RCB
Rządowe Centrum Bezpieczeństwa

BIURO
ANALIZ I REAGOWANIA

BIULETYN

KWARTALNY

NUMER 32 STYCZEŃ – MARZEC 2021

Zespół redakcyjny

Biuletynu kwartalnego Rządowego Centrum Bezpieczeństwa:

Grzegorz Świszcz

Martyna Olejnik-Kołodziej

Anna Zasadzińska-Baraniewska

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

Terroryzm aktualnym wyzwaniem

Stanisław Żaryn
Rzecznik Ministra Koordynatora Służb Specjalnych,
Dyrektor Departamentu Bezpieczeństwa Narodowego KPRM

W marcu minęło pięć lat od zamachów terrorystycznych w Belgii, które pochłonęły życie ponad 30 ofiar. Od tego czasu, o czym przypomniał ostatnio szef NATO, dochodziło do kolejnych ataków, organizowanych przez islamskich zabójców w różnych częściach świata. Jens Stoltenberg pisał o zamachach w Paryżu, Londynie, Kabulu, Christchurch. Lista jest jednak znacznie dłuższa. Informacje o zamachach pojawiają się systematycznie w mediach, bowiem zagrożenie terroryzmem nie zniknęło. Terroryzm islamski pozostaje wyzwaniem dla państw i narzędziem zastraszania społeczeństw. Choć poziom zagrożenia zamachami na terytorium RP jest niski, Polska również nie jest wolna od zagrożeń związanych z terroryzmem. Także dla polskiego państwa terroryzm, radykalizacja pozostają wieloelementowym wyzwaniem, które wymaga od służb ciągłej pracy. Jesteśmy członkiem kampanii antyterrorystycznej, bierzemy udział w operacjach NATO i UE, więc musimy liczyć się z możliwością wrogich działań odwetowych. Ponadto, położenie geograficzne sprawia, że Polska jest atrakcyjnym krajem do prób tworzenia zaplecza logistycznego.

Mimo relatywnie dobrej sytuacji, Polska musi kwestie zagrożeń terrorystycznych traktować poważnie. Z jakimi wyzwaniami się mierzymy pokazała nam choćby sprawa z 2016 roku, kiedy Agencja Bezpieczeństwa Wewnętrznego zatrzymała Mourada T., który usłyszał zarzuty związane z działalnością terrorystyczną. Jak wynikało z materiałów ABW, Marokańczyk brał udział w spotkaniach z najważniejszymi bojownikami ISIS, którzy odpowiadali za zamachy w Europie Zachodniej. T. miał m.in. organizować szlaki przemieszczania się po Europie jednego z najgroźniejszych bojowników Państwa Islamskiego. Ostatecznie sąd skazał T. jedynie za drobniejsze przestępstwa, jednak ta sprawa powinna budzić do refleksji dotyczącej zagrożeń terrorystycznych w naszym kraju. Ustalenia ABW wskazały bowiem, że w Polsce lokowani są ludzie stanowiący zaplecze logistyczne dla dżihadu. Od 2016 roku 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.

O tym, jak ważne jest wczesne identyfikowanie zagrożeń i działań „zaplecza", możemy się przekonać przy okazji niemal każdego zamachu terrorystycznego, który jest finalnym etapem działań dżihadystów. Udowadnia to choćby przykład zamachu na WTC z 2001 roku. W jego przygotowanie zaangażowana była komórka terrorystyczna działająca z Hamburga. Atak w USA był finalnym etapem wcześniej prowadzonych działań, skoordynowanych od strony logistycznej i finansowej. Efekt finalny pracy zaplecza terrorystów zobaczył cały świat – porwane przez terrorystów samoloty uderzyły w wieże World Trade Center w Nowym Jorku oraz w siedzibę Pentagonu w Waszyngtonie. Ten i inne zamachy pokazują, że identyfikowanie zagrożeń na wcześniejszym etapie – na etapie prac logistycznych – jest kluczowe dla neutralizowania zagrożeń. Autorzy każdego zamachu potrzebują bowiem finansów, ludzi i sprzętu, by wprowadzić swoje zbrodnicze plany w życie.

Na co przede wszystkim służby zwalczające zagrożenia terrorystyczne powinny zwracać uwagę? Jednym z elementów niezbędnych do przeprowadzenia zamachu jest broń, czy materiały wybuchowe. Samobójca z Ansbach, który zaatakował w 2016 r., dokonał ataku z wykorzystaniem bomby umieszczonej w plecaku. Zamachowcy z Paryża, którzy przeprowadzili trzy eksplozje, dysponowali również bronią palną. Podobnie było podczas ataku na Polach Elizejskich w Paryżu w 2017 r., gdzie zamachowcy posłużyli się bronią automatyczną. Zamachowiec z Wiednia strzelał do ludzi z karabinku automatycznego. Te przypadki pokazują, jak ważne jest monitorowanie dostępu do broni palnej, która często służy do masowych morderstw. Większym wyzwaniem staje się stosowana w ostatnich latach taktyka wykorzystywania przez islamskich terrorystów sprzętów zwykłego użytku, np. noży. Taką broń wykorzystał choćby agresor w Szwecji w marcu br.

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

Wyzwaniem dla służb pozostaje nie tylko monitorowanie dostępu terrorystów do broni palnej, czy broni białej, ale także zjawisko finansowania terroryzmu. W ostatnich miesiącach Agencja Bezpieczeństwa Wewnętrznego odnotowała w tym zakresie sukces, zatrzymując dwóch Irakijczyków, którzy zostali oskarżeni o finansowanie Państwa Islamskiego. Wykorzystywali do tego nieoficjalny system finansowy, tzw. Hawala. To między innymi za jego pośrednictwem pieniądze na terroryzm płyną z całego świata. Mechanizm oparty na przekazach odbywających się poza oficjalnym systemem finansowym czy bankowym jest ogromnym wyzwaniem dla służb zajmujących się identyfikowaniem przypadków finansowania terroryzmu. Służbom specjalnym państw walczących z terroryzmem rzadko udaje się namierzyć takie przekazy, co tylko dowodzi trudności związanych z identyfikowaniem osób zaangażowanych w zbieranie funduszy na dżihad. Zadanie to komplikują jeszcze uwarunkowania światowego systemu finansowego. W dobie cyfryzacji i dostępu do nowych technologii, przepływy środków finansowych mają zasięg globalny, wiążą podmioty z różnych miejsc na świecie. Tymczasem każda próba transferu środków z przeznaczeniem ich na finansowanie terroryzmu powinna zostać zablokowana. Państwa nie mogą bagatelizować tej sprawy, bowiem przestępstwo finansowania terroryzmu polega nie tylko na finansowaniu aktów terrorystycznych, ale również innych aktywności grup terrorystycznych, tj. werbunku, szkolenia, transportu, zdobywania fałszywych dokumentów, czy publikacji materiałów propagandowych. Terroryści są świadomi o jaką stawkę grają, więc zwodzą państwowe instytucje, wykorzystując choćby szyld znanych podmiotów czy organizacji charytatywnych, aby zbierać środki. Nowoczesne technologie, zwłaszcza media społecznościowe są wykorzystywane nie tylko w celu dotarcia do sympatyków, ale także przyciągnięcia darczyńców. Organizacje terrorystyczne uzyskane fundusze przeznaczają również na wynagrodzenia lub odszkodowania dla członków oraz zapewnienie im i ich rodzinom warunków bytowych.

Służby państwowe i organizacje związane ze zwalczaniem terroryzmu coraz częściej notują przypadki zdobywania środków finansowych na działalność organizacji terrorystycznych poprzez korzystanie z działań kryminalnych. Porwania dla okupu, przemyt papierosów, dóbr kultury, zasobów naturalnych, nielegalny handel bronią, narkotykami, a także handel ludźmi i wymuszenia stały się opłacanym sposobem zdobywania środków finansowych przez grupy terrorystyczne. Coraz silniejsze są powiązania między przestępczością zorganizowaną i grupami terrorystycznymi. Raport hiszpańskiego Ministerstwa Spraw Wewnętrznych z 2015 r. wskazał aż około 200 przypadków powiązań pomiędzy aktami łamania prawa o charakterze kryminalnym a działalnością terrorystyczną. Np. na terenie Barcelony i Walencji zatrzymano osoby, którym postawiono zarzuty fałszowania dokumentów, handlu ludźmi oraz narkotykami. Zyski przeznaczane były na prowadzenie działalności ekstremistycznej. Rozbito również siatkę (złożoną głównie z migrantów z Maghrebu), która zajmowała się sprzedażą substancji psychoaktywnych, a część zysków przeznaczała na finansowanie komórek dżihadystycznych. W model takich działań wpisuje się również aktywność Al.-Shabaab, tzw. somalijskich piratów. Modus operandi tej organizacji terrorystycznej polega na zdobywaniu funduszy z procederu przestępczego, tj. porywania statków morskich i żądaniu okupu. Jak widać terroryści szukają różnych sposobów na pozyskiwanie funduszy na zbrodniczą działalność.

W dobie ogólnoświatowej pandemii, organizacje terrorystyczne starają się również korzystać z nowych kanałów komunikacyjnych, by szerzyć swoją propagandę i oddziaływać na potencjalnych zwolenników islamskiego terroryzmu. Blokowanie treści o charakterze propagandowym, a także identyfikowanie osób zajmujących się propagandą terrorystyczną (w Polsce sądzonych było w ostatnich latach kilka osób w tej sprawie) to kolejne działania „na zapleczu", które są elementem skutecznego neutralizowania zagrożeń terrorystycznych. Ostatnio znaczenie tego zadania rośnie. Coraz częściej terroryści eksplorują bowiem cyberprzestrzeń i wykorzystują ją do propagowania ideologii, szerzenia propagandy, rekrutacji i zbierania funduszy, nawoływania do aktów przemocy, radykalizacji postaw, czy publikowania poradników dotyczących konstruowania ładunków wybuchowych, tudzież przeprowadzenia ataku w cyberprzestrzeni. Internet jest dziś wiodącym kanałem kontaktu ze światem, szczególnie dla osób młodych, najbardziej podatnych na socjotechnikę. Informatyzacja ułatwia szybsze rozprzestrzenianie się przekazu, w tym również treści terrorystycznych. Współczesny terrorysta sprawnie posługuje się mediami, komunikatorami czy aplikacjami.

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

Powyższa analiza wskazuje jak wiele obszarów muszą monitorować i badać służby odpowiedzialne za neutralizowanie zagrożeń terrorystycznych. Organizacje prowadzące dżihad dostosowują się do aktualnych uwarunkowań, wobec czego zwalczanie terroryzmu pozostaje wyzwaniem dla zagrożonych państw. Skuteczność działań systemu antyterrorystycznego zależy od identyfikacji zagrożeń na wczesnym etapie, ale także od profilaktyki. ABW, a w szczególności Centrum Prewencji Terrorystycznej ABW, jest specjalną jednostką Agencji dedykowaną do prowadzenia szkoleń i programów uświadamiających, jaki jest charakter aktualnych zagrożeń terrorystycznych. Rzetelna informacja oraz propagowanie właściwych postaw wzmacniają odporność społeczeństwa. Powszechna wiedza dotycząca terroryzmu jest kluczowa, by społeczeństwa były w stanie realnie oceniać zagrożenia i skalę wyzwań. Kolejnym czynnikiem kluczowym jest profesjonalna i szybka wymiana informacji między instytucjami odpowiedzialnymi za zwalczanie terroryzmu. Współpraca służb na poziomie międzynarodowym, dzielenie się wiedzą o organizacjach terrorystycznych, dżihadystach i ich sposobach działania, przynosi wymierne efekty. Terroryzm ma charakter przestępczości transgranicznej, wobec czego wymaga współdziałania.

Skuteczność w walce z terroryzmem zależy od wielu czynników. Terroryzm jest zjawiskiem wielopłaszczyznowym. Jego zwalczanie pozostanie w najbliższych latach najważniejszym zadaniem służb antyterrorystycznych na całym świecie. Polska nie jest tu wyjątkiem.

Rozpoznanie i sabotowanie potencjału infrastruktury krytycznej krajów Europy Środkowowschodniej i Północnej jako przykład strategicznych celów aktywności rosyjskich służb specjalnych

Damian Szlachter

Współzałożyciel Polskiego Towarzystwa Bezpieczeństwa Narodowego,
ekspert przy Centrum Studiów i Edukacji nad Bezpieczeństwem Uniwersytetu Wrocławskiego

Jeśli zrobilibyśmy sondaż wśród osób zajmujących się zawodowo budową odporności infrastruktury krytycznej (IK) w obszarze bezpieczeństwa fizycznego, osobowego czy teleinformatycznego pytając o kształt piramidy ryzyka dla ciągłości działania dostarczanych usług, to może się okazać, że wśród strategicznych priorytetów ochrony tego typu obiektów nie znajdzie się ochrona przed aktywnością wrogich służb specjalnych. Czy zagrożenie takie powinno być traktowane przez wszystkich operatorów IK jako mało prawdopodobne lub bliskie zeru? Dlaczego percepcja zagrożenia ze strony służb specjalnych państw wrogich RP dla obiektów, od których zależy żywotność obywateli i ciągłość sprawowania władzy jest tak marginalizowana?

Kwerenda choćby polskojęzycznych materiałów badawczo-naukowych na ten temat jest równie mocno niepokojąca. Zagrożenia dla ciągłości działania infrastruktury krytycznej państw Europy Środkowowschodniej i Północnej (należących do NATO lub UE) ze strony aktywności rosyjskich służb specjalnych pojawia się fragmentarycznie w kontekście zagrożeń hybrydowych, czyli taktyki wykorzystywanej już przeciwko II RP, a odkrytej „na nowo" po konflikcie Federacji Rosyjskiej z Gruzją w 2008 r.

Celem niniejszego materiału jest jedynie zaznaczenie, że rozpoznanie i niszczenie potencjału infrastruktury krytycznej państw Europy Środkowowschodniej i Północnej poprzez aktywność rosyjskich służb specjalnych jest rzeczywistym zagrożeniem dla ich bezpieczeństwa narodowego. Ocena tego ryzyka powstała w wyniku przeglądu wybranych historycznych materiałów dedykowanych militarnej doktrynie strategicznej FR[1] oraz incydentom opisanym w raportach służb odpowiedzialnych za bezpieczeństwo wewnętrzne krajów Europy Środkowowschodniej i Północnej. Autor liczy tym samym, na wywołanie dalszej dyskusji nad ww. problematyką i przeniesienie jej na forum debaty

[1] W trakcie opracowywania niniejszego eseju autor korzystał przede wszystkim z serii materiałów publikowanych w Przeglądzie Bezpieczeństwa Wewnętrznego (PBW) przez dr Michała Wojnowskiego, m.in.: Wojnowski M., *Paradygmat wojny i pokoju. Rola i znaczenie materializmu dialektycznego w rosyjskiej nauce wojskowej w XXI* w., PBW nr 17 (9), Emów 2017 r.

akademickiej, które powinno być inkubatorem projektów rozwiązań systemowych dla bezpieczeństwa RP.

Rosyjskie służby specjalne od początku swojego ustanowienia wykazywały szczególne zainteresowanie obiektami o znaczeniu strategicznym dla żywotności krajów ościennych i ich potencjału militarnego, które dziś możemy uznać z definicji za infrastrukturę krytyczną. Nie miało tu znaczenia, czy kraj jest wrogiem, czy sojusznikiem Rosji, ponieważ jej historyczna, bizantyjska doktryna militarna nie przewiduje czegoś takiego jak „stan pokoju". Materiały historyczne wskazują m.in. na zainteresowanie rosyjskich służb specjalnych oraz ich sowieckich kontynuatorów systemem wodociągów w dużych skupiskach miejskich. Z czasem to zainteresowanie operacyjne zostało poszerzone na system produkcji i dystrybucji energii elektrycznej. Naczelna zasada działań aktywnych w tym obszarze brzmiała przez szereg dekad tak samo – utrudniać dywersyfikację, prowadzić sabotaż opóźniający proces planowania i realizacji inwestycji w infrastrukturę krytyczną, a w przypadku ich zakończenia dokonywać rozpoznania podatności oraz luk w systemie ochrony, jak również przeprowadzać systemowe dewastacje zdolności do ciągłości działania.

Bez względu na korekty w doktrynie militarnej FR, w ramach operacyjnego modus operandi, zmianie ulegają tylko narzędzia realizacji celu, który w XXI wieku nie przeszedł strategicznego przewartościowania. Rosyjskie służby specjalne (GRU, FSB, SVR)[2] realizują działania aktywne w wielu obszarach funkcjonowania administracji państwowej przeciwnika (w formie operacyjnej, inwestycyjnej, czy prawno-instytucjonalnej), zmierzające do niszczenia jego infrastruktury krytycznej, tak aby doprowadzić do radykalnych zmian w jego sytuacji polityczno-militarnej oraz tzw. środowisku strategicznym. W militarnej doktrynie strategicznej Rosji (nadrzędnej wobec każdej innych strategii resortów siłowych) element IK to obiekt, którego brak ciągłości działania może doprowadzić do utraty kontroli nad gospodarką kraju (na poziomie lokalnym i narodowym w zależności od wielkości przeciwnika), zaburzeniem integralności terytorialnej, znacznego obniżenia odporności ludności na zagrożenia. Dodatkowo, współczesne konflikty zbrojne FR, realizowane przy wykorzystaniu prowadzonych wcześniej działań hybrydowych w tym tych o charakterze terrorystycznym, nie są ukierunkowane na niszczenie sił przeciwnika, a na paraliżowanie jego infrastruktury krytycznej (czasowym i umożliwiającym jego wtórne wykorzystanie)[3]. Przykładem tego typu strategii były ataki cybernetyczne na ukraiński system elektroenergetyczny w latach 2015-2016 r.

O tym jak wyglądało rozpoznanie i sabotowanie potencjału infrastruktury krytycznej krajów Europy Środkowowschodniej i Północnej poprzez aktywność rosyjskich służb specjalnych mówią nam doroczne raporty o stanie bezpieczeństwa państwa, publikowane przez właściwe w tym obszarze instytucje z krajów bałtyckich, skandynawskich, czy Republiki Czeskiej i RP (do 2015 r.)[4]. W poprzedniej dekadzie (2010-2019) opisywały one w sposób precyzyjny obszary i cele służb rosyjskich na ich terytorium, wymieniając również obiekty, które z uwagi na swoją rolę można kwalifikować jako narodową lub europejską infrastrukturę krytyczną (cywilną i wojskową). Należy tu wymienić następujące lokalizacje, powtarzające się w poszczególnych krajach tego regionu:

- system zaopatrzenia w energię, surowce energetyczne i paliwa (m.in. ropociągi i gazociągi tranzytowe, elektrownie jądrowe – istniejące i planowane wraz z systemem zaopatrzenia w paliwo jądrowe, infrastruktura przesyłowa energii – wysokie napięcia, połączenia energetyczne, rafinerie, gazoporty, technologie wydobywcze w warunkach arktycznych);
- system transportowy (m.in. porty morskie – cywilne i wojskowe, terminale morskie cargo, kolejowe ciągi towarowe, mosty rzeczne i przeprawy morskie);
- system sieci teleinformatycznych (m.in. cywilny i wojskowy potencjał obrony w cyberprzestrzeni oraz czas reagowania na incydenty);
- system łączności (m.in. obiekty odpowiedzialne za komunikację z NATO oraz łączność szyfrowana);
- system ochrony zdrowia (m. in. obiekty prowadzące badania w obszarze bio- i nano-technologii, farmacji).

[2] *Foreign Intelligence Service* (SVR), *Foreign Military Intelligence* (GRU), *Federal Security Service* (FSB).

[3] Za: Depczyński M., Elak L., *Rosyjska Sztuka Operacyjna u progu XXI wieku*, Fundacja Historia i Kultura, Warszawa 2020 r., s. 369-370; Baraniuk K., *Działalność służb wywiadowczych federacji rosyjskiej w świetle raportów służb specjalnych wybranych państw Unii Europejskiej*, Adam Marszałek, Toruń 2017 r.

[4] Za: Baraniuk K., *Działalność służb wywiadowczych federacji rosyjskiej w świetle raportów służb specjalnych wybranych państw Unii Europejskiej*, Adam Marszałek, Toruń 2017 r.

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

Rozpoznanie informacyjne ww. obiektów IK realizowane było poprzez wywiad agenturalny oraz wywiad lotniczy i satelitarny, ataki cybernetyczne, wywiad radioelektroniczny[5]. Warto zaznaczyć, że w ramach rozpoznania lotniczego wykorzystuje się również popularne bezzałogowe statki powietrzne (UAV).

Z początkiem nowej dekady, w optyce zainteresowania m.in. rosyjskich służb specjalnych, w prezentowanym regionie Europy pojawiły się dwa priorytetowe systemy IK. Pierwszy związany z rozwojem nowych technologii (infrastruktura telekomunikacyjna standardu 5G oraz inwestycje typu „*smart city*"), drugi będący wypadkową pandemii COVID-19 (obiekty opracowujące technologie szczepionkowe). Potwierdzają to najnowsze raporty o stanie bezpieczeństwa państwa, opublikowane w marcu 2011 r. przez norweskie i szwedzkie służby specjalne.

Raport norweskiej wspólnoty wywiadowczej z 2020 r. mówi o tym, że służba kontrwywiadowcza PST (*Politiets sikkerhetstjeneste*) odnotowuje wrogie działania państw, które wykorzystują dynamiczny rozwój technologii typu „smart city" w obiektach IK, w celu pozyskiwania informacji pozwalających na zakłócenie ich funkcjonowania. Pozyskiwane w ten sposób dane mogą być wykorzystywane do paraliżowania miast, a nawet całych regionów Norwegii. W raporcie PST wymienione są priorytetowy systemy IK podlegające wrogiemu rozpoznaniu, są to m.in. system zaopatrzenia w energię, system transportowy (kontrola ruchu drogowego), system zaopatrzenia w wodę oraz jej oczyszczanie[6].

Z kolei w opinii szwedzkiej służby SAPO (*Säkerhetspolisen*) wyrażonej w ocenie zagrożeń dla bezpieczeństwa państwa za rok 2020, wskazano na próby rozpoznania i zakłócenia funkcjonowania obiektów infrastruktury krytycznej poprzez cyberataki przy wykorzystywaniu technologii bazujących na standardzie transmisji danych 5G, która jest w tych lokalizacjach wdrażana[7].

Powyższe przypadki pokazują jak bardzo ważnym elementem bezpieczeństwa narodowego państw stanowiących „najbliższe sąsiedztwo" RP będzie w ciągu najbliższych lat cyberbezpieczeństwo IK, a tym samym zbudowanie spójnego systemu ochrony dla tego typu obiektów, który łączy uprawnienia organów administracji państwowej z możliwościami finansowo-organizacyjnymi operatorów. Równie ważnym aspektem przeciwdziałania przyszłym aktom sabotażu w obiektach IK jest ich ochrona fizyczna, osobowa na etapie planowania i realizacji samej inwestycji (IK w RP staje się obiekt ukończony, spełniający odpowiednie kryteria i dostarczający usługę).

Mając na uwadze postępujący w Polsce proces przemiany energetycznej i związane z tym projekty budowy elektrowni atomowych oraz morskich farm wiatrowych (*offshore*), jak również redefiniowanie kolejowych i drogowych szlaków transportowych związanych z budową Centralnego Portu Komunikacyjnego, w tym również remontu największych magistrali kolejowych (odpowiadających za płynność ponad ¾ krajowego ruchu kolejowego), zabezpieczenie kontrwywiadowcze i antyterrorystyczne procesu planowania inwestycyjnego i jego fizycznej realizacji powinno stanowić element składowy całego programu modernizacji systemu energetycznego i transportowego RP.

W przypadku infrastruktury krytycznej w Polsce, już dziś możemy w znaczący sposób ograniczyć możliwości pozyskiwania informacji o podatności tego typu obiektów przez wrogie państwa. Tym samym systemowo wzmacniać odporność IK na działania hybrydowe, realizowane według scenariusza rosyjskich służ specjalnych, stając się regionalnym pionierem w tym obszarze. Należy rozważyć następujące kroki, które wpisują się w unijne plany przyjęcia przyszłej Dyrektywy o odporności podmiotów krytycznych (*Proposal for a Directive of the European Parliament and of the Council on the resillience of critical entities* z 16.12.2020 r.) zapowiadanej przez obecną, portugalską Prezydencję w Radzie UE:

- wdrożenie opracowanego w latach 2017-2018 pod egidą MSWiA (Międzyresortowy Zespół ds. Zagrożeń Terrorystycznych) projektu standaryzacji ochrony IK w obszarze bezpieczeństwa fizycznego, teleinformatycznego i osobowego (tego typu rozwiązania nie oznaczają znaczącego wzrostu kosztów przeznaczanych na ochronę) – tzw. minimalne wymogi bezpieczeństwa dla funkcjonujących obiektów IK oraz tych na etapie realizacji inwestycji (projekt nowelizacji ustawy o zarządzaniu kryzysowym

[5] Za: Baraniuk K., *Działalność służb wywiadowczych federacji rosyjskiej w świetle raportów służb specjalnych wybranych państw Unii Europejskiej*, Adam Marszałek, Toruń 2017 r., s. 89-191, 217-224.
[6] *National threat assessment 2021*, PST, Oslo 2021.
[7] *Säkerhetspolisen arsbok 2020*, Sztokholm 2021, s. 9.

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

ustanawiając standaryzację bezpieczeństwa dla IK znajduje się od marca 2020 r., na etapie prac sejmowych);

- ustanowienie krajowej instytucji wiodącej odpowiedzialnej za dokonywanie testów bezpieczeństwa (fizycznego, osobowego) w obiektach IK, na wzór uprawnień posiadanych przez Urząd Lotnictwa Cywilnego w cywilnych portach lotniczych[8];
- wdrożenie obowiązkowego programu szkoleniowego z profilaktyki kontrwywiadowczej dla członków zarządów operatorów IK, realizowanego w zależności od właściwości przez ABW lub SKW;
- wypracowanie wiążących wytycznych/ rekomendacji dla operatorów IK dedykowanych podniesieniu skuteczności reagowania na incydenty naruszenia systemów bezpieczeństwa przez bezzałogowe statki powietrze[9] (opcjonalnie utworzenie wieloletniego planu finansowania programu budowy narodowego sytemu antydronowego przez NCBiR, ukierunkowanego na krajowe uczelnie techniczne).

Od praktycznego wdrożenia nowej odsłony działań hybrydowych przez FR upłynęło już kilkanaście lat. Żadna, powszechnie znana taktyka nie jest skuteczna, dlatego w tej dekadzie należy spodziewać się jej przewartościowania lub zmiany w kierunku tego, co dziś stanowi przedmiot studiów rosyjskich strategów z akademii wojskowych. To, co dziś leży na ich biurkach będzie w niedalekiej przyszłości kolejnym wyzwaniem w zapewnieniu ciągłości dziania dla obiektów infrastruktury krytycznej coraz bardziej zależnych od nowoczesnych technologii, a tym samym otwartych na cyberataki i podatnych na sabotaż przy wykorzystaniu bezzałogowych platform mobilnych (powietrznych, lądowych i wodnych). Dzisiaj ten strategiczny przeciwnik jest o krok do przodu, nie możemy pozwolić, aby ten dystans się zwiększył.

Opisane powyżej zagadnienia są prywatnymi poglądami autora.

Zagrożenia wynikające ze współzależności na przykładzie pożaru serwerowni w Strasburgu

Witold Skomra
Rządowe Centrum Bezpieczeństwa

W nocy z 9 na 10 marca w serwerowni OVHcloud w Strasburgu we Francji wybuchł pożar. W jego wyniku wiele firm światowych utraciło część swoich danych lub miało problemy z dostępnością do swoich serwisów. Dotyczyło to również firm polskich. Sama informacja jest interesująca z dwóch powodów. Po pierwsze świadczy o błędach w zarządzaniu bezpieczeństwem w firmie dotkniętej pożarem. Zniszczeniu lub uszkodzeniu uległy zarówno serwery podstawowe jak i zapasowe. Co prawda były one umieszczone w dwóch różnych blokach, ale zlokalizowanych obok siebie. W efekcie, pożar w jednym obiekcie miał destrukcyjny wpływ na infrastrukturę w obiekcie sąsiadującym. Drugi powód, dla którego informacja jest interesująca to fakt, że nadal wiele osób dziwi się, że zdarzenie w jednym miejscu może mieć wpływ na firmy (a właściwie na ich procesy) realizowane nieomal w każdym możliwym zakątku świata.

Tego typu zdarzenia nazywamy zagrożeniami wynikającymi ze współzależności i nie trzeba sięgać do Francji, by wskazać skutki takich współzależności. W wyniku powodzi w Jenie (RFN), 11 czerwca 2013 r. przestały funkcjonować systemy rowerów miejskich w Warszawie, Wrocławiu, Poznaniu i Opolu. Przyczyną było zalanie serwerów, które utrzymywały aplikację rozliczającą klientów tych systemów. Pożar mostu Łazienkowskiego 14 lutego 2015 r. wywołał zakłócenia w funkcjonowaniu usług internetowych i telekomunikacyjnych. Przyczyną zakłócenia było uszkodzenie traktów światłowodowych umieszczonych pod mostem. Pożar hurtowni warzyw 31 stycznia 2019 r., w wyniku którego doszło do uszkodzenia infrastruktury sieci T-mobile i ograniczenia skali świadczonych usług (w tym ostatnim przypadku należałoby dodać, że dzięki właściwie prowadzonemu systemowi utrzymania ciągłości działania, w wyniku pożaru doszło jedynie do ograniczenia skali świadczonych usług, a nie do ich przerwania).

[8] Za: Raport PTBN *Zagrożenia o charakterze terrorystycznym a system antyterrorystyczny w RP*, wersja *on-line* 1.0., 13 marca 2021 r., s. 43-44

[9] Za: Łukasiewicz J., *Ochrona infrastruktury krytycznej przed bezzałogowymi statkami powietrznymi*, Ochrona i bezpieczeństwo obiektów i biznesu, nr 6/2020, s. 26-27.

Wszystkie te przypadki są tylko dowodem na poprawność twierdzenia, że wszystkie współczesne organizacje działają w warunkach współzależności, a zasięg tych współzależności zaczyna obejmować cały świat. Formalnie współzależności możemy podzielić na następujące kategorie:[1]

- współzależność fizyczna – fizyczne połączenie wyjścia i wejścia, przykładowo usługa lub produkt dostarczane przez jedną infrastrukturę są niezbędne, by inna infrastruktura mogła funkcjonować;
- współzależność cyfrowa – działalność infrastruktury jest uzależniona od informacji przesyłanych systemami transmisji danych;
- współzależność geograficzna – kilka obiektów lub rodzajów infrastruktury znajduje się w swoim bezpośrednim sąsiedztwie (w efekcie zagrożenie w jednym obiekcie może oddziaływać na pozostałe);
- współzależność logiczna – dwa lub więcej rodzajów infrastruktury wzajemnie na siebie oddziałuje bez żadnego powiązania fizycznego, cyfrowego czy geograficznego.

Z przytoczonych zdarzeń można by wyciągnąć wniosek, że współzależności są jedynie zagrożeniem, które należy wyeliminować. Nic bardziej mylnego. Istnienie współzależności pomiędzy systemami jest w zasadzie elementem pożądanym i niezbędnym dla dalszego rozwoju współczesnych społeczeństw. W efekcie takich powiązań powstają systemy złożone[2] (Systems of Systems – SoS). Standard „*Systems and Software Engineering – System Life Cycle Processes* ISO/IEC/IEEE"[3] definiuje to pojęcie następująco. SoS jest zbiorem systemów realizujących zadanie, jakiego żaden z tych systemów nie byłby w stanie realizować samodzielnie. Jednocześnie, każdy z systemów zachowuje własną strukturę zarządzania, cele i zasoby w ramach skoordynowanych działań, mających na celu osiągnięcie wspólnego efektu[4]. Niektóre z systemów złożonych bazują na infrastrukturze globalnej, której ewentualna dysfunkcja będzie powodować skutki ogólnoświatowe. Przykłady takiej infrastruktury „bazowej" to:

- sieć szkieletowa internetu zapewniająca ogólnoświatową wymianę danych pomiędzy węzłami regionalnymi;
- sieć SWIFTnet, zarządzana przez Stowarzyszenie na rzecz Światowej Międzybankowej Telekomunikacji Finansowej (Society for Worldwide Interbank Financial Telecommunication – SWIFT), łącząca poszczególne banki, giełdy, domy maklerskie i inne instytucje finansowe;
- systemy pozycjonowania (GPS, GLONASS, Galileo), na bazie których funkcjonują zarówno samochody autonomiczne czy drony, jak i całe systemy, jak np. system kierowania ruchem morskim i lotniczym.

W efekcie nawet jeśli posiadacze systemów opartych na systemie bazowym mają świadomość jego możliwej dysfunkcji, to nie są w stanie określić ryzyka z tym związanego ani zarządzać tym ryzykiem. Pojawia się więc pytanie – jak zarządzać bezpieczeństwem w systemach złożonych? Klasycznie, organizacje zabezpieczają się przed negatywnym wpływem awarii poprzez zawieranie umów SLA (Service Level Agreement – umowa o gwarantowanym poziomie świadczenia usług) oraz poprzez weryfikację dostawców. Wiarygodny dostawca musi posiadać stosowne certyfikaty i raporty z audytów. Często przeprowadza się inspekcję bezpośrednio u dostawców, by potwierdzić prawdziwość deklarowanej ciągłości świadczenia usług czy dostaw. Jednak ten sposób kontroli ryzyka coraz częściej jest niewystarczający. W obszarze usług cyfrowych łańcuch dostawców ma złożoność fraktala – dostawcy i usługodawcy też mają swoich dostawców i usługodawców, a ci kolejnych. Z praktycznego punktu widzenia, łańcuch dostaw przemysłu telekomunikacyjnego jest nieskończenie złożony i stale się rozwija[5]. W efekcie nikt nie ma zdolności to wiarygodnego sprawdzenia czy kontrahent utrzyma deklarowany poziom świadczenia usługi czy nie. Pół biedy, jeśli awaria dotyczy relacji biznesowych. Tu ewentualne straty można ubezpieczyć. Gorzej, jeśli dojdzie do zakłócenia usług kluczowych dla bezpiecznego funkcjonowania społeczeństwa. Z tego powodu coraz częściej regulacją poziomu bezpieczeństwa u operatorów usług kluczowych zajmuje się państwo. Pierwszymi

[1] Rinaldi S.M., Peerenboom J.P., Kelly T.K. *Identifying, understanding, and analyzing critical infrastructure interdependencies*. IEEE Control Systems Magazine 2001;11-25

[2] Takie tłumaczenie pojęcia „Systems of Systems" nie jest jeszcze ugruntowane w literaturze krajowej.

[3] *Systems and Software Engineering – System Life Cycle Processes*. Geneva, Switzerland: International Organisation for Standardisation / International Electrotechnical Commissions / Institute of Electrical and Electronics Engineers, ISO/IEC/IEEE 15288:2015.

[4] Metodologia definiowania, wyodrębniania, modelowania i analizowania problemów związanych z funkcjonowaniem systemów złożonych uzyskało nazwę inżynierii systemów złożonych (*System of systems engineering* SoSE). Zob. szerzej Międzynarodowa Rada ds. Inżynierii Systemów Spraw https://www.incose.org/ [dostęp 1.12.2018].

[5] https://www.kozminski.edu.pl/pl/review/bezpieczenstwo-lancucha-dostaw

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

symptomami tego trendu była dyrektywa RODO[6] oraz NIS[7]. Obecnie, na forum Komisji Europejskiej trwają prace nad dwoma dokumentami, które mają być ze sobą komplementarne. Jest to znowelizowana dyrektywa NIS (tzw. NIS2) oraz zupełnie nowa dyrektywa, dotycząca odporności podmiotów krytycznych (tzw. Dyrektywa CER)[8]. Generalnie, każdy operator mający wpływ na realizację usługi o kluczowym znaczeniu dla państwa i jego obywateli będzie zobowiązany do wdrożenia minimalnych standardów bezpieczeństwa, przeprowadzania analizy ryzyka i wszystkich innych elementów składających się na proces zarządzania ryzykiem i utrzymania ciągłości działania. Rygorowi temu mają być poddane wszystkie podmioty z danego obszaru, a nie tylko te, którym udało się udowodnić powiązanie z operatorem usługi kluczowej. Wskazywanie podmiotów krytycznych nie będzie ograniczone granicami państw. Każdy kraj UE będzie mógł wskazać podmiot zlokalizowany w innym państwie, jeśli tylko uzna, że jego działalność jest związana z utrzymaniem usługi kluczowej. Jeśli 1/3 państw uzna podmiot za krytyczny, automatycznie stanie się podmiotem krytycznym dla całej UE.

I tu możemy powrócić do pożaru omawianego na wstępie. W artykułach omawiających ten przypadek po raz kolejny wskazywano, że przecież wystarczyło przestrzegać zasad bezpieczeństwa zasobowego, by pomimo pożaru do utraty danych nie doszło. Jedną z tych zasad jest reguła podwójnego, a niekiedy potrójnego zabezpieczenia. Wśród informatyków jest ona znana pod nazwą 3,2,1 (minimum trzy kopie, minimum na dwóch urządzeniach, z czego minimum jedno jest zlokalizowane poza siedzibą macierzystej organizacji). Jak zwykle wszyscy są mądrzy po szkodzie. Jednocześnie presja zawierania umów po jak najniższej cenie powoduje, że nie zawierają one zazwyczaj klauzul odpowiedzialności za skutki utraty danych. To z kolei osłabia wolę usługodawcy inwestowania w bezpieczeństwo na odpowiednio wysokim poziomie. W efekcie opłaca się nie inwestować w bezpieczeństwo. Wygląda na to, że po wejściu w życie dyrektywy CER niezależnie od zawieranych umów pomiędzy kontrahentami, jeśli tylko podmiot będzie związany z utrzymaniem usługi kluczowej, to z mocy prawa będzie zobowiązany do utrzymywania właściwego poziomu bezpieczeństwa. Bez znaczenia będzie fakt, że firma zlokalizowana jest we Francji, a świadczy usługi w Polsce. Jeśli jednak ten poziom bezpieczeństwa nie będzie właściwy, to podmiot krytyczny musi się liczyć z konsekwencjami finansowymi, gdyż w projektowanej dyrektywie znalazł się rozdział zatytułowany „sankcje".

Źródła:

1. *https://tvn24.pl/biznes/ze-swiata/ovh-pozar-serwerowni-w-strasburgu-nie-dziala-wiele-stron-internetowych-w-polsce-5040011*
2. *https://www.computerworld.pl/news/Pozar-w-serwerowni-OVH,426085.html*
3. *https://wiadomosci.wp.pl/strasburg-pozar-w-serwerowni-ovh-utrudnienia-w-internecie-6616562457221696a*
4. *https://www.money.pl/gospodarka/pozar-serwerowni-ovh-sparalizowal-internet-znamy-zasieg-szkod-6617217694849632a.html*

[6] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

[7] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii

[8] https://ec.europa.eu/home-affairs/sites/homeaffairs/files/pdf/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf

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

Morskie farmy wiatrowe jako potencjalne cele ataku z użyciem bezzałogowych statków powietrznych

Jędrzej Łukasiewicz

Adiunkt w Zakładzie Lotnictwa na Wydziale Inżynierii Lądowej i Transportu Politechniki Poznańskiej

Wobec wymagań stawianych przed producentami energii elektrycznej przez normy zanieczyszczenia powietrza atmosferycznego i wobec rosnącego popytu na energię elektryczną, rządzący państwami coraz częściej spoglądają na czyste źródła energii. Do takich czystych źródeł należy energetyka wiatrowa. Morska energetyka wiatrowa jest jednym z najszybciej rozwijających się sektorów produkcji energii. W Polsce za budowę farm wiatrowych odpowiada firma PGE Polska Grupa Energetyczna SA. ze wsparciem merytorycznym PGE Baltica. Obecnie, ze względu na odpowiednie warunki wiatrowe, planuje się budowę farm w polskiej strefie ekonomicznej na Bałtyku.

Jak podaje PGE Baltica na swoich stronach internetowych, planowane inwestycje dostarczą użytkownikom w Polsce energię elektryczną o mocy 1 045 MW do 2026 roku oraz do 1 498 MW do 2030 roku. Farma wiatrowa, jako źródło energii, może zostać zgodnie z ustawą wpisana na listę obiektów infrastruktury krytycznej. Obiekt taki jako obiekt o kluczowym znaczeniu dla gospodarki musi być chroniony we właściwy sposób, który będzie wynikał z analizy ryzyka.

Analizę ryzyka dla obiektów morskich farm wiatrowych należy przeprowadzić zgodnie ze znanym schematem, a wartość ryzyka można obliczyć korzystając z równania:

$$R = P_A \times P_S \times C$$

gdzie:

R – to wartość ryzyka, akceptowalna/tolerowana/nieakceptowalna,

P_A – jest prawdopodobieństwem ataku na obiekt,

P_S – jest prawdopodobieństwem, że atak zakończy się sukcesem,

C – jest konsekwencją ataku.

Zakładając, że 100%-owemu prawdopodobieństwu ataku przypiszemy wartość liczbową 1, a pewności, że atak nie nastąpi przypiszemy wartość 0 – to prawdopodobieństwo ataku będzie równe liczbie z przedziału 0-1. Zakładając także, że 100%-owemu prawdopodobieństwu, że atak zakończy się sukcesem przypiszemy wartość liczbową 1, a pewności, że atak zakończy się niepowodzeniem przypiszemy wartość liczbową 0. Prawdopodobieństwo, że atak zakończy się sukcesem atakującego będzie zatem równe liczbie z przedziału 0-1. Konsekwencjom ataku także można przypisać wartość liczbową z przedziału 0-1, przy czym wartość 0 będzie przypisana do konsekwencji minimalnych, a wartość 1 do konsekwencji maksymalnych. Po wymnożeniu wszystkich wyżej wymienionych wartości otrzymujemy wartość ryzyka R. W zależności od założeń, wartość ta wskaże czy ryzyko jest akceptowalne, tolerowane lub czy ryzyko jest nieakceptowalne i należy podjąć działania zmierzające do obniżenia jego wartości.

Określenie wartości prawdopodobieństwa ataku z użyciem bezzałogowego statku powietrznego jest zadaniem trudnym i powinno należeć do służb mających dostęp do informacji o aktywności terrorystycznej, mogącej zagrozić morskiej farmie wiatrowej. Możliwości kompetencyjnych umożliwiających przelot i dokonanie ataku osób prowadzących działalność terrorystyczną w artykule nie można ocenić z powodu braku danych, ale można przeanalizować techniczną możliwość przelotu bezzałogowego statku powietrznego z miejsca startu do celu, czyli do turbiny wiatrowej. Możliwości te będą oczywiście zależały od modelu bezzałogowego statku powietrznego, ale na potrzeby artykułu wybrano model DJI Phantom 4. Jest to multirotor, jeden z najczęściej kupowanych w Polsce i na świecie modeli bezzałogowców. Model ten charakteryzuje się maksymalną prędkością postępową, mierzoną względem powietrza, wynoszącą 72 km/h i masą wraz z pakietem litowo-polimerowym 1 370 g. Jest to zatem model lekki, podatny na podmuchy wiatru. Statek ten może unosić się w powietrzu w idealnych warunkach pogodowych, takich jak odpowiednia temperatura i brak wiatru, od około 20 minut do około 30 min. Dołożenie dodatkowego pakietu zasilającego nie zwiększa proporcjonalnie czasu lotu, ponieważ wraz ze zwiększeniem ilości energii zwiększa się, co oczywiste, masa statku powietrznego. Czas lotu skraca się w przypadku wykonywania misji przy temperaturach poniżej 15 stopni Celsjusza. Zużycie

energii rośnie także radykalnie w przypadku lotu statku powietrznego pod wiatr lub w czasie lotu z wiatrem bocznym, co prowadzi do skrócenia możliwego czasu, w którym statek powietrzny utrzyma się w powietrzu. Warunki wiatrowe na Bałtyku południowym, zgodnie z danymi podanymi przez PGE Baltica, są dobre, a średnia prędkość wiatru jest wyraźnie wyższa niż 32 km/h. Oznacza to, że w przypadku wiatru przeciwnego do kierunku lotu bezzałogowca oraz przy założeniu, że leci on z prędkością maksymalną 72 km/h, to w czasie 30 minut przebędzie drogę o długości około 15 km od miejsca startu. Jeżeli zatem morska farma wiatrowa zostanie zbudowana w odległości większej niż 15 km od miejsca startu bezzałogowego statku powietrznego, to z technicznego punktu widzenia nie będzie możliwości, by typowy multirotor do takiej farmy doleciał. Być może, specjalnie skonstruowany, nietypowy multirotor, o dłuższym czasie lotu taką misję mógłby wykonać. Kolejną przeszkodą utrudniającą wykorzystanie bezzałogowego statku powietrznego jest problem zasięgu aparatury służącej do komunikacji pomiędzy pilotem a bezzałogwcem. Zasięg ten w warunkach idealnych, bez przeszkód terenowych, bez interferujących zakłóceń wynosi około 3.5 km. Po utracie łączności, statek powietrzny albo wykona procedurę FailSafe, zgodnie z którą może np. powrócić do miejsca startu albo polecieć dalej do celu jeśli pilot przed startem zaprogramował trasę. Pilot nie będzie miał jednak możliwości, by przy pomocy kamery precyzyjnie zbliżyć się do celu lotu. Powyższe rozważania wskazują, że sposób atakowania morskiej farmy wiatrowej za pomocą bezzałogowego statku powietrznego jest raczej mało prawdopodobny.

Określenie podatności turbiny wiatrowej na atak jest zagadnieniem z mechaniki i wytrzymałości materiałów. Zakładając, że bezzałogowiec o masie 1 370 g będzie poruszał się z prędkością 72 km/h, to energia uderzenia zgodnie ze wzorem:

$$E_K = ½ mV^2$$

wyniesie 274 J. Zatem bezzałogowiec uderzy z energią o połowę mniejszą niż energia uderzenia pocisku z broni krótkiej, która wynosi około 500 J. Biorąc pod uwagę brak możliwości ręcznej kontroli położenia drona z dużej odległości, wysokość turbin wiatrowych, która może wynosić do 250 m od poziomu morza, długość łopat wirnika dochodząca do 110 metrów oraz fakt, że wirnik turbiny obraca się pod wpływem wiatru, można założyć, że prawdopodobieństwo trafienia dronem w element turbiny jest bardzo niskie. Trudność utrzymania bezzałogowca przy łopacie rotującego wirnika powoduje, że kontrola stanu technicznego turbin wiatrowych odbywa się przy nieobracającym się wirniku.

Konsekwencje skutecznego ataku można rozpatrywać z punktu widzenia strat finansowych dla operatora farmy. Uszkodzoną turbinę wiatrową trzeba naprawić lub wymienić. Koszt takiej operacji będzie zależny od skali zniszczeń. Wartość ryzyka obliczona dla małego prawdopodobieństwa ataku i małego prawdopodobieństwa sukcesu ataku będzie zatem niska, a więc tolerowana lub akceptowalna.

Powyższe rozważania jasno pokazują, że typowe bezzałogowce kupione w sklepie nie stanowią zagrożenia dla farm wiatrowych. Niestety, łatwy dostęp do elementów służących do budowy takiego bezzałogowego statku powietrznego pozwala przypuszczać, że użycie nietypowej konstrukcji, o większej masie, o większym udźwigu, o lepszych właściwościach lotnych, pozwalającego na przeniesienie ładunku wybuchowego w rejon turbiny wiatrowej może skutkować przeprowadzeniem ataku, którego skuteczność będzie bardzo wysoka. Konsekwencje takiego ataku będą wysokie i zależne od wielkości ładunku wybuchowego przenoszonego przez statek powietrzny.

BEZZAŁOGOWE STATKI POWIETRZNE JAKO POTENCJALNE ZAGROŻENIE DLA MORSKICH FARM WIATROWYCH

Bezzałogowe statki powietrzne wykonują loty na podstawie poleceń wydawanych drogą radiową przez pilota lub na podstawie algorytmu działania zaprogramowanego przez pilota przed startem. Do bezzałogowych statków powietrznych zaliczamy statki typu: multirotor (MR), samolot (A), śmigłowiec (H) oraz aerostat (AS). Ze względu na łatwość pilotażu, najczęściej spotykanym typem bezzałogowego statku powietrznego jest multirotor. Drugim pod względem łatwości pilotażu, najczęściej spotykanym statkiem powietrznym, jest samolot. Konstrukcje obu tych typów statków mają swoje zalety i wady. Do zalet multirotorów niewątpliwie można zaliczyć możliwość nieruchomego zawisu w przestrzeni powietrznej, w miejscu wybranym przez pilota. Zaletą multirotorów są także: niewielki rozmiar, łatwość ich transportu oraz niewielkie wymagania dotyczące miejsca startu i lądowania. Do wad statków powietrznych typu multirotor zaliczamy stosunkowo niewielki zasięg przelotu, wynikający z ograniczeń pojemności pakietu litowo-polimerowego stanowiącego źródło energii elektrycznej służącej

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

do zasilania urządzeń pokładowych i silników oraz niewielką prędkość przelotu.

Drugim najczęściej spotykanym typem bezzałogowego statku powietrznego jest samolot. Zaletą samolotu jest możliwość wykonania lotu na długim dystansie, z dużą prędkością i utrzymywanie się w powietrzu w długim okresie czasu. Wadą tego typu konstrukcji jest brak możliwości nieruchomego zawisu w jednym punkcie przestrzeni powietrznej. Ostatnio pojawiły się hybrydy multirotorów i samolotów, pozwalające na pionowy start samolotu, ale należy pamiętać, że konstrukcje takie nie są powszechnie spotykane. Bezzałogowe śmigłowce oraz aerostaty są konstukcjami stosunkowo rzadko spotykanymi.

Bezzałogowe statki powietrzne wykorzystywane są coraz częściej w różnych obszarach działalności człowieka. O ich wykorzystaniu decydują takie czynniki jak: niska cena bezzałogowego statku powietrznego w porównaniu z załogowym statkiem powietrznym, uniwersalność platformy latającej pozwalająca na umieszczenie na niej dowolnego, wymaganego w danej chwili ładunku, w tym urządzenia technicznego, krótki czas nauki pilotażu lub zastosowanie komputera pokładowego, który samodzielnie ustabilizuje bezzałogową platformę w locie i wykona zaprogramowaną wcześniej misję.

Doniesienia prasowe wskazują, że bezzałogowe statki powietrzne mogą być źródłem zagrożeń dla człowieka lub dla instalacji mających kluczowe znaczenie dla funkcjonowania społeczeństwa i gospodarki. Jako przykład ataku zrealizowanego za pomocą bezzałogowego statku powietrznego można wskazać atak, przeprowadzony 4 sierpnia 2018 roku w stolicy Wenezueli – Caracas, na prezydenta tego kraju Nicolása Maduro. Zamach polegał na detonacji granatów przymocowanych do lecących w pobliżu polityka dronów. Politykowi nic się nie stało, ale w wyniku detonacji granatów rannych zostało kilku żołnierzy z ochrony. Zamach wywołał także wybuch paniki w zgromadzonym tłumie. Także ataki z 23 stycznia 2021 roku na Al Yamamah Palace w Rijadzie, będący oficjalną siedzibą króla Arabi Saudyjskiej zostały przeprowadzone z użyciem bezzałogowych statków powietrznych, przenoszących ładunki wybuchowe. Ataki te wywołały napięcia polityczne w regionie.

Przykładem ataku, zrealizowanego za pomocą bezzałogowego statku powietrznego na instalacje lub obiekty mające kluczowe znaczenie dla funkcjonowania gospodarki, był atak z 14 sierpnia 2019 roku na saudyjskie instalacje naftowe Abqaiq. Atak został zrealizowany za pomocą, prawdopodobnie, 18 platform bezzałogowych. W wyniku uszkodzenia instalacji spadła produkcja ropy. Jako inny przykład ataku na obiekty można wskazać atak przeprowadzony w dniach 19-21 grudnia 2018 roku na lotnisko Gatwick w Wielkiej Brytanii. Atak polegał na przelotach bezzałogowca w pobliżu lotniska i spowodował paraliż lotniska. Straty finansowe, wynikające z konieczności zwrotu opłat za bilety oraz zapewnienia opieki pasażerom, zostały ocenione na około 50 milionów funtów brytyjskich.

SEKWENCJA ZDARZEŃ W CZASIE ATAKU Z UŻYCIEM BEZZAŁOGOWEGO STATKU POWIETRZNEGO

Sekwencję zdarzeń ataku na dowolny obiekt infrastruktury krytycznej z użyciem bezzałogowej platformy można przedstawić w postaci schematu:

Zagrożeniem jest w tym przypadku możliwość działania pilota przy użyciu bezzałogowego statku powietrznego, mającego na celu przeprowadzenie ataku na człowieka lub obiekt.

Działania prewencyjne to wszelkie działania, w tym prawne, mające na celu zniechęcenia atakującego do rozpoczęcia ataku. Do działań prewencyjnych należą z pewnością działania mające na celu ustanowienie, zgodnie z obowiązującymi przepisami prawa lotniczego, tzw. stref geograficznych, w których będzie obowiązywał zakaz wykonywania lotów bezzałogowymi statkami powietrznymi innymi niż należącymi do operatora obiektu infrastruktury krytycznej. Do działań prewencyjnych można także

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

zaliczyć podnoszenie świadomości lokalnej społeczności o ograniczeniach i zakazach wykonywania lotów bezzałogowcami oraz podnoszenie stopnia znajomości prawa lotniczego lokalnych jednostek policji.

Aktywizacja zagrożenia to uruchomienie bezzałogowca i rozpoczęcie ataku.

Atak to zdarzenie niepożądane, które może spowodować stratę.

Obrona to wszelkie działania mające na celu przeszkodzenie atakującemu w kontynuacji jego działań. Do obrony przed atakiem realizowanym za pomocą platform bezzałogowych służą systemy złożone z urządzeń wykrywających i urządzeń niszczących lub zakłócających lot. Urządzenia wykrywające to najczęściej radary, zestawy mikrofonów rejestrujących hałas emitowany przez bezzałogowca, kamery działające w paśmie widzialnym i/lub podczerwieni promieniowania elektromagnetycznego, służące do obserwacji przestrzeni powietrznej nad obiektem i umożliwiające identyfikację za pomocą algorytmów AI lecącego obiektu innego niż ptak. Lecącego bezzałogowca można także wykryć przez analizę sygnału komunikacji pomiędzy urządzeniem sterującym, będącym w ręku pilota a statkiem powietrznym. Niestety, każde z tych urządzeń można oszukać, a osoba mająca elementarne pojęcie o zasadach działania statków powietrznych i o fizyce nie będzie miała z tym żadnego problemu. Każda z wyżej opisanych metod detekcji ma także swoje ograniczenia, na przykład wynikające z położenia chronionego obiektu. Dla przykładu – zakładając, że obiekt infrastruktury leży w obszarze dużego miasta, w sąsiedztwie innych zabudowań, w rejonie ulic o dużym natężeniu ruchu, można zadać pytania: na jakiej minimalnej wysokości system radarowy wykryje drona? Bezzałogowy statek powietrzny może lecieć na wysokości około 0,5 metra nad powierzchnią ulicy, wykorzystując lidarowy miernik wysokości. Jaki hałas, którego źródłem będą rotujące silniki bezzałogowca wykryje mikrofon, jeśli w rejonie, w którym leci bezzałogowiec znajdują się inne źródła hałasu o dużo wyższym natężeniu i charakterystyce częstotliwościowej zbliżonej do charakterystyki drona? Takimi źródłami mogą być samochody i tramwaje. Jak wykryje drona kamera, jeśli bezzałogowiec ten zostanie tak skonstruowany, by swoim kształtem oraz umalowaniem przypominał lecącego ptaka, a jego elementy zostaną zaizolowane cieplnie? Należy także zapytać jaki sygnał komunikacji zarejestruje skaner, jeśli trasa bezzałogowca zostanie przez pilota zaprogramowana przed startem i bezzałogowiec wykona swoją misję całkowicie autonomicznie? W trybie lotu autonomicznego, bezzałogowiec może nie emitować sygnału komunikacji, a działać wyłącznie jako pasywny odbiornik sygnałów np. GPS. Systemy detekcji dronów obecnie oferowane na rynku są zatem systemami, których użycie obarczone jest ograniczeniami i działającymi skutecznie w przypadku bezzałogowców standardowych, tych łatwo dostępnych na półkach sklepowych. Dużym wyzwaniem technologicznym oraz prawnym jest także sposób neutralizacji wykrytego bezzałogowca, stanowiącego zagrożenie. Do najczęściej stosowanych metod należą metody oparte na fizycznym przechwyceniu drona, np. przez złapanie go w siatkę plątającą śmigła, zakłócenie sygnału komunikacji pilot – bezzałogowiec, fizycznym uszkodzeniu przy wykorzystaniu promieniowania laserowego o dużej mocy, zakłóceniu sygnału pozycjonowania GPS. Metody te będą skuteczne tylko w przypadku pojedynczego drona, w przypadku gdy przechwycenie odbywa się na terenie, w którym nie ma ludzi i upadek drona na ziemię nie stanowi zagrożenia i nie spowoduje dużych strat materialnych. Potencjalne konsekwencje w postaci obrażeń doznanych przez człowieka lub zniszczeń chronionego obiektu przez upadającą platformę bezzałogową mogłyby być duże.

Za konsekwencje skutecznego ataku można uznać znaczące straty finansowe, straty ekologiczne w przypadku spowodowania kontaminacji terenu, straty polityczne polegające np. na utracie zaufania do personelu ochrony, służb, władz państwa i straty społeczne w przypadku śmierci człowieka.

WNIOSKI

1. Przed nieautoryzowanym zbliżeniem się bezzałogowego statku powietrznego, pilotowanego przez nieświadomego operatora należy się zabezpieczyć poprzez ustanowienie strefy zakazu lotów dla bezzałogowych statków powietrznych w rejonie farmy. Takie strefy wyznacza, na żądanie operatora chronionej instalacji, Polska Agencja Żeglugi Powietrznej,

2. Należy ustanowić strefy z zakazem lotów bezzałogowych statków powietrznych wzdłuż linii brzegowej morza Bałtyckiego na odcinku bezpośrednio przylegającym do miejsca budowy farmy. Wraz z tymi działaniami należy podnieść świadomość prawną w zakresie prawa lotniczego funkcjonariuszy policji odpowiedzialnych za patrolowanie rejonu zakazu lotów.

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

3. Otwarta przestrzeń pomiędzy linią brzegową a farmą wiatrową umożliwia stosowanie systemów radarowych, służących do wykrycia nieautoryzowanych przelotów bezzałogowych statków powietrznych, a zastosowanie urządzeń zakłócających lot lub niszczących drona nie będzie stanowiło zagrożenia dla ludzi i ewentualnie chronionej instalacji.

4. Powyższe rozważania dotyczą sytuacji, w której potencjalny atak wyprowadzony zostanie od strony lądu. Atak prowadzony przy użyciu drona startującego z jednostki pływającej, która może zbliżyć się do rejonu budowy farmy, może okazać się dużo bardziej skuteczny i tym samym spowodować wyższe straty.

5. Nienajlepszy stan polskiej Marynarki Wojennej powinien być powodem rozpoczęcia prac nad bezzałogowymi okrętami patrolowymi, o niewielkiej wyporności, ale zaopatrzonymi w systemy radarowe i systemy zwalczania dronów. Okręty takie mogłyby bronić instalacji od strony morza.

6. Budowa morskich farm wiatrowych powinna być impulsem do budowy systemu nasłuchowego, złożonego z systemu mikrofonów, chroniącego farmę przed zagrożeniami, których źródłem mogą być podwodne drony.

Transformacja energetyczna UE z punktu widzenia ochrony infrastruktury krytycznej

Krzysztof Malesa
Rządowe Centrum Bezpieczeństwa

Wodór jest nie tylko paliwem przyszłości, ale też przede wszystkim szansą dla Europy na przyspieszenie procesu dekarbonizacji. Zastąpienie paliw kopalnych czystym (bezemisyjnym) źródłem energii to filar europejskiej strategii klimatycznej, ale też przedsięwzięcie wymagające ogromnych inwestycji, które z pewnością wymusi zmiany w podejściu do wyłaniania i ochrony infrastruktury krytycznej. Na forum UE i w państwach członkowskich trwają intensywne prace legislacyjne w tym obszarze. Rządowe Centrum Bezpieczeństwa dołączyło do prac Międzyresortowego Zespołu ds. Gospodarki Wodorowej. Przedstawiciele Centrum są też krajowymi delegatami w unijnej grupie roboczej przygotowującej dyrektywę CER.

TRANSFORMACJA ENERGETYCZNA W RAMACH ZIELONEGO ŁADU UE

11 grudnia 2019 roku została zaprezentowana nowa strategia rozwoju gospodarczego Unii Europejskiej, tzw. Europejski Zielony Ład. Zawiera ona plan działań umożliwiających efektywne wykorzystywanie zasobów poprzez przestawienie gospodarki na odnawialne źródła energii, powstrzymanie zmian klimatu i radykalne ograniczenie zanieczyszczeń we wszystkich sektorach gospodarki, zwłaszcza w sektorach określanych jako *hard-to-decarbonize*[1]. Zgodnie z ogłoszoną 7 lipca 2020 roku, strategią wodorową UE, jednym z celów do realizacji w tym obszarze w ramach Zielonego Ładu jest **integracja systemów energetycznych i sektora technologii wodorowych.**

Wizja Zielonego Ładu, zakładająca stopniowe osiągnięcie do 2050 roku znaczącego udziału wodoru w europejskim miksie energetycznym, w kolejnych etapach opiera się na rozwiązaniach przejściowych, opartych o różne rodzaje wodoru, umownie oznaczane kolorami. Ich klasyfikacja opiera się na technologii produkcji wodoru, podczas której dochodzi do **wysokiej, niskiej lub zerowej emisji dwutlenku węgla.**

Wodór szary to naturalny produkt uboczny w przemyśle rafineryjnym. Niezależnie od metody produkcji (reforming metanu lub zgazowanie węgla) towarzyszy mu wysoka emisja CO_2. Czyściejszym surowcem jest **wodór niebieski**. Proces jego produkcji jest taki sam jak wodoru szarego, ale dwutlenek węgla jest wychwytywany i składowany lub wykorzystywany w przemyśle. Jest to proces niskoemisyjny.

Najbardziej pożądany z punktu widzenia środowiska i zmian klimatu jest **wodór zielony**. Wytwarza się go z odnawialnych źródeł energii (fotowoltaika, farmy wiatrowe) np. w procesie elektrolizy wody. **Jest to proces całkowicie bezemisyjny**.

Rzadziej stosowane technologie produkcji wodoru to **wodór turkusowy** pozyskiwany w dość skomplikowanym, lecz niskoemisyjnym procesie pyrolizy gazu oraz **wodór fioletowy (purpurowy)**

[1] Sektory, w których szczególnie trudne lub niemożliwe jest odejście od węgla na rzecz energii z OZE, np. hutnictwo, transport, chemia itp.

produkowany w procesie elektrolizy wody prądem z elektrowni atomowych.

Unijna strategia wodorowa zakłada odchodzenie od wodoru szarego, poprzez okres przejściowy zakładający zwiększenie zaangażowania wodoru niebieskiego, aż po ostatnią fazę, w której zielony wodór pozwoli wypełnić cele klimatyczne i w roku 2050 osiągnąć neutralność klimatyczną UE. Będzie to realizowane w ramach dużych, transgranicznych projektów objętych pomocą publiczną w formule IPCEI[2], gwarantującej bezpieczeństwo energetyczne w aspekcie regionalnym.

NOWA DYREKTYWA W SPRAWIE OCHRONY INFRASTRUKTURY KRYTYCZNEJ

W tym samym czasie na forum UE trwają prace nad adaptacją obszaru nieodłącznie towarzyszącego energetyce, tj. ochrony infrastruktury krytycznej. W grudniu 2020 roku Komisja przedstawiła wnioski ustawodawcze dotyczące dyrektywy w sprawie środków na rzecz wspólnego wysokiego poziomu cyberbezpieczeństwa w całej Unii (zmieniona dyrektywa NIS) oraz nowej dyrektywy w sprawie odporności podmiotów krytycznych.

Proponowana dyrektywa CER zastępuje dyrektywę z 2008 roku w sprawie europejskiej infrastruktury krytycznej. Pojęcie CIP (Critical Infrastructure Protection) zastąpiono bardziej elastycznym **CER (Critical Entities Resilience)**. **Nowa dyrektywa wprowadza** dziesięć sektorów, a mianowicie sektory energii, transportu, bankowości, infrastruktury rynku finansowego, zdrowia, wody pitnej, ścieków, infrastruktury cyfrowej, administracji publicznej i przestrzeni kosmicznej.

WODÓR W KRAJOWYM SYSTEMIE OCHRONY IK

W nowej dyrektywie CER, w sektorze Energia, pojawił się nowy podsektor „Wodór", w którym jako „Podmiot" wskazano „Operatorów produkcji, magazynowania i przesyłu wodoru". Z punktu widzenia polskiego systemu prawnego, w którym funkcjonuje ustawa o zarządzaniu kryzysowym i szereg dokumentów niższego rzędu, będzie to oznaczać wiele zmian legislacyjnych i organizacyjnych.

Zależnie od przyjętego przez Rząd modelu rozwoju gospodarki wodorowej – **scentralizowanego**, z krajowym systemem przesyłu i magazynowania lub też **zdecentralizowanego**, z lokalnymi dolinami wodorowymi, w których podaż i popyt są równoważone lokalnie – konieczne będzie zdefiniowanie nowych kryteriów, umożliwiających ujęcie elementów infrastruktury wodorowej na wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej.

Dla właścicieli tych instalacji, przyszłych operatorów infrastruktury krytycznej, będzie to oznaczać nie tylko dodatkowe (nieliczne zresztą) obowiązki, ale też szczególne traktowanie ze strony państwa.

Dyrektywa CER zakłada szersze niż dotychczas spojrzenie na bezpieczeństwo, uwzględniające zapewnienie świadczenia usług koniecznych do utrzymania niezbędnych funkcji społecznych lub działalności gospodarczej oraz zwiększenie odporności podmiotów świadczących takie usługi. Takie podejście, odwołujące się do krajowej oceny ryzyka opracowanej na podstawie Unijnego Mechanizmu Ochrony Ludności, będzie zapewne wymagało dostosowania nie tylko kryteriów, ale też całego mechanizmu wyłaniania infrastruktury krytycznej, opisanego w Narodowym Programie Ochrony IK.
Jest to podejście w pełni zgodne z wnioskami z wdrażania dotychczasowych rozwiązań z zakresu ochrony infrastruktury krytycznej, również w podkreślanym przez Komisję istotnym aspekcie zgodności nowej dyrektywy CER z procedowaną równolegle dyrektywą NIS2.

[2] Important Projects of Common European Interest.

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

Aktualna sytuacja epidemiologiczna COVID-19[1,2]

Beata Michulec
Główny Inspektorat Sanitarny

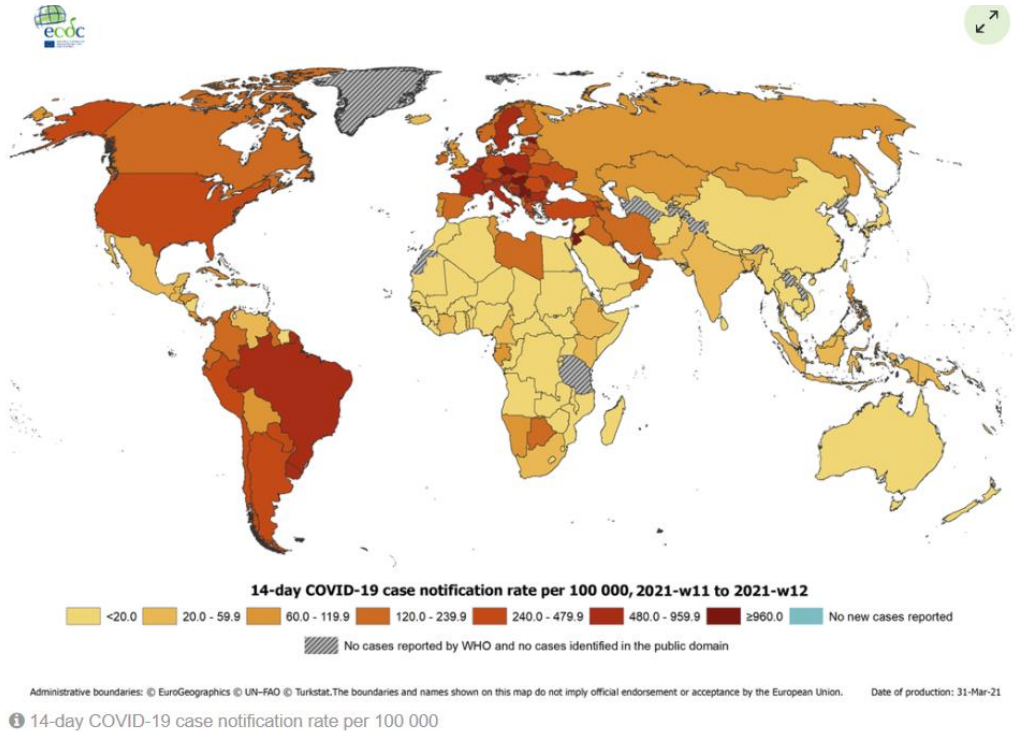
W 12 tygodniu bieżącego roku wartości wskaźników epidemiologicznych pozostawały wysokie, co wskazuje, że transmisja jest nadal powszechna. Wg ECDC istnieje duże prawdopodobieństwo, że w nadchodzących tygodniach nastąpi dalszy wzrost liczby przyjęć do szpitali, oddziałów intensywnej terapii i śmiertelności w tych krajach, w których obecnie obserwuje się rosnącą zapadalność.

Na świecie, w okresie od 31 grudnia 2019 r. do 12 tygodnia 2021 r., odnotowano 127 628 928 przypadków COVID-19 (zgodnie z definicjami przypadków przyjętych w krajach), w tym 2 791 055 zgonów z powodu zakażenia SARS-CoV-2.

Na kontynencie afrykańskim odnotowano 4 186 456 przypadków COVID-19, w tym najwięcej przypadków w Republice Południowej Afryki (1 545 431) i Maroku (494 659). W Azji odnotowano 24 072 463 zakażenia, najwięcej przypadków w Indiach (12 039 644) i Iranie (1 846 923). Na kontynentach amerykańskich odnotowano 56 084 701 przypadków, najwięcej w Stanach Zjednoczonych (30 331 794) i Brazylii (12 573 615). W Oceanii odnotowano 63 734 zakażenia, najwięcej w Australii (29 260) i Polinezji Francuskiej (18 607). Przypadki COVID-19 były rejestrowane na statku wycieczkowym w Japonii (705). W Europie zanotowano 43 220 869, najwięcej we Francji (4 545 589) i Rosji (4 528 543).

W omawianym okresie (od 31 grudnia 2019 r, na tydzień 2021-12) w Afryce odnotowano 111 945 zgonów, najwięcej w Republice Południowej Afryki (52 663) i Egipcie (11 882). W Azji zanotowano 383 005 zgonów, najwięcej w Indiach (161 843) i Iranie (62 308). Na kontynentach amerykańskich najwięcej zgonów stwierdzono w Stanach Zjednoczonych (550 036) i Brazylii (313 866), łącznie 1 348 214. W Oceanii zanotowano 1 263 zgony, w tym w Australii (909) i Polinezji Francuskiej (141). Odnotowano 6 zgonów na statku wycieczkowym w Japonii. W Europie odnotowano 946 622 zgony, najwięcej w Wielkiej Brytanii (126 592) i we Włoszech (107 933).

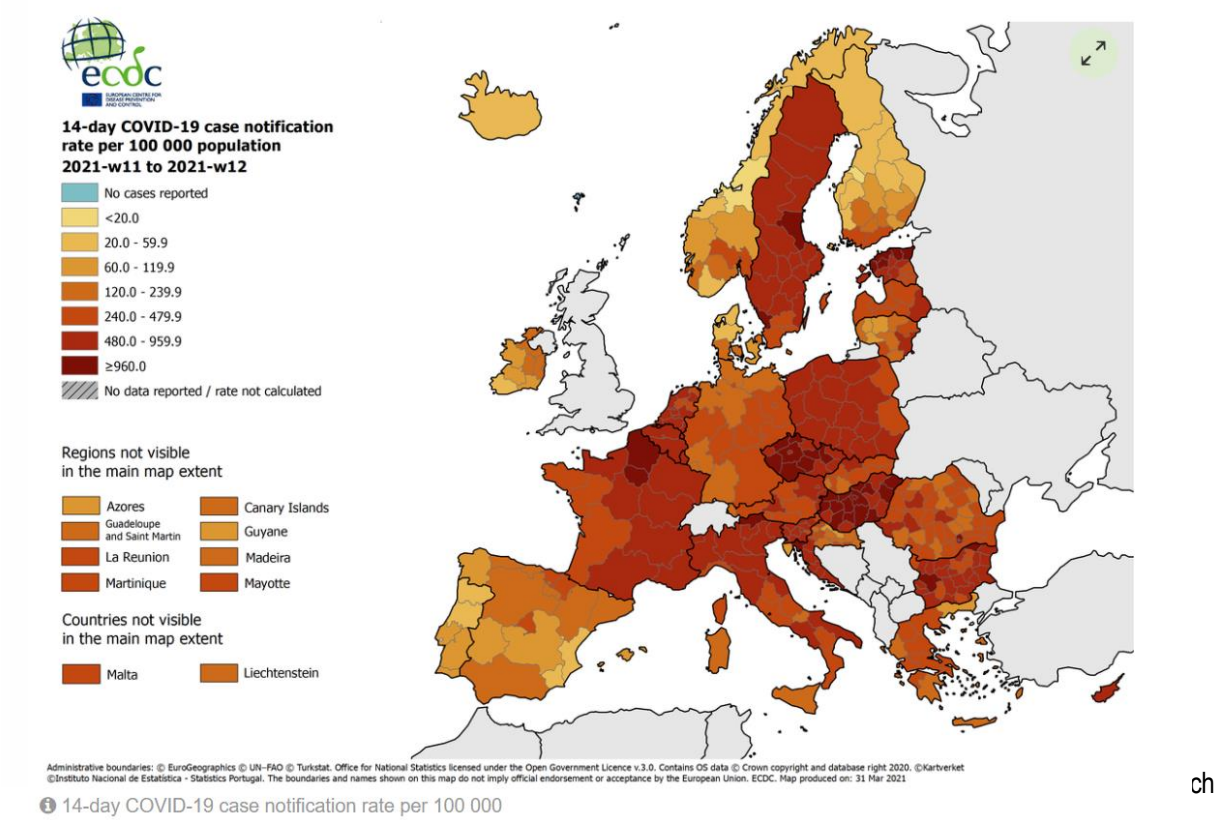
Ryc. 1. 14-dniowa skumulowana zapadalność (na 100 000 mieszkańców) w poszczególnych krajach świata. Stan na 15-28.03.2021 r. (11 i 12 tydzień)



Źródło strona ECDC: https://www.ecdc.europa.eu/en/geographical-distribution-2019-ncov-cases

[1] Na podstawie informacji dostępnych na stronie European Centre for Disease Prevention and Control (ECDC).
[2] https://www.gov.pl/web/koronawirus

Ryc. 2. 14-dniowa zapadalność (na 100 000 mieszkańców) w UE/EOG. Stan na 15-28.03.2021 r. (11 i 12 tydzień).



Źródło: strona ECDC: https://www.ecdc.europa.eu/en/cases-2019-ncov-eueea.

W krajach Unii Europejskiej/Europejskiego Obszaru Gospodarczego (UE/EOG) w omawianym okresie odnotowano 26 393 414 przypadków zakażeń oraz 610 455 zgonów.

W 12 tygodniu 2021 r. (wg ECDC jest to 22-28.03.2021 r.) sytuacja epidemiologiczna zakażeń SARS-CoV-2 w krajach Unii Europejskiej przedstawiała się następująco:

- w 18 krajach Unii Europejskiej (UE / EOG) wzrosła zapadalność na COVID-19 (pozytywny wynik testu w kierunku SARS-CoV-2),
- w 6 krajach odnotowano wzrost zapadalności w starszych grupach wiekowych,
- w 13 krajach odnotowano wzrost liczby przyjęć do szpitali lub na OIT (oddział intensywnej terapii) i/lub obłożenia łóżek z powodu COVID-19,
- 12 krajów zgłosiło wzrost śmiertelności w porównaniu do ubiegłych tygodni.

w 12 tygodniu roku pozostają wysokie, co wskazuje, że transmisja jest nadal powszechna. Wg ECDC, istnieje duże prawdopodobieństwo, że w nadchodzących tygodniach nastąpi dalszy wzrost liczby przyjęć do szpitali, oddziałów intensywnej terapii i śmiertelności w tych krajach, w których obecnie obserwuje się rosnącą zapadalność.

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

Tab.1. Dane dla poszczególnych krajów UE / EOG.

EU/EEA	Cases	Deaths	14-day case notification rate per 100 000 inhabitants	14-day death notification rate per 1 000 000 inhabitants
France	4545589	94623	703.99	61.91
Italy	3532057	107933	517.95	97.05
Spain	3270825	75199	160.07	58.63
Germany	2782273	75913	248.21	30.00
Poland	2267964	51932	923.22	124.51
Czechia	1518772	26137	1069.32	257.90
Netherlands	1257561	16455	553.57	22.29
Romania	940443	23234	402.31	86.35
Belgium	874123	22929	547.48	32.20
Portugal	820716	16843	60.25	14.47
Sweden	793477	13 398	687.13	10.17
Hungary	641124	20161	1196.86	315.06
Austria	533511	9006	481.29	37.86
Slovakia	358115	9542	369.28	171.68
Bulgaria	328753	12710	722.09	204.99
Croatia	267522	5911	402.84	55.69
Greece	254031	7880	306.79	73.61
Ireland	234541	4666	157.12	26.59
Denmark	228892	2415	130.88	3.78
Lithuania	214365	3560	312.12	53.68
Slovenia	212965	4311	590.97	43.42
Estonia	104214	879	1364.06	113.62
Latvia	101040	1878	380.52	58.19
Norway	93145	660	236.70	3.73
Finland	76425	817	164.53	3.08
Luxembourg	60755	738	459.67	78.26
Cyprus	44631	252	560.81	13.51
Malta	28938	388	375.46	66.08
Iceland	6183	29	27.46	0.00
Liechtenstein	2664	56	126.46	0.00
Total	26393414	610455	489.94	72.86

Źródło: strona ECDC: https://www.ecdc.europa.eu/en/cases-2019-ncov-eueea.

OCENA RYZYKA ECDC

Ze względu na zwiększoną zdolność przenoszenia się nowych wariantów wirusa SARS-CoV-2 o istotnym znaczeniu (VOC), dowody na występowanie cięższego przebiegu choroby oraz potencjał częściowej lub mniejszej skuteczności istniejących (licencjonowanych) szczepionek przeciwko tym wariantom COVID-19, w połączeniu z wysokim prawdopodobieństwem, że wzrośnie odsetek zakażeń SARS-CoV-2 spowodowanych wariantem B.1.1.7 (brytyjski), a być może również B.1.351 (południowoafrykański) i P.1 (brazylijski), ryzyko związane z dalszym rozprzestrzenianiem się VOC SARS-CoV-2 w krajach UE/EOG jest obecnie oceniane jako wysokie do bardzo wysokiego dla całej populacji i bardzo wysokie dla osób należących do grup podwyższonego ryzyka.

Analiza modelowa pokazuje, że jeśli wprowadzone restrykcje i działania prewencyjne nie będą kontynuowane lub przestrzegane w większym stopniu, w nadchodzących miesiącach należy spodziewać się znacznego wzrostu liczby przypadków i zgonów związanych z COVID-19 w krajach UE/EOG. Chociaż realizacja szczepień złagodzi efekt zastąpienia przez warianty szybciej rozprzestrzeniające się, a trendy sezonowości mogą potencjalnie zmniejszyć przenoszenie się w miesiącach letnich, przedwczesne łagodzenie restrykcji może doprowadzić do szybkiego wzrostu wskaźników zachorowalności, występowania ciężkich przypadków i wzrostu śmiertelności. Opóźnienia w zakupie, dystrybucji i podawaniu szczepionek, gdyby wystąpiły, również opóźniłyby możliwość łagodzenia wprowadzonych restrykcji. Niezbędne jest szybkie zaszczepienie grup priorytetowych, szczególnie narażonych, aby możliwie szybko zmniejszyć liczbę hospitalizacji, przyjęć na OIOM i zgonów z powodu COVID-19.

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

Ryc. 3. Przypadki potwierdzone w Polce. Stan na 12 tydzień 2021 r.

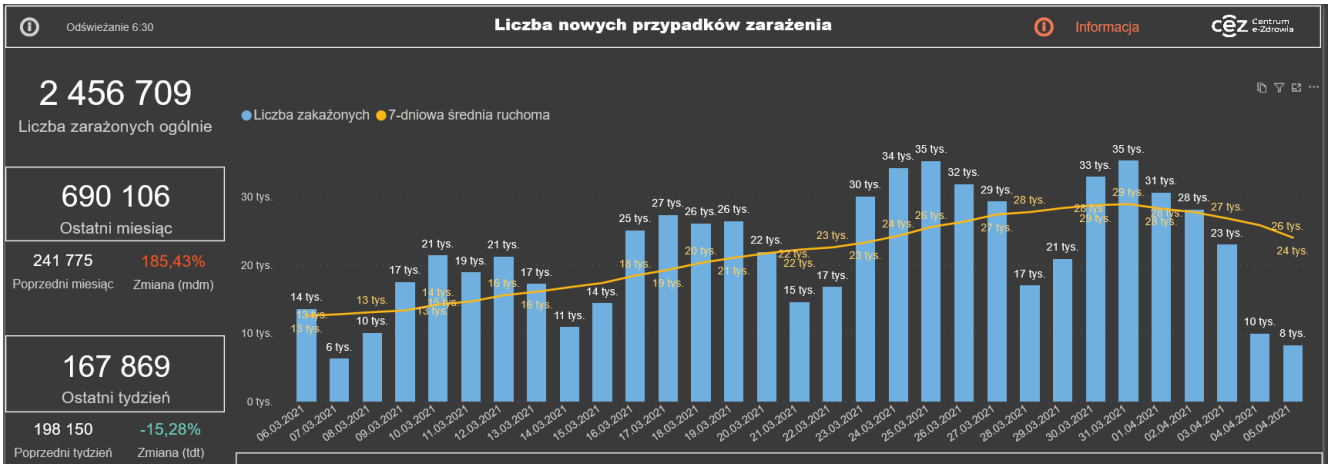
Źródło: NIZP-PZH.

W Polsce, od pierwszego przypadku zakażenia tj. od 04.03.2020 r. do 05.04.2021 r. zanotowano łącznie 2 456 709 zakażeń SARS-CoV-2, w tym 55 065 przypadków śmiertelnych.

W ostatnim miesiącu tj. od 06.03.2021 r. do 05.04.2021 r. odnotowano 690 106 przypadków. W stosunku do analogicznego okresu w poprzednim miesiącu, w którym odnotowano 241 775 przypadków, nastąpił wzrost zakażeń o 185,43%.

W ostatnim tygodniu tj. od 30.03.2021 r. do 05.04.2021 r. odnotowano 167 869 przypadków, tj. o 15,28% mniej w porównaniu do poprzedniego tygodnia, w którym odnotowano –198 150 przypadków zakażeń, potwierdzonych laboratoryjnie.

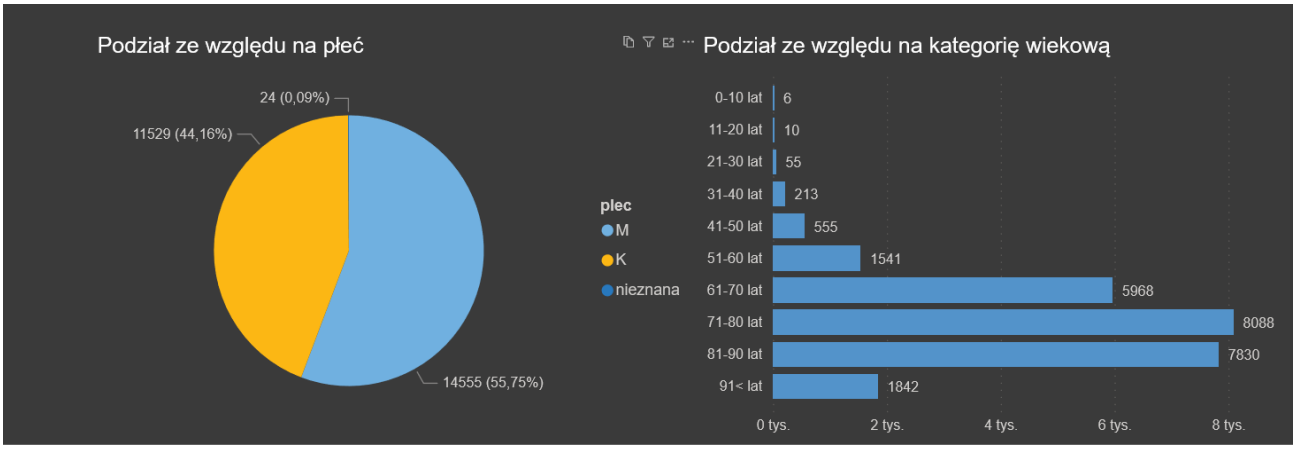
Ryc. 4. Liczba nowo rejestrowanych przypadków zakażeń dziennie w okresie 06.03.-05.04.2021. r.



Źródło: Centrum e-Zdrowia.

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

Ryc. 5. Przykładowy obraz występowania zgonów w Polsce wg płci i kategorii wiekowej



Źródło: Centrum e-Zdrowia.

Liczba zgonów w Polsce waha się od kilkudziesięciu do kilkuset dziennie z tendencją wzrostową od początku marca 2021 r. Wg stanu na 05.04., średnia 7-dniowa liczby zgonów wyniosła 439 przypadków, średnia 7-dniowa wg stanu na 29.03.2021 r. to 367 zgonów, zaś na 22.03.2021 r. – 308 zgonów.
Wg danych Centrum e-Zdrowia, zgony osób zakażonych wirusem SARS-CoV-2 dominują wśród mężczyzn. Dominującą grupą osób, w której dochodzi najczęściej do zgonu w wyniku zakażenia SARS-CoV-2, jest grupa wiekowa 71-80 lat.

W celu ograniczenia szerzenia się wirusa w populacji, obok szczepień i stosowania się do wprowadzanych restrykcji tzw. lock down, należy ściśle przestrzegać kilku podstawowych zasad przeciwepidemicznych, w tym:

- w miejscach publicznych zachowywać dystans społeczny, wynoszący min. 1,5 m od innej osoby, nie gromadzić się w jednym miejscu, nie witać się poprzez podanie ręki, pocałunki, przytulanie (wirus przenosi się drogą oddechową, ale także przez kontakt ze skażoną powierzchnią),
- będąc w otoczeniu innych osób zasłaniać usta i nos maseczką, najlepiej z filtrem lub, wg ECDC, stosować podwójną maseczkę (wirus przenosi się drogą oddechową podczas np. mówienia, kichania, kaszlu). Kaszląc lub kichając zasłaniać usta i nos chusteczką lub zgięciem łokciowym,
- często myć ręce wodą z mydłem (min 30 sek.) lub dezynfekować je wcierając ok. 3 ml preparatu dezynfekcyjnego (1 doza), aż do całkowitego wyschnięcia (istnieje ryzyko przeniesienia wirusa z zanieczyszczonych powierzchni na ręce),
- regularnie wietrzyć pomieszczenia w domu, a także w pracy (w niewietrzonych pomieszczeniach stężenie wirusa utrzymuje się),
- myć wodą z detergentem lub dezynfekować powierzchnie często dotykane, takie jak np.: klamki, poręcze, telefon, kierownica, włączniki światła
(na powierzchniach często dotykanych łatwo gromadzą się i utrzymują drobnoustroje chorobotwórcze, w trym wirusy).

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