Incydent z bezzałogowym statkiem powietrznym w pobliżu amerykańskiej bazy obrony przeciwrakietowej w Redzikowie można potraktować jako kolejne naruszenie strefy zakazu lotów. Można jednak spojrzeć na niego szerzej – jako na test tego, czy polski system bezpieczeństwa nadąża za zmianą charakteru współczesnych zagrożeń.

15 września w pobliżu bazy wykryto cywilny bezzałogowy statek powietrzny. Ministerstwo Obrony Narodowej poinformowało 22 września, że obiekt znajdował się około kilometra od instalacji, nie operował bezpośrednio nad bazą, ale naruszał obowiązującą strefę zakazu lotów. Według MON dron pozostawał pod obserwacją wojskowych systemów obrony powietrznej, nie zbliżył się do newralgicznych elementów bazy, a miejsce przebywania operatora zostało ustalone. Wcześniejsze informacje medialne mówiły również o uruchomieniu procedur obejmujących powiadomienie służb poprzez numer alarmowy 112.

Nie wiemy obecnie, kim był operator ani jaki był rzeczywisty cel lotu. Nie ma podstaw, aby twierdzić, że konkretny incydent w Redzikowie był elementem rosyjskiej lub białoruskiej operacji. Nie mamy również wystarczających danych, żeby oceniać, czy w tej konkretnej sytuacji dron należało zakłócić, przejąć czy zniszczyć.

Nie to jest jednak najważniejszym pytaniem. Kluczowe jest: czy gdyby podobny obiekt był elementem rozpoznania, przygotowania sabotażu albo bezpośredniego ataku, państwo byłoby zdolne przejść w czasie liczonym w sekundach od jego wykrycia do identyfikacji, klasyfikacji zagrożenia, decyzji i skutecznego działania?

Przeciwnik testuje nie pojedynczy radar, lecz cały system państwa

Współczesnych rosyjskich i białoruskich działań hybrydowych nie można analizować wyłącznie jako zbioru odrębnych incydentów. Ich wartość może polegać także na pozyskiwaniu wiedzy o sposobie funkcjonowania przeciwnika: czasie reakcji, procedurach, podziale kompetencji, sposobie komunikacji oraz progach podejmowania decyzji.

Dron jest do tego narzędziem niemal idealnym. Jest tani, łatwo dostępny, pozwala zachować niejednoznaczność intencji i charakteryzuje się niewielkim kosztem ewentualnej utraty. Może wykonywać zwykłe zdjęcia. Może jednak **również prowadzić rozpoznanie, obserwować ochronę fizyczną obiektu, sprawdzać reakcję systemów walki radioelektronicznej czy po prostu mierzyć czas od wykrycia do działania.**

Potencjalny przeciwnik nie musi przy tym zdobywać całej wiedzy metodami klasycznego wywiadu. Przepisy są jawne. Kompetencje instytucji można w dużej części odtworzyć. Dyskusje parlamentarne są publiczne. Po kolejnych incydentach sami opisujemy, kto wykrył obiekt, kogo powiadomiono, jak długo trwała reakcja i jakie środki uruchomiono. Dlatego system bezpieczeństwa trzeba projektować przy założeniu, **że przeciwnik zna nasze słabości albo aktywnie próbuje je poznać.**

Istotny jest również drugi aspekt. Reakcja na tani obiekt może sama stać się źródłem informacji. Uruchomienie sensorów, systemów walki radioelektronicznej, łączności czy efektorów pozwala obserwować nie tylko to, czy potrafimy zniszczyć drona, lecz także w jaki sposób zorganizowana jest nasza obrona. Nie na każdą prowokację powinniśmy więc reagować identycznie. Potrzebna jest przygotowana **wcześniej drabina reakcji – graduated response –** pozwalająca dobrać środek do charakteru zagrożenia, znaczenia chronionego obiektu, ryzyka dla otoczenia oraz kosztu i konsekwencji ujawnienia własnych zdolności.

Prawo zaczyna nadążać. Czy nadąża system?

Jeszcze do niedawna problemem była nie tyle sama możliwość prawna zwalczania dronów – takie uprawnienia wybrane służby i Siły Zbrojne posiadały już wcześniej – ile niespójność regulacji oraz ograniczone możliwości aktywnej ochrony infrastruktury krytycznej. W ostatnich latach przepisy zostały jednak istotnie rozszerzone. Art. 156ze Prawa lotniczego pozwala na zniszczenie, unieruchomienie lub przejęcie kontroli nad BSP stwarzającym zagrożenie dla chronionych obiektów, a uprawnienia te posiadają m.in. Siły Zbrojne, Żandarmeria Wojskowa, Policja i Straż Graniczna. Od lipca 2026 r. poszerzono również możliwość stosowania środków zakłócających w ochronie infrastruktury krytycznej przez pracowników specjalistycznych uzbrojonych formacji ochronnych, w ramach określonego prawem reżimu.

Luka prawna została więc w znacznym stopniu ograniczona. Nie oznacza to jednak automatycznie zamknięcia luki operacyjnej. Przepis nie wykrywa drona, nie identyfikuje jego zamiaru i nie gwarantuje, że przy chronionym obiekcie znajduje się właściwy sensor lub efektor, obsługiwany przez wyszkolony personel zdolny do podjęcia działania w czasie liczonym w sekundach. To właśnie na styku prawa, technologii, procedur, ludzi i dowodzenia może znajdować się dziś największa podatność systemu.

Nie na każdą prowokację należy odpowiadać kolejnymi miliardami

Drugim błędem byłoby wyciągnięcie z kolejnych incydentów wniosku, że odpowiedzią na każde nowe zagrożenie powinien być następny wielomiliardowy program zakupowy. Polska uruchomiła program SAN – ważny element rozwijanej wielowarstwowej obrony przeciwlotniczej, mający zapewnić między innymi skalowalne kinetyczne i niekinetyczne możliwości zwalczania BSP. Potrzebujemy takich zdolności. Nie można jednak traktować żadnego pojedynczego systemu jako ostatecznej odpowiedzi na problem. **Współczesna wojna dronowa jest bowiem także wojną ekonomiczną.**

Doświadczenia Ukrainy, a w 2026 r. również Bliskiego Wschodu, pokazują coraz wyraźniej logikę cost-imposition. Iran podczas kampanii przeciwko państwom Zatoki Perskiej wykorzystywał dużą liczbę relatywnie tanich bezzałogowców równolegle z droższymi systemami rakietowymi. Według CSIS w ciągu pierwszego tygodnia kampanii przeciwko Zjednoczonym Emiratom Arabskim wykryto 1422 drony i 246 pocisków [1]. Jak wskazuje CSIS, celem takiego modelu działania jest nie tylko zadawanie strat, ale **również przeciążanie obrony i wymuszanie zużywania kosztownych interceptorów przeciwko wielokrotnie tańszym środkom napadu.**

Analogiczną ewolucję widzimy w Ukrainie: masowe wykorzystanie tanich dronów, wabików oraz pocisków różnych typów ma stworzyć obrońcy problem jednocześnie operacyjny, technologiczny i ekonomiczny. Dlatego nie możemy odpowiadać na każdy tani środek najdroższym dostępnym efektorem. Jeżeli cel stanowi bezpośrednie zagrożenie dla ludzi albo strategicznego obiektu, należy oczywiście użyć środka gwarantującego jego zniszczenie bez względu na cenę. Problem zaczyna się wtedy, gdy **brak tańszych warstw obrony pozostawia nam wyłącznie najdroższą możliwość reakcji**.

Pięć warstw ochrony – stale aktualizowanych

Polska nie potrzebuje więc jednego „systemu antydronowego”. Potrzebujemy **narodowej, wielowarstwowej architektury ochrony przed bezzałogowymi i innymi precyzyjnymi środkami rażenia**.

1. Pierwszą warstwą powinna być **odporność fizyczna infrastruktury**. Elementy, których utrata powoduje długotrwałe wyłączenie zdolności, powinny być identyfikowane już na etapie projektowania. Krytyczne

transformatory, węzły sterowania, centra łączności, elementy energetyczne i technologiczne powinny – tam, gdzie jest to uzasadnione – otrzymywać osłony konstrukcyjne, separację, redundancję, zabezpieczenia przeciwko uderzeniom z góry, częściowe zagłębienie albo alternatywne możliwości szybkiego odtworzenia. Nie każdy obiekt należy chronić jednakowo. O jego strategicznym znaczeniu nie może decydować wyłącznie cena. Znacznie ważniejsze jest pytanie: **ile czasu potrzeba na odtworzenie zdolności po jego utracie?** Doświadczenia Ukrainy pokazują wagę decentralizacji, fizycznego utwardzania najważniejszych elementów, mobilnych źródeł zastępczych, standardyzacji sprzętu oraz utrzymywania zapasów krytycznych komponentów. Międzynarodowa Agencja Energetyczna wskazuje właśnie te mechanizmy jako jedne z najważniejszych wniosków płynących z wieloletnich rosyjskich ataków na ukraiński system energetyczny.

2. Drugą warstwą musi być **detekcja, śledzenie i identyfikacja**. Nie wystarczy pojedynczy radar. Potrzebna jest fuzja danych pochodzących z sensorów radarowych, radioelektronicznych, optoelektronicznych, akustycznych oraz innych źródeł w jeden obraz sytuacyjny. System powinien możliwie szybko odróżnić własny BSP od obcego, przypadkowe naruszenie od potencjalnego rozpoznania oraz wabik od środka uderzeniowego.
3. Trzecią warstwą powinna być **walka radioelektroniczna i inne środki soft-kill**. W sytuacji, w której jest to możliwe, zakłócenie łączności, nawigacji czy systemu sterowania może być rozwiązaniem szybszym, bezpieczniejszym i zdecydowanie tańszym niż wykorzystanie efektora kinetycznego. Nie wolno jednak budować systemu przy założeniu, że każdy przyszły dron będzie uzależniony od GNSS albo klasycznego radiowego kanału sterowania. Konflikt rosyjsko-ukraiński pokazuje szybki rozwój autonomii, nawigacji wizyjnej, rozwiązań odpornych na zakłócenia oraz alternatywnych metod sterowania.
4. Czwartą warstwą powinny być **relatywnie tanie interceptory**, w tym bezzałogowe systemy przechwytujące, zdolne fizycznie zwalczać cele odporne na EW bez natychmiastowego angażowania kosztownych rakiet przeciwlotniczych.
5. Dopiero piątą warstwę powinny stanowić **klasyczne efektory kinetyczne** – broń lufowa, odpowiednia amunicja, systemy rakietowe i inne środki przeznaczone przede wszystkim dla najbardziej wymagających i niebezpiecznych celów.

Wszystkie warstwy musi połączyć jeden system

Sama liczba sensorów i efektorów nie tworzy jednak zdolności. Nad nimi musi znajdować się odpowiedni system **C2 – command and control** – umożliwiający zamianę informacji w decyzję, a decyzji w działanie. Sensor powinien móc przekazać cel do efektora najlepszego w danej sytuacji. System powinien oceniać prawdopodobieństwo zniszczenia, charakter zagrożenia, znaczenie chronionego obiektu, koszt reakcji i ryzyko uboczne. Musi istnieć jasno zdefiniowany poziom decyzyjny pozwalający działać w czasie odpowiadającym prędkości współczesnego zagrożenia. NATO[2] rozwija obecnie dokładnie takie podejście w ramach Layered Counter-UAS Initiative – LCI-X. Program nie koncentruje się na znalezieniu jednego idealnego systemu, ale na łączeniu sensorów, efektorów, C2 i przemysłu w interoperacyjną architekturę. Co równie istotne, prace prowadzone są w krótkich cyklach eksperymentalnych, z wykorzystaniem doświadczeń wojny w Ukrainie.

I właśnie to powinno być jednym z podstawowych założeń polskiego systemu. **Nie możemy kupić rozwiązania w 2026 r. i zakładać, że w niezmienionej formie będzie odpowiadało zagrożeniom roku 2030 czy 2032.** Architektura musi być otwarta. Musi pozwalać wymieniać sensory, dodawać nowe efektory, modyfikować algorytmy, aktualizować biblioteki zagrożeń oraz wprowadzać rozwiązania, które dzisiaj jeszcze nie istnieją. W tej domenie przewagę uzyska nie państwo, które raz kupiło najlepszy system, ale to, **którego system uczy się szybciej niż system przeciwnika**.

Trzeba również zakładać, że część środków przedostanie się przez obronę. Jest jeszcze jedna lekcja Ukrainy, którą łatwo przeoczyć. Żaden system obronny nie zapewni stuprocentowej skuteczności. Dlatego do sekwencji wykrycia i zwalczania należy dodać jeszcze dwa elementy: **odtwarzanie i uczenie się**. Nie wystarczy zadać pytanie: jak nie dopuścić do trafienia? Trzeba również zapytać: **co stanie się, jeżeli przeciwnik jednak trafi?**

Czy istnieje zapasowy transformator? Czy część zdolności można przejąć z innego obiektu? Czy centrum dowodzenia ma lokalizację alternatywną? Czy dostępne są mobilne źródła energii? Jak szybko przedsiębiorstwo, wojsko albo administracja mogą odzyskać podstawową funkcjonalność? Dlatego też pełny cykl odporności powinien wyglądać:

Anticipate – Protect – Detect – Identify – Decide – Defeat – Recover – Learn.

Ostatnie dwa słowa są równie ważne jak pierwsze sześć.

Technologia wymaga również właściwej polityki kadrowej

Zdolność do uczenia się wymaga nie tylko właściwej technologii, ale również ludzi i ciągłości kompetencji. W domenie systemów bezzałogowych, która zmienia się w tempie liczonym w miesiącach, **polityka kadrowa musi premiować doświadczenie operacyjne, rozumienie technologii, zdolność współpracy z przemysłem oraz szybkie wykorzystywanie doświadczeń z Ukrainy.**

Dzisiejsze nieoficjalne informacje o planowanym odejściu gen. Mirosława Bodnara ze stanowiska Inspektora Wojsk Bezzałogowych Systemów Uzbrojenia nie dają podstaw do oceny personalnej. Stawiają jednak ważniejsze pytanie systemowe: czy zmiana człowieka oznacza również zmianę koncepcji, czy też państwo potrafi zapewnić ciągłość wiedzy, zespołów i kierunku rozwoju niezależnie od rotacji na stanowiskach dowódczych? W tak dynamicznej domenie właściwa polityka kadrowa jest elementem zdolności bojowej. **System musi być oparty na kompetencjach i pamięci instytucjonalnej, a nie na pojedynczych osobach.**

Wojsko musi szerzej otworzyć system na przemysł i doświadczenia pola walki. Elementem uczenia się musi być także sposób pozyskiwania i testowania technologii. Z własnego doświadczenia wielokrotnie spotykam przedsiębiorców, przedstawicieli startupów oraz ludzi wywodzących się z wojska czy służb, którzy dysponują interesującymi rozwiązaniami technologicznymi i jednocześnie sami próbują tworzyć możliwość ich walidacji w warunkach możliwie zbliżonych do realnego konfliktu zbrojnego. Państwo powinno ten potencjał wykorzystywać – ale robić to w sposób zorganizowany, kontrolowany i bezpieczny.

MON wykonało w tym zakresie ważny krok. Decyzja nr 123/MON[3] ustanowiła nowy tryb testowania bezzałogowych statków powietrznych, systemów bezzałogowych i środków ich zwalczania. Testy mają być rozproszone, możliwe do prowadzenia w wielu miejscach, a uczestniczące podmioty podlegają uproszczonej weryfikacji zapewniającej osłonę kontrwywiadowczą. W 2026 r. prowadzono już kolejne nabory, m.in. dotyczące bezzałogowych platform przeznaczonych do zwalczania celów powietrznych.

To właściwy kierunek. Kolejnym krokiem powinien być sprawny mechanizm prowadzący perspektywiczne rozwiązanie od polskiego testu poligonowego do **kontrolowanej walidacji w warunkach odpowiadających realnemu polu walki**, a tam, gdzie jest to możliwe i uzgodnione z partnerem ukraińskim – również do weryfikacji opartej na doświadczeniach wojny trwającej bezpośrednio za naszą granicą. Nie chodzi o wysyłanie przedsiębiorców na front na własną rękę. Wręcz przeciwnie. Taki proces powinien być koordynowany lub nadzorowany przez państwo, objęty właściwą osłoną kontrwywiadowczą oraz adekwatną ochroną informacji wrażliwych: parametrów systemów, wykrytych podatności, odporności na EW, rzeczywistej skuteczności sensorów i efektorów czy stosowanych procedur. Jednocześnie nie można tego procesu nadmiernie zbiurokratyzować.

Jeżeli od zgłoszenia rozwiązania do jego testu upływa rok, podczas gdy technologia pola walki zmienia się co kilka miesięcy, to nawet najlepiej napisana procedura staje się częścią problemu. Państwo nie musi wszystkiego samo wynajdować. Musi natomiast umieć **wyłowić najlepsze rozwiązanie, bezpiecznie je zweryfikować, przekazać rzeczywistemu użytkownikowi, zebrać informację zwrotną, poprawić produkt i szybko zwiększyć skalę jego wykorzystania**. W wojnie technologicznej jednym z najważniejszych parametrów staje się długość cyklu:

problem – rozwiązanie – test – doświadczenie operacyjne – poprawka – produkcja – ponowne użycie.

Jeżeli przeciwnik przechodzi taki cykl w trzy miesiące, a my w trzy lata, nawet wielokrotnie większy budżet nie musi zlikwidować powstałej przewagi.

Nie kolejny system. Architektura odporności

Incydent w Redzikowie nie powinien więc prowadzić wyłącznie do pytania: dlaczego drona nie zestrzelono? Poważniejsze pytanie brzmi: **czy dla Redzikowa, lotniska, rafinerii, terminalu LNG, portu, elektrowni, zakładu przemysłu obronnego, centrum danych czy strategicznej stacji elektroenergetycznej istnieje jeszcze przed pojawieniem się zagrożenia przygotowana architektura działania?**

Kto wykrywa? Kto identyfikuje? Kto podejmuje decyzję? Jaki środek jest pierwszym wyborem? Kiedy uruchamiamy EW, kiedy interceptor, a kiedy efektor kinetyczny? Jak chroniony jest sam obiekt? Co robimy po trafieniu? Jak szybko odbudowujemy

zdolność? I w jaki sposób doświadczenia z jednego incydentu zmieniają ochronę pozostałych obiektów?

Rosja i Białoruś będą poszukiwać naszych słabości i – tam, gdzie będzie to dla nich użyteczne – testować je możliwie niskim kosztem. Nie wiemy, czy dron pod Redzikowem był takim testem i nie ma podstaw, aby dziś to przesądzać. Państwo nie może jednak czekać na potwierdzenie zamiaru przeciwnika, zanim przygotuje się na jego wykorzystanie. Dlatego nie potrzebujemy reaktywnego kupowania kolejnego rozwiązania po każdym incydencie. Potrzebujemy **otwartej, wielowarstwowej architektury odporności**, w której ochrona fizyczna, rozpoznanie, walka radioelektroniczna, tanie interceptory i efektory kinetyczne są połączone wspólnym systemem dowodzenia, odpowiednimi regulacjami, zapleczem przemysłowym oraz mechanizmem ciągłego testowania i adaptacji.

Bo współczesną przewagę uzyska niekoniecznie państwo posiadające najwięcej systemów. Uzyska ją państwo, które **szybciej zamienia informację w decyzję, decyzję w działanie, a doświadczenie z działania w zmianę całego systemu**.

---

[1] Kateryna Bondar, “Unpacking Iran’s Drone Campaign in the Gulf: Early Lessons for Future Drone Warfare”, Center for Strategic and International Studies (CSIS), 10 March 2026. Dane za okres 1–8 marca 2026 r.: 1,422 wykryte drony i 246 pocisków skierowanych przeciwko ZEA.

[2] https://www.act.nato.int/activities/lci-x/ NATO Allied Command Transformation, “Layered Counter-UAS Initiative”, 2026. LCI-X integruje sensory, efektory i systemy command-and-control w interoperacyjną, warstwową architekturę; program realizowany jest w trzymiesięcznych cyklach obejmujących analizę, testowanie i integrację nowych zdolności C-UAS oraz wykorzystuje doświadczenia Ukrainy w zwalczaniu rosyjskich systemów bezzałogowych.

[3] Decyzja Nr 123/MON Ministra Obrony Narodowej z dnia 12 września 2025 r. w sprawie organizacji i trybów testowania w Siłach Zbrojnych RP bezzałogowych statków powietrznych i bezzałogowych systemów uzbrojenia oraz środków zwalczania bezzałogowych statków powietrznych i bezzałogowych systemów uzbrojenia, Dz. Urz. MON z 2025 r., poz. 147.