obiektów infrastruktury krytycznej RP, której realizacją zajęłaby się instytucja państwowa właściwa w zakresie ochrony osób i mienia;

5. spłaszczenie procedur związanych z wykorzystaniem sił kontrterrorystycznych poprzez uproszczenie procedur ustawowych (m in. przesunięcie decyzji z poziomu resortowego na poziom taktyczny) oraz ujednolicenie w tym zakresie procedur realizacji czynności służbowych dla wszystkich formacji wykorzystywanych do wsparcia wyspecjalizowanych formacji Policji;

6. powiązanie stanów etatowych wojewódzkich sił kontrterrorystycznych oraz poziomu zdolności i gotowości do działania z możliwymi do wystąpienia zagrożeniami, w szczególności wielkością ośrodków miejskich, natężeniem ilości infrastruktury krytycznej oraz innych współczesnych celów ataków, przy jednoczesny zwiększeniu ich mobilności;

7. utworzenia zespołów mogących wspomagać podmioty systemowe ratownictwa medycznego, jak np. Rescue Task Force (Medyczne Zespoły Szybkiego/Specjalnego Reagowania – MZSR) i podjęcie prac nad rozwiązaniami włączającymi MZSR do polskiego systemu ratownictwa medycznego, a także unormowania ich zakresu kompetencji i odpowiedzialności w obszarze medycznego zabezpieczenia zdarzeń o charakterze terrorystycznym lub nadzwyczajnym.

Dwa lata później wszystkie opisane w poprzednim raporcie wzywania i #ZaleceniaAT pozostają aktualne i wymagają wdrożenia.

Dodatkowo zostają one uzupełnione o deficyty bezpieczeństwa antyterrorystycznego jakie zostały zdefiniowane w aktualnej wersji Raport PTBN. W 2023 r. proponujemy następujące #ZaleceniaAT:

- Wdrożenie postanowień Dyrektywy UE nr 2017/541 z 15 marca 2017 r. w sprawie zwalczania terroryzmu w zakresie ustanowienia pojedynczego punktu kontaktowego dla ofiar terroryzmu, aby zagwarantować obywatelom RP równe prawa w przypadku dochodzenia roszczeń powstałych na skutek ataku terrorystycznego, w wyniku którego ucierpieli.
- Poprawę zdolności w zakresie zapobiegania zdarzeniom o charakterze terrorystycznym na polskich obszarach morskich i wybrzeżu poprzez:
  - » uznanie wyłącznej strefy ekonomicznej jako obszaru, na którym mogą być prowadzone działania antyterrorystyczne – pozwoli to na prowadzenie działań w razie zagrożenia bezpieczeństwa żeglugi lub infrastruktury na całości obszarów morskich RP;
  - » wskazanie, że działaniami antyterrorystycznymi na obszarach morskich (lub szerzej: w obszarze właściwości miejscowej Straży Granicznej) może kierować funkcjonariusz tej formacji lub bezpośrednio oficer Marynarki Wojennej;

- zapewnienie obiektom portowym, zlokalizowanym na obszarach morskich (platformy wydobywcze, fermy wiatrowe) oraz położonym na wybrzeżu (w tym projektowanej elektrowni jądrowej) ochrony przed działaniami terrorystycznymi, w tym prowadzonymi z wykorzystaniem bezzałogowych pojazdów podwodnych i bezzałogowych statków powietrznych;
- rozwój potencjału morskich komponentów sił zbrojnych oraz formacji policyjnych w zakresie zapewnienia bezpieczeństwa antyterrorystycznego i antysabotażowego na obszarach morskich, w tym do ochrony posiadanych platform wiertniczych;
- dążenie do posiadania możliwie uniwersalnych okrętów przeznaczonych do wykonywania zadań na równi w czasie pokoju, kryzysu oraz wojny. Trzonem tych sił powinny być wielozadaniowe fregaty, okręty podwodne oraz samoloty i śmigłowce lotnictwa morskiego, wspierane przez siły przeciwminowe. Określając przyszłość komponentu patrolowego należy uwzględnić wykonywanie przez te jednostki zadań także w czasie kryzysu i wojny. Zdolności potrzebne na czas wojny pozwalają bowiem na skuteczne wykonywanie zadań także w czasie pokoju i kryzysu, zwłaszcza w zakresie wsparcia działań kontrterrorystycznych i ochrony infrastruktury krytycznej;
- dokonanie oceny zdolności do prowadzenia działań kontrterrorystycznych w środowisku morskim, w tym określenie najbardziej prawdopodobnych scenariuszy prowadzenia działań kontrterrorystycznych. W szczególności należy zwrócić uwagę na uniknięcie dublowania kompetencji i zadań między różnymi formacjami. Należy wskazać jedną lub dwie służby i ich komponenty jako wiodące i w nich koncentrować zasoby kadrowe, sprzętowe i szkoleniowe.

- Systematyczne (przy użyciu narzędzi statystycznych) monitorowanie indykatorów narastania potencjalnego zagrożenia terrorystycznego: (a) niepolitycznych przestępstw z użyciem przemocy (zwłaszcza ciężkiej i technicznie zaawansowanej), (b) mowy nienawiści, pochwał przemocy i nawoływania do przemocy w przestrzeni publicznej (odnoszące się nie do wybranych grup, lecz wszystkich uczestników konfliktu).
- Transferowanie norm z zakresu zwalczania cyberprzestępczości i cyberterroryzmu z obszaru prawa karnego do prawa administracyjnego.
- Aktualizację *Krajowej oceny ryzyka prania pieniędzy oraz finansowania terroryzmu* (nie była aktualizowana od 2019 r.).

Treść Raportu zawiera wyłącznie prywatne poglądy autorów i nie mogą być one utożsamiane z instytucjami, których autorzy są pracownikami

Wybrana bibliografia

Publikacje zwarte:

Bolechów B., *Słowa w cieniu mieczy – Dabiq i narracja państwa islamskiego*, Wrocław: Wydawnictwo Uniwersytetu Wrocławskiego, 2020.

Burczaniuk P., *Legal aspects of the European inteligence services' activities,* Warsaw: Wydawnictwo ABW, 2022.

Cymerski J., Zubrzycki W., *Terroryzm i sposoby jego finansowania*, Szczytno: Wydawnictwo WSPol, 2022.

Cymerski J., Zubrzycki W., *Terroryzm/Antyterroryzm dwie dekady po zamachach z 11/9*, Szczytno: Wydawnictwo WSPol, 2023.

Encyklopedia Bezpieczeństwa Wewnętrznego. Warszawa: INP UW – ELIPSA, 2021.

Izak K., *Leksykon organizacji i ruchów islamistycznych*. Warszawa: Dialog, 2014.

Hołub A., *Ekstremizm i radykalizm wobec państwa*, Szczytno: Wydawnictwo WSPol, 2020.

Olech A., *French and polish fight against terrorism*, Poznań: Kontekst Publishing House, 2022.

Olech A., *Walka z terroryzmem polskie rozwiązania a francuskie doświadczenia*, Warszawa: Difin, 2021.

Olender D., *Przeciwdziałanie i zwalczanie piractwa morskiego*, Warszawa: Difin, 2017.

Olejnik Ł., Kurasiński A., *Filozofia cyberbezpieczeństwa*, Warszawa: PWN, 2022.

Piasecka P., Maniszewska K., Borkowski R. (red.), *Dwie dekady walki z terroryzmem*, Warszawa: Difin, 2022.

Piekarski M., *Ewolucja Sił Zbrojnych RP w latach 1990-2020 w kontekście kultury strategicznej*, Toruń: Wydawnictwo Adam Marszalek, 2022.

Piekarski M., Wojtasik K., *Polski system antyterrorystyczny a realia zamachów drugiej dekady XXI wieku*. Toruń: Wydawnictwo Adam Marszalek, Toruń 2020.

Piekarski M., *Ochrona infrastruktury krytycznej na polskich obszarach morskich w kontekście zagrożeń hybrydowych*, Ekspertyzy PTBN, nr 1 (2023), Warszawa 2023.

Poradnik Prewencji Terrorystycznej, Warszawa: Centrum Prewencji Terrorystycznej ABW, 2022.

Rękawek K., *Foreign Fighters in Ukraine – The Brown–Red Cocktail*, Abingdon-on-Thames: Routledge 2022.

Wiśniewska-Paź B., Szlachter D. (red.), *XX-lecie Wojny z terroryzmem – bilans i konsekwencje* (Tom I: *Współczesne zagrożenia, strategie reagowania, edukacja*), Toruń: Wydawnictwo Adam Marszalek, 2022.

Wiśniewska-Paź B., Szlachter D. (red.), *XX-lecie Wojny z terroryzmem – bilans i konsekwencje* (*Tom II: Infrastruktura krytyczna, analizy, case study*), Toruń: Wydawnictwo Adam Marszalek, 2022.

Wojtasik K., *Ścieżki radykalizacji i działalności dżihadystycznych organizacji terrorystycznych*, Toruń: Wydawnictwo Adam Marszalek, 2021.

Wojtasik K., *Anatomia zamachu.* Warszawa, Medium, 2019.

Wojtasik K., *Wyniki badania na temat percepcji zagrożeń o charakterze terrorystycznym wśród uczestników EU PSA*, Analizy PTBN, nr 1 (2023), Warszawa 2023.

Artykuły/rozdziały:

Gasztold A., Szlachter D., *The Role of Anti-Terrorist Coordination Centers in the Security Systems of Germany and Poland. A Comparative Analysis,* „Studia Politologiczne" 2022, vol. 63.

Piekarski M., *Zamachy z użyciem urządzeń wybuchowych w możliwych scenariuszach wojny hybrydowej w Polsce.* [w]: Wilk-Woś Z., Stawicki R. (red.). *Wokół bezpieczeństwa wewnętrznego i zewnętrznego: wyzwania, metody i narzędzia*, Łódź: Wydawnictwo Społecznej Akademii Nauk, 2019.

Piekarski M., *Broń strzelecka jako narzędzie ataków terrorystycznych: dotychczasowe trendy i kierunki ewolucji,* [w]: Wiśniewska-Paź B., Stelmach J. (red.) *Bezpieczeństwo antyterrorystyczne budynków użyteczności publicznej*. (T. I) Warszawa: Difin, 2021.

Szlachter D., *Dwie dekady budowy systemu AT w warunkach RP*, [w:] Piasecka P., Maniszewska K., Borkowski R. (red.), *Dwie dekady walki z terroryzmem*, Warszawa: Difin, 2022.

Szlachter D., *Dwie dekady walki z terroryzmem w warunkach RP*, [w:] Stelmach J. (red.), *Terroryzm i antyterroryzmu w opiniach ekspertów w XX rocznicę zamachów na WTC i Pentagon*, Warszawa: Difin, 2022.

Szlachter D., *Rozpoznanie i sabotowanie potencjału infrastruktury krytycznej krajów Europy Środkowowschodniej i Północnej jako przykład strategicznych celów aktywności rosyjskich służb specjalnych*, „Biuletynu Biura Analiz i Reagowania" (Rządowe Centrum Bezpieczeństwa) 2021, nr 32.

Tomasiewicz J., *Ideologia przemocy w „wieku końca ideologii': idee i ideologie w terroryzmie XXI w.* [w:] Piasecka P., Maniszewska K., Borkowski R. (red.), *Dwie dekady walki z terroryzmem*, Warszawa: Difin, 2022.

Tomasiewicz J., *The Ideological Component in 21st Century Terrorism*, "Studia Politologiczne" 2002, t. 63.

Tomasiewicz J., *Zagrożenia z przyszłości: próba ekstrapolacji*, [w:] Wiśniewska-Paź B., Szlachter D. (red.), *XX-lecie Wojny z terroryzmem – bilans i konsekwencje* (Tom I), Toruń: Wydawnictwo Adam Marszalek, 2022.

Wojtasik, K. *Implementacja tzw. załącznika AT w zakładach produkcyjnych. Doświadczenia, wnioski i rekomendacje.* [w]: Wiśniewska-Paź B., Szlachter D. (red.), *XX-lecie Wojny z terroryzmem – bilans i konsekwencje* (Tom II), Toruń: Wydawnictwo Adam Marszalek, 2022.

Raporty:

Applied Cybersecurity and Internet Governance (2022).

Country Report on Terrorism (2021-2022).

Cross-national level report on digital sociability and drivers of self-radicalisation in Europe (DARE: Dialogue about Radicalisation and Equality), bmw 2020.

EU Terrorism Situation & Trend Report (TE-SAT) (2021-2022).

Global Terrorism Index (2021-2023).

Systematic Review of Quantitative Studieson Inequality and Radicalisation (DARE: Dialogue about Radicalisation and Equality), bmw 2018.

Periodyki:

„Biuletyn Biura Analiz i Reagowania RCB" (2021-2021).

„Frag-Out" 2020-2023.

„Internal Security" (2020-2023).

„Polska Zbrojna" (2020-2023).

„Przegląd Bezpieczeństwa Wewnętrznego" (2020-2023).

„Przegląd Policyjny" (2020-2023).

„Przegląd Strategiczny" (2020-2023)

„Securo – badania nad terroryzmem" (2022).

„Special-Ops" (2020-2023).

„Studia Politologiczne" (2021-2022).

„Terroryzm. Studia, analizy, prewencja" (2022-2023).

Wydarzenia/Projekty medialne/ Nagrania audio-wideo

#20latWTC

Centrum Studiów i Edukacji na rzecz Bezpieczeństwa Uniwersytetu Wrocławskiego oraz Polskie Towarzystwo Bezpieczeństwa Narodowego zorganizowało 10 września 2021 r. konferencję pt. „20-lecie wojny z terroryzmem – bilans i perspektywy", której celem było podsumowanie dwóch dekad walki z terroryzmem na poziomie narodowym oraz międzynarodowym, a także upamiętnienie ofiar tamtych wydarzeń ze szczególnym uwzględnieniem obywateli RP.

Wydarzenie zostało objęte patronatem honorowym m.in. przez Biuro Bezpieczeństwa Narodowego, Ministerstwo Spraw Wewnętrznych i Administracji, Rządowe Centrum Bezpieczeństwa, Urząd Lotnictwa Cywilnego oraz Instytut Zachodni im. Zygmunta Wojciechowskiego.

Celem konferencji była analiza konsekwencji zamachów z 11 września w jak najszerszym aspekcie, od skutków geopolitycznych poprzez ewolucję systemów ochrony, metod i form rozpoznawania i zwalczania zagrożeń terrorystycznych, po rozwój platform bezzałogowych i sposobów udzielania pomocy medycznej ofiarom ataków terrorystycznych. Zagadnienia zostały omówione podczas paneli dyskusyjnych, sprzyjających wymianie opinii pomiędzy specjalistami reprezentującymi różne grupy zawodowe i różne perspektywy.

W konferencji uczestniczyło ponad 50 prelegentów reprezentujących kluczowe, cywilne i mundurowe, ośrodki akademickie, uznane ośrodki analityczne, największy polski portal informacyjny dedykowany bezpieczeństwu, szereg instytucji państwowych (tj. RCB,

BBN, ABW, Policję, ULC, SOP) oraz partnerzy zagraniczni reprezentujących m. in. amerykańską misję dyplomatyczną w RP, Komisję Europejską (DG HOME) i FRONTEX. #20latWTC obejrzało kilkuset widzów oglądających łącznie wszystkie transmisje on-line.

Poniższe lista nagrań z konferencji #20latWTC, które są dostępne na kanale YT, pod adresem: **https://www.youtube.com/@20latwtc27**

- Otwarcie konferencji oraz Panel nr 1: Skutki geopolityczne ataków terrorystycznych z 11 września 2001 r.
- Panel nr 2: Bezpieczeństwo przestrzeni publicznych i infrastruktury krytyczne
- Panel nr 3: Edukacja antyterrorystyczna
- Panel nr 4: Ewolucja ideologii, organizacji, strategii i taktyk grup terrorystycznych oraz kierunki działań kontrterrorystycznych
- Panel nr 5: Reforma systemów bezpieczeństwa państw członkowskich UE i NATO
- Panel nr 6: Nowoczesne technologie jako narzędzie terroryzmu drugiej dekady XXI w.
- Panel nr 7: Metody analizy i oceny zagrożeń o charakterze terrorystycznym

Polskie Towarzystwo Bezpieczeństwa Narodowego jest interdyscyplinarnym towarzystwem naukowym skupiającym badaczy zajmujących się różnymi dziedzinami bezpieczeństwa.

Celem Towarzystwa jest rozwój i upowszechnianie wiedzy na temat budowania odporności państwa wobec zagrożeń dla bezpieczeństwa narodowego i międzynarodowej pozycji Rzeczypospolitej Polskiej.

PTBN jest członkiem ogólnoeuropejskiej sieci przeciwdziałania zagrożeniom hybry--dowym EU-HYBNET. Specjalizacją PTBN w ramach EU-HYBNET jest m.in. ochrona infrastruktury krytycznej. Przedstawiciele PTBN uczestniczą również w grupie roboczej DG MOVE Komisji Europejskiej ds. systemów dronowych oraz biorą udział w inicjatywach i spotkaniach dedykowanych budowaniu odporności na zamachy terrorystyczne w przestrzeniach publicznych realizowanych przez DG HOME Komisji Europejskiej.

Członkowie Towarzystwa opracowują i wydają m.in. serię „Raport PTBN", w której analizowane są współczesne zagrożenia dla bezpieczeństwa RP i polskiej racji stanu (terroryzm, walka informacyjna w cyberprzestrzeni, nowoczesne technologie a ochrona infrastruktury krytycznej, zagrożenia hybrydowe wobec sektora energetycznego na lądzie i na morzu).

Każdy Raport PTBN zawiera zalecenia dla organów i instytucji państwowych, a także kluczowych podmiotów gospodarczych z punktu, których zadaniem jest zapewnienie ciągłości funkcjonowania gospodarki i państwa.

Dotychczas ukazały się:

» Raport PTBN, Tom I (2020): „Zagrożenia o charakterze terrorystycznym a system antyterrorystyczny w RP",
» Raport PTBN, Tom II (2021): „Bezpieczeństwo infrastruktury krytycznej wobec zagrożeń ze strony platform bezzałogowych",
» Raport PTBN, Tom III (2022): „Zagrożenia informacyjne dla infrastruktury krytycznej na przykładzie technologii 5G".W 2023 r.

PTBN wprowadził dwie nowe serie specjalistyczne: „Ekspertyzy PTBN" oraz „Analizy PTBN", w ich ramach dotychczas ukazały się następujące publikacje:

- Piekarski M., Ochrona infrastruktury krytycznej na polskich obszarach morskich w kontekście zagrożeń hybrydowych, Ekspertyzy PTBN, nr 1 (2023), Warszawa 2023.
- Wojtasik K., Wyniki badania na temat percepcji zagrożeń o charakterze terrorystycznym wśród uczestników EU PSA, Analizy PTBN, nr 1 (2023), Warszawa 2023.

BEZPIECZEŃSTWO PONAD PODZIAŁAMI

www.PTBN.online