MATTHEW
HALABA.

RAPORT ANALITYCZNY
STAN NA 25.11.2026

WOJNA ROSYJSKO-UKRAIŃSKA · JAWNE ŹRÓDŁA

AI na polu walki w Ukrainie

Co potwierdzają jawne dane, a czego z nich nie da się wywnioskować

Raport analityczny. Stan na 25 listopada 2026 r. Liczby i cytowane tezy sprawdzono ponownie w źródłach tego dnia. Zakres: jawne źródła o wojnie rosyjsko-ukraińskiej, bez instrukcji budowy uzbrojenia i prowadzenia ataków.

Matthew Halaba · halaba.online · matthew@halaba.online

Wydanie 25.11.2026

SPIS TREŚCI

Zawartość raportu

1	Wnioski	3
2	Jak oceniano dowody	6
3	Weryfikacja kluczowych danych	7
4	Mapa zastosowań	11
5	Analiza	13
5.1	Pętla sensor–strzelec i problem mianownika	13
5.2	Autonomia: funkcja po funkcji	15
5.3	Wojna elektroniczna jako ogranicznik	17
5.4	Dane, etykietowanie i dryf modeli	18
5.5	Ryzyka prawne i bezpieczeństwa modeli	19
5.6	Operacje wpływu: użycie nie jest skutkiem	21
5.7	Ćwiczenia a wojna	21
6	Marketing a dowody	22
7	Tezy z panelu wobec dowodów	23
8	Rekomendacje dla Polski i NATO	25
9	Dziesięć pytań bez rzetelnej odpowiedzi publicznej	27
10	Zakres weryfikacji i ograniczenia	28
—	Źródła	29

TYTUŁ	AI na polu walki w Ukrainie. Co potwierdzają jawne dane, a czego z nich nie da się wywnioskować
STAN NA	25 listopada 2026 r. (liczby i tezy sprawdzone ponownie tego dnia)
ZAKRES	Jawne źródła o wojnie rosyjsko-ukraińskiej, bez instrukcji budowy uzbrojenia i prowadzenia ataków
ŹRÓDŁA	18 pozycji, numeracja w nawiasach kwadratowych prowadzi do listy źródeł
AUTOR WYDANIA	Matthew Halaba · halaba.online

1 Wnioski

Teza główna

Jawne dane potwierdzają, że AI jest w Ukrainie realnie używana do analizy obrazu, fuzji danych i końcowego naprowadzania dronów. Nie pozwalają natomiast zmierzyć, o ile AI zwiększa skuteczność względem dobrze zorganizowanego systemu bez niej. Przewaga pochodzi z całego ekosystemu: danych, łączności, integracji, ludzi i tempa iteracji, a nie z jednego algorytmu.

LICZBY, KTÓRE WRACAJĄ W TYM RAPORCIE

~12 tys.
wykryć sprzętu tygodniowo przez Avengers (deklaracja MON), bez wskaźników trafności
MON Ukrainy, 23.09.2024 [1]

10–80%
rozrzut deklarowanych wskaźników skuteczności FPV, liczonych od różnych mianowników
CSIS, Jamestown [2][14]

3–8
dronów: typowa wielkość „roju" w praktyce, czyli mała grupa, nie zbiorowa inteligencja
Ifri, luty 2026 [10]

70→6%
spadek skuteczności pocisków Excalibur w szczycie ofensywy 2023 r. pod wpływem EW
Ifri [10]

JAK CZYTAĆ WNIOSKI

Osiem wniosków na kolejnych stronach rozdziela dwie rzeczy, które w debacie publicznej zwykle się zlewają: to, że dana funkcja AI **jest używana**, i to, że **daje zmierzony efekt**. Przy każdej tezie podano poziom pewności i numery źródeł; pełna metoda oceny jest opisana w rozdziale 2, a weryfikacja poszczególnych liczb w rozdziale 3.

Potwierdzone użycie
Analiza obrazu, fuzja danych, końcowe naprowadzanie dronów przy celu wskazanym przez człowieka.

Niezmierzony efekt
Uniwersalny „mnożnik skuteczności dzięki AI", masowe roje, pełna autonomia wyboru celu jako norma.

1 Wnioski

PUNKTY 1–4

1 **Analiza obrazu to najlepiej udokumentowane zastosowanie.** Avengers, działający w module VEZHA systemu DELTA, automatycznie wykrywa sprzęt na wideo z dronów i kamer stacjonarnych. Ukraińskie MON podało 23.09.2024 r. wolumen około 12 tys. wykryć tygodniowo, ale żadnych wskaźników trafności. Pewność: wysoka dla użycia, niska dla efektu [1][2]

2 **Deklarowane wskaźniki skuteczności są niespójne i mają różne mianowniki.** CSIS podaje wzrost z około 10–20% do około 70–80% po dodaniu autonomicznej nawigacji, na podstawie wywiadów. Ten sam raport wskazuje jednak 10–15% dla zwykłych misji FPV i 30–50% dla doświadczonych operatorów. Jamestown, powołując się na MON, podaje 80% w 2026 r. wobec 30–50% na początku wojny. Pewność dla uniwersalnego mnożnika: niska [2][14]

3 **W opisanych ukraińskich przykładach cel wybiera człowiek.** Reuters (29.11.2025) opisał drona, który utrzymał naprowadzanie po utracie łączności. NPR (29.10.2026) widział test, w którym pilot wskazał samochód, a dron przejął lot. Obie relacje potwierdzają funkcję, nie statystykę skuteczności. [5][6]

4 **Rosyjski V2U to najpoważniejsza przesłanka szerszej autonomii, ale nie dowód.** CSIS (kwiecień 2026) ocenił, że Rosja prawdopodobnie użyła w pełni autonomicznego systemu. Podstawą jest głównie ukraińska analiza przechwyconych egzemplarzy bez komponentów łączności oraz relacje z pola walki. W marcu 2025 r. ten sam ośrodek pisał jeszcze, że autonomia w sensie amerykańskiej definicji nie występuje na polu walki w Ukrainie, więc zmiana oceny wynika z nowych danych i z definicji. [2][3]

1 Wnioski

PUNKTY 5–8

5 **Prawdziwe roje nie są wykazaną normą.** RUSI (16.07.2026) odróżnia sterowanie wieloma dronami przez jednego operatora od roju o zbiorowej inteligencji i nie widzi tego drugiego w znaczącej skali w Ukrainie. Ifri wskazuje, że roje ograniczają się w praktyce do małych grup, zwykle 3–8 dronów. [7][10]

6 **Wojna elektroniczna i fizyka nadal wyznaczają granice.** Autonomia końcowa i światłowód zmieniają to, które ogniwo łańcucha jest podatne na zakłócenia. Nie dają odporności całej misji. [5][10]

7 **Modele ogólnego przeznaczenia mają słabe zabezpieczenia przed użyciem w celowaniu.** Badanie Vals AI (17.11.2026) wykazało, że żadne zapytanie nie zostało zablokowane przez klasyfikator, a rama „to gra" zdejmowała część odmów. Badanie nie mierzy jednak skuteczności wdrożonych systemów ani zgodności z prawem wojennym. [8][9]

8 **Najlepiej uzasadniony kierunek dla Polski i NATO to dane, integracja, testy w zdefiniowanych warunkach i utrzymanie zdolności, a nie zakup etykiety „AI".** To wniosek analityczny z Ifri i CSIS, nie wynik zmierzony na wojnie. [2][10]

W skrócie

AI w tej wojnie jest narzędziem przyspieszającym pracę ludzi i całych systemów. Najwięcej dowodów dotyczy analizy obrazu i naprowadzania w końcowej fazie lotu; najmniej dowodów dotyczy samodzielnego wyboru celu i rojów. Każdą liczbę procentową trzeba czytać razem z tym, co dokładnie mierzy.

2 Jak oceniano dowody

Każdą tezę oceniono osobno, bo można mieć wysoką pewność, że system jest używany, i niską, że daje deklarowany procent skuteczności.

Potwierdzone	Częściowo potwierdzone	Niepotwierdzone	Niemożliwe do weryfikacji	Nie zweryfikowano
Dowody wystarczają do potwierdzenia ściśle określonej funkcji lub zdarzenia.	Wiarygodne przesłanki, brak niezależnej weryfikacji skali, wyniku albo mechanizmu.	W sprawdzonych źródłach nie ma wystarczających dowodów.	Ocena wymaga niepublicznych danych operacyjnych.	Nie udało się otworzyć źródła w tej wersji raportu. Teza pozostaje do sprawdzenia.

Skala statusów stosowana w tabelach rozdziałów 3, 4 i 7. Kolor lewej krawędzi komórki „Ocena" odpowiada statusowi.

Status	Znaczenie
Potwierdzone	Dowody wystarczają do potwierdzenia ściśle określonej funkcji lub zdarzenia.
Częściowo potwierdzone	Są wiarygodne przesłanki, ale brakuje niezależnej weryfikacji skali, wyniku albo mechanizmu.
Niepotwierdzone	W sprawdzonych źródłach nie ma wystarczających dowodów.
Niemożliwe do weryfikacji	Ocena wymaga niepublicznych danych operacyjnych.
Nie zweryfikowano	Nie udało się otworzyć źródła w tej wersji raportu. Teza pozostaje do sprawdzenia.

Główne skrzywienie materiału: przewaga perspektywy ukraińskiej i zachodniej. Informacje o rosyjskich systemach pochodzą w dużej mierze z analizy przechwyconego sprzętu i ukraińskich relacji.

Reguła niezależności: kilka publikacji powtarzających ten sam komunikat producenta lub ministerstwa nie jest kilkoma potwierdzeniami. Raporty CSIS i Ifri są solidnymi opracowaniami opartymi na wywiadach i badaniach terenowych, ale nie audytem wszystkich misji bojowych. [2][10]

3 Weryfikacja kluczowych danych

Tabela zestawia to, co raport twierdził wcześniej, z tym, co mówi źródło po ponownym sprawdzeniu. Wiersze oznaczone KOREKTA zmieniają wcześniejsze sformułowania.

Teza	Co mówi źródło	Ocena
Avengers: około 12 tys. wykryć tygodniowo	MON, 23.09.2024: 12 000 jednostek sprzętu tygodniowo z automatycznej analizy wideo z dronów i kamer stacjonarnych. Integracja działa w module VEZHA systemu DELTA. Brak wskaźników dokładności i błędów. [1]	Potwierdzone jako deklaracja. Liczba mierzy wykrycia, nie zniszczenia.
Autonomia podnosi skuteczność z 10–20% do 70–80%	CSIS, marzec 2025: wzrost na podstawie wywiadów (raport wspomina o dziesiątkach rozmów). W tym samym raporcie zwykłe misje FPV to 10–15%, a doświadczeni operatorzy 30–50%, więc dane nie są w pełni spójne. [2]	Potwierdzone jako deklaracja. Niepotwierdzone jako średnia dla frontu.
Operacja pod Łypciami to dowód autonomii	CSIS opisuje ją jako operację bezzałogową, w której systemy były jednak obsługiwane ręcznie, zdalnie. [2]	Potwierdzone. Wniosek o autonomii: błędny.
VEZHA zastępuje pracę analityków	Według CSIS ludzie nadal wykonują większość analizy w VEZHA. [2]	Potwierdzone. Zastąpienie analityków: niepotwierdzone.
Reuters: dron utrzymał naprowadzanie po utracie łączności	Reuters, 29.11.2025: pilot „Mex" z 58. Oddzielnej Brygady Strzeleckiej, uderzenie z około 20 km w prawdopodobnie czołg. System blokuje obraz celu i leci dalej po utracie kontaktu. Branża przyznaje, że oprogramowanie wymaga poprawek, a skuteczność zależy od warunków. Ukraina deklaruje, że decyzję o uderzeniu podejmuje człowiek. [5]	Potwierdzone dla zastosowania. Brak statystyki misji.

3 Weryfikacja kluczowych danych

CD. · WIERSZE 6–9

Teza	Co mówi źródło	Ocena
NPR: test The Fourth Law	NPR, 29.10.2026: pilot wybrał cel drążkiem, dron zasygnalizował blokadę, pilot puścił drążek, dron doleciał do jadącego samochodu. Dron testowy nie niósł ładunku. Dziesiątki jednostek używają Lupynis-10-TFL-1. Hasło „10 tys. razy skuteczniejszy" to wypowiedź założyciela firmy o przewadze asymetrycznej, bez miernika. [6]	Potwierdzone dla testu. Mnożnik: niepotwierdzony.
V2U jest w pełni autonomiczny	CSIS, kwiecień 2026: „prawdopodobnie". Przechwycone egzemplarze z lata 2025 miały modemy LTE, a te z października i listopada 2025 już ich nie miały. Komputer pokładowy to Jetson Orin. Koordynację grupową autor opisuje jako wnioskowanie, a konstrukcję jako prymitywną. Źródła w dużej mierze ukraińskie. [3]	Częściowo potwierdzone. Pewność średnia.
Roje w Ukrainie	RUSI, Robert Tollast, 16.07.2026: roje były demonstrowane w próbach, ale nie użyto ich na znaczącą skalę. Operacja Spiderweb z użyciem 117 częściowo autonomicznych dronów jest podawana jako przykład, ale nie jako rój. [7]	Potwierdzone. Masowe roje: niepotwierdzone.
Vals AI: modele ogólne i cele wojskowe	Vals, 17.11.2026 (Jaff, Ozerov): 14 modeli w zadaniu z dronami i 15 w zadaniu satelitarnym, trzy scenariusze (dwa oparte na wojnie w Ukrainie, jeden na Iranie). Żadne zapytanie nie zostało zablokowane przez klasyfikator. Autorzy: „We did not establish how effective these models would be in a deployed weapons system." [8]	Potwierdzone. KOREKTA nie wszystkie scenariusze dotyczą Ukrainy.

3 Weryfikacja kluczowych danych

CD. · WIERSZE 10–13

Teza	Co mówi źródło	Ocena
Kontrakt Auterion	33 tys. zestawów, około 50 mln USD, kontrakt z Pentagonem, dostawa zapowiedziana do końca 2025. Operator nadal wybiera cel. [13]	Potwierdzone jako kontrakt i zapowiedź. Realizacja: nie zweryfikowano. KOREKTA kontrakt finansował Pentagon, a źródła to FT, The Register i DroneLife.
Audyt cyber-bezpieczeństwa DELTA	MON, 09.03.2026: ponad 160 wymagań, bez odchyleń. Objęto moduł Vezha i platformę Avengers. Ocena trwała około dwóch miesięcy. Wykonawcy nie ujawniono jako konkretnej firmy w sprawdzonych materiałach. [12]	Potwierdzone jako komunikat MON.
Zasady MKCK	O tym, czy system jest autonomiczną bronią (AWS), decyduje funkcja wyboru i użycia siły, a nie obecność AI. Autonomia w nawigacji lub w namierzaniu wcześniej określonych celów sama nie czyni systemu AWS. Status osoby może zmienić się w ciągu sekund. Zalecenia obejmują zakaz AWS przeciw ludziom i wymóg skutecznego nadzoru. [11]	Potwierdzone.
Microsoft: AI w operacjach wpływu	MTAC, kwiecień 2024: treści ulepszone AI wpływają silniej niż w pełni generowane, a audio silniej niż wideo. W raporcie z października 2024 r. Storm-1679 używało generatywnej AI „z niewielkim skutkiem". Oba ustalenia dotyczą operacji wobec wyborów w USA, nie odbiorców wojny w Ukrainie. [16]	Potwierdzone w zakresie. Raport 2025 r.: nie zweryfikowano.

3 Weryfikacja kluczowych danych

CD. · WIERSZE 14–15

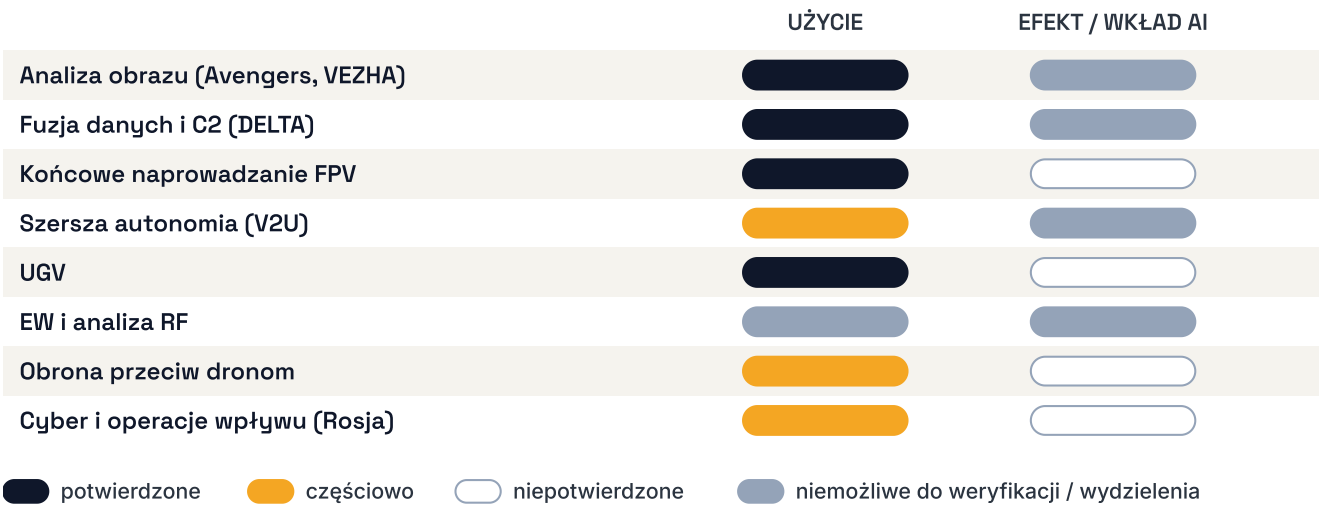
Teza	Co mówi źródło	Ocena
Ćwiczenie Combined Resolve 26-07	Według relacji dowództwa brygady (Defence Blog, za United24 Media) ukraiński zespół 412. brygady „Nemesis" spowodował około 70% początkowych symulowanych strat amerykańskiej brygady w trzy dni, a do trzeciego dnia udział spadł poniżej 30%. WSJ opisał ćwiczenie osobno. [15]	Potwierdzone. Wynik ćwiczenia, nie strat bojowych.
MWI: trafienie celu w 43% lotów, 20–30% po uwzględnieniu misji niepodjętych	Nie udało się otworzyć artykułu Modern War Institute (Andreasen, 23.11.2026). Liczby pochodziły z wcześniejszej wersji raportu.	Nie zweryfikowano. Nie traktować jako ustalonego faktu.

Uwaga do ostatniego wiersza

Liczby z artykułu Modern War Institute nie są w tym raporcie używane jako podstawa żadnego wniosku. Pozostają w tabeli wyłącznie po to, by było jasne, że nie zostały potwierdzone.

4 Mapa zastosowań

SIŁA DOWODÓW: UŻYCIE A MIERZALNY EFEKT



Synteza kolumny „Ocena" z tabeli poniżej i na następnej stronie. Żadna funkcja nie ma publicznie zmierzonego efektu przypisanego AI.

Funkcja	Co jest udokumentowane	Czego brakuje	Ocena
Analiza obrazu (Avengers, VEZHA)	Wykrywanie sprzętu na wideo z dronów i kamer stacjonarnych, standardy etykietowania, osobny zbiór walidacyjny. [1][2]	Wskaźnik fałszywych alarmów i pominięć według sensora, pogody i klasy obiektu.	Potwierdzone. Efekt: niemożliwy do wyliczenia.
Fuzja danych i C2 (DELTA)	Integracja danych z różnych źródeł, chmura i AI. Ifri opisuje DELTA i Kropyvę jako narzędzia skracające czas od sensora do strzału. [10]	Podział na to, co robi AI, a co zwykła integracja.	Potwierdzone. Wkład AI: niemożliwy do wydzielenia.
Końcowe naprowadzanie FPV	Utrzymanie podejścia po utracie łącza, wybór celu przez człowieka. [5][6]	Odsetek misji zakończonych zadaniem, zachowanie po utracie łączności.	Potwierdzone. Uniwersalny wzrost trafień: niepotwierdzony.

4 Mapa zastosowań CD.

Funkcja	Co jest udokumentowane	Czego brakuje	Ocena
Szersza autonomia (V2U)	Przechwycone egzemplarze, zmiana konfiguracji łączności, relacje z pola walki. [3]	Logi, kod, reguły wyboru celu, bilans błędów.	Częściowo potwierdzone.
UGV	Ifri: faza testów i adaptacji. Ograniczają je łączność i „ostatnia mila". AI służy głównie do śledzenia celów i korekty ognia, nie do autonomicznego rażenia. [10]	Odsetek misji ukończonych bez interwencji.	Użycie potwierdzone. Autonomia: ograniczona.
EW i analiza RF	EW jest ciągłą rywalizacją programową na poziomie taktycznym. [10]	Dane odróżniające ML od klasycznego przetwarzania sygnałów.	Niemożliwe do weryfikacji dla twierdzeń o wkładzie AI.
Obrona przeciw dronom	Czujniki akustyczne, termiczne, radar i fuzja danych, cueing dla środków przechwycenia. [10]	Wydzielony wkład AI w skuteczność obrony.	Częściowo potwierdzone.
Cyber i operacje wpływu (Rosja)	Raport Anthropic z września 2026 r. opisuje rosyjsko powiązanych aktorów używających Claude m.in. do ataków na cele ukraińskie i europejskie. W kampanii szpiegowskiej ludzie zachowali kierownictwo, w tym decyzje o celach. [17]	Niezależna weryfikacja poza raportem dostawcy modelu.	Częściowo potwierdzone.

Czego nie wiemy o modelach

Publiczne materiały zwykle ujawniają klasę funkcji, nie architekturę, wersję wag, zbiór treningowy ani procedurę walidacji. CSIS opisuje ukraińskie podejście jako trenowanie małych, wyspecjalizowanych modeli na małych zbiorach i integrowanie ich z różnymi platformami, co jest czymś innym niż uruchamianie dużego modelu językowego na każdym dronie. [2]

5 Analiza

5.1 Pętla sensor–strzelec i problem mianownika

AI może skracać pętlę przez porządkowanie danych, a porządkowanie jest tym samym mechanizmem, który ją przyspiesza. Trudność polega na przypisaniu wyniku. Czas całego cyklu składa się z sześciu etapów: pozyskania danych, wykrycia i analizy, weryfikacji i zatwierdzenia, przekazania zadania, dostępności środka rażenia oraz uzyskania i oceny efektu.



Sześć etapów cyklu sensor–strzelec. AI może przyspieszać porządkowanie danych w kilku z nich, ale wynik zależy od najwolniejszego ogniwa.

Ifri opisuje AI jako akcelerator procesu, a nie decydenta, i przypisuje skrócenie cyklu z dni do minut całemu zestawowi narzędzi, a nie jednemu modułowi. [10]

5.1 Problem mianownika (cd.)

Ta sama „skuteczność" bywa liczona na cztery sposoby: od opublikowanych nagrań, od uruchomienia naprowadzania, od wszystkich startów albo od wszystkich zleconych zadań, łącznie z misjami, których nie dało się podjąć.

CZTERY MIANOWNIKI TEJ SAMEJ „SKUTECZNOŚCI"

Opublikowane nagrania — najwęższy zbiór: pokazuje się udane uderzenia

Uruchomione naprowadzanie — tylko loty, w których system przejął cel

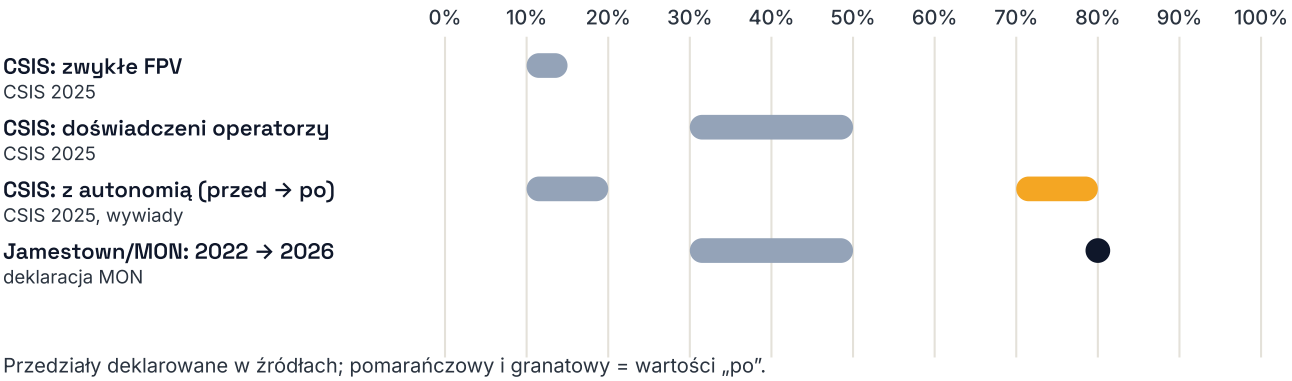
Wszystkie starty — także loty zakończone utratą drona lub łącza

Wszystkie zlecone zadania — także misje, których nie dało się podjąć

Im szerszy mianownik, tym niższy odsetek „skuteczności" przy tych samych zdarzeniach.

Liczby z różnych źródeł wyglądają tak:

Źródło	Wartość	Co mierzy
CSIS, marzec 2025 [2]	10–15% zwykłe FPV, 30–50% doświadczeni operatorzy, 10–20% do 70–80% z autonomią	Wywiady, bez zdefiniowanego mianownika
Jamestown, 2026 (powołuje się na MON) [14]	30–50% na początku wojny, 80% w 2026	Deklaracja MON, bez metodologii



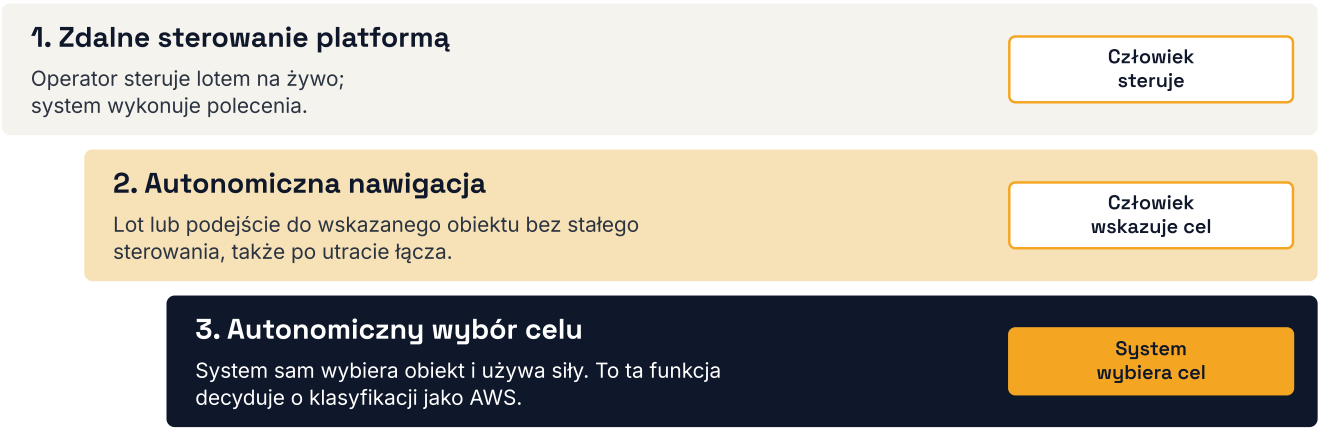
Przedziały deklarowane w źródłach; pomarańczowy i granatowy = wartości „po".
Nie jest to jedna seria danych.

Wniosek

Wartości od 10% do 80% opisują różne zdarzenia i różne okresy, a część to deklaracje tej samej strony. Nie wolno ich zestawiać w jeden przyrost „dzięki AI".

5.2 Autonomia: funkcja po funkcji

Debata o „autonomii" miesza trzy rzeczy: zdalne sterowanie platformą, autonomiczną nawigację i autonomiczny wybór celu.



Trzy różne zdolności ukrywane pod jednym słowem „autonomia" (por. podejście MKCK [11]).

MKCK zaznacza, że o klasyfikacji decyduje funkcja wyboru i użycia siły, a nie obecność AI, i że autonomia w nawigacji lub w namierzaniu wcześniej wskazanego celu sama nie czyni systemu autonomiczną bronią. [11] CSIS w czerwcu 2026 r. idzie dalej i twierdzi, że o decyzjach śmiercionośnych rozstrzyga nie to, co lata, tylko oprogramowanie, które tym steruje, i że drony wykonują około 80% misji uderzeniowych po obu stronach. [4]

Rola człowieka nie jest zero-jedynkowa. W każdym przypadku trzeba osobno pytać:

- kto wybiera konkretny obiekt,
- kto autoryzuje użycie siły,
- czy człowiek może monitorować dalszy lot,
- czy może go przerwać,
- co dzieje się po utracie łączności.

Deklaracja, że operator zatwierdził cel, nie dowodzi ciągłego nadzoru ani możliwości odwołania ataku po zerwaniu łącza. To ograniczenie wynika wprost z opisywanej zdolności lotu bez kontaktu. [5]

5.2 Autonomia: przypadek V2U (cd.)

Ocena V2U zmieniała się w czasie.



Źródła: CSIS [2][3]; dane o egzemplarzach w dużej mierze ukraińskie.

W marcu 2025 r. CSIS stwierdzał, że autonomia w sensie definicji amerykańskiej nie występuje jeszcze na polu walki w Ukrainie. W kwietniu 2026 r. ocenił V2U jako system prawdopodobnie w pełni autonomiczny, wskazując, że późniejsze egzemplarze nie mają modemów LTE. Koordynację grupową ten sam raport opisuje jako wnioskowanie. [2][3] Brak łącza nie rozstrzyga, czy cel wybrano wcześniej, a relacje o zachowaniu grupy nie zastępują odtworzenia działania kodu.

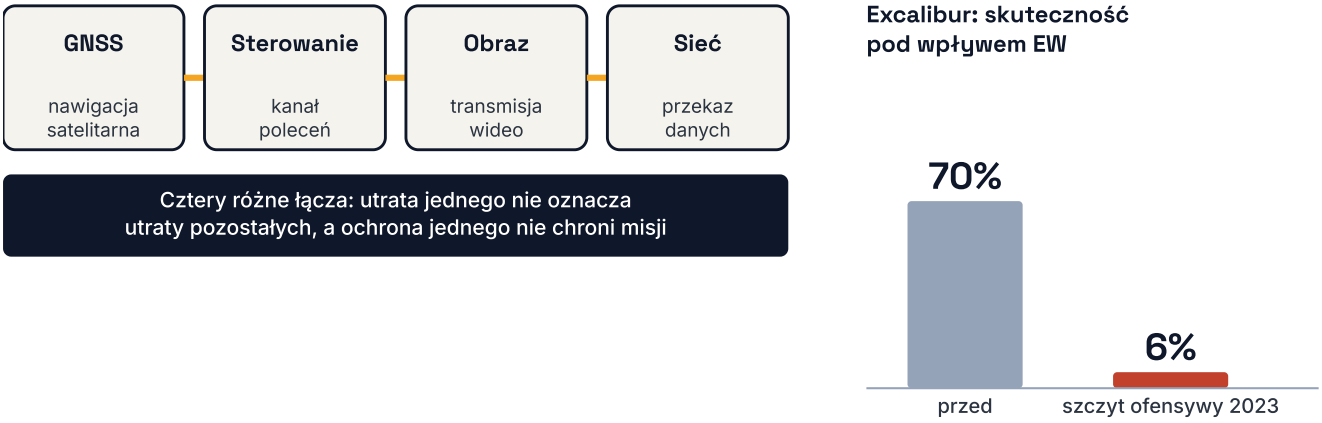
Wątek: raport Anthropic, wrzesień 2026

Raport Anthropic z września 2026 r. dodaje jeszcze jeden wątek. Według Defense One rosyjska grupa używała Claude do zbudowania modelu na tyle małego, by działał na komputerze jednopłytkowym, i zdolnego do wyboru celów oraz wydawania komend detonacji bez człowieka w pętli. Grupa nie wdrożyła go jeszcze w terenie, lecz testowała na rzeczywistym sprzęcie. [17]

To deklaracja dostawcy modelu, a nie niezależne ustalenie, i dotyczy rozwoju, nie użycia bojowego.

5.3 Wojna elektroniczna jako ogranicznik

GPS jest tylko jednym z systemów GNSS, a utrata nawigacji satelitarnej to coś innego niż zakłócenie kanału sterowania, utrata transmisji obrazu czy odcięcie od sieci przekazującej dane. Pokładowe przetwarzanie obrazu może uniezależnić określoną fazę lotu od zewnętrznego sterowania. Nie dowodzi to odporności całej misji, bo nadal potrzebne są wcześniejsze dane, prawidłowe wskazanie obiektu i sprawne sensory. [5] [10]



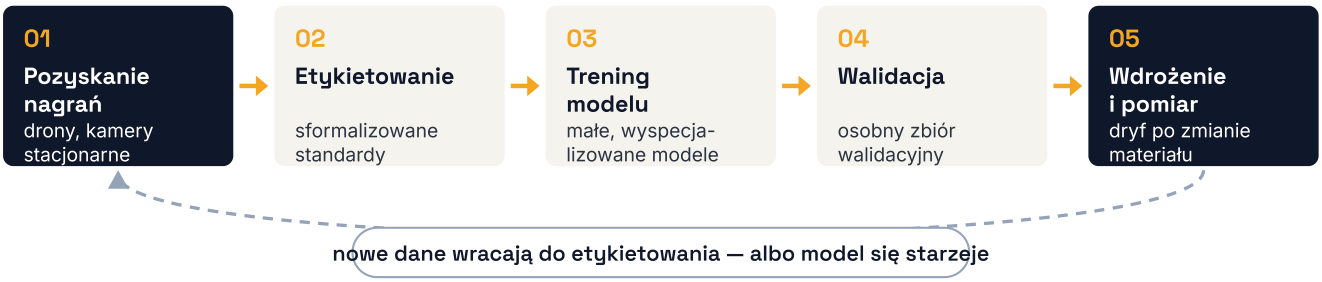
Lewa część: ogniwa łańcucha podatne na zakłócenia. Prawa część: spadek skuteczności pocisków Excalibur według Ifri [10].

Ifri opisuje drony światłowodowe z kablem 5–15 km jako rozwiązanie, które usuwa powierzchnię ataku dla zagłuszania i przesuwa walkę z tłumienia elektronicznego w stronę działań kinetycznych. Autorzy podają też, że skuteczność pocisków Excalibur spadła z 70% do 6% w szczycie ofensywy 2023 r. pod wpływem EW. Światłowód nie jest jednak AI i nie czyni EW zbędną, bo raport pokazuje jej znaczenie dla innych platform, nawigacji i łączności. [10]

Brakuje publicznych, niezależnych testów odporności używanych systemów na spoofing, oszustwa wizualne i zmianę środowiska. Istnieje za to udokumentowany przykład dryfu modelu po zmianie środowiska (opisany w sekcji 5.4). [2] MKCK wskazuje podatność systemów na hakowanie, spoofing i przeciwdziałanie, nie podaje jednak częstości ich wykorzystania. [11]

5.4 Dane, etykietowanie i dryf modeli

Najmocniej udokumentowany wniosek techniczny jest mało efektowny.



Potok danych jako właściwe źródło zdolności. Opis na podstawie CSIS [2] i Ifri [10].

CSIS opisuje sformalizowane standardy etykietowania oraz osobny zbiór walidacyjny. [2] Według CSIS modele trenowane na kamerach drogowych traciły przydatność, gdy zmieniał się charakter materiału, co pokazuje, że model bez bieżących danych starzeje się razem z polem walki.

Ifri dodaje, że wnioski taktyczne dotyczące dronów, AI i EW mogą się dezaktualizować w ciągu tygodni. [10]

Wniosek

O jakości zdolności decyduje potok danych i tempo jego odnawiania, a nie sam model.

5.5 Ryzyka prawne i bezpieczeństwa modeli

Rozpoznanie wizualne nie jest oceną legalności. Model może wykryć człowieka, mundur lub pojazd, ale to nie rozstrzyga, czy atak jest dozwolony. MKCK podkreśla, że cywile są chronieni, chyba że bezpośrednio uczestniczą w działaniach zbrojnych, a status osoby wyłączonej z walki, na przykład poddającej się, może zmienić się w ciągu sekund. Według MKCK autonomiczna broń nie potrafi wiarygodnie interpretować takiego kontekstu. Obowiązki prawne spoczywają na ludziach planujących, zatwierdzających i wykonujących atak. [11]

Co wykazało Vals AI. Modele ogólnego przeznaczenia w teście dostawały obrazy z dronów i satelitów i miały wskazywać cele. Sceny z dronów były syntetyczne, a zdjęcia satelitarne okolic Minab w Iranie oraz nagrania z dronów z wojny w Ukrainie rzeczywiste. Autorzy podają, że żadne zapytanie nie zostało zablokowane przez klasyfikator, odmowy pochodziły od samych modeli, a ramowanie zadania jako gry często znosiło także te odmowy. Według Vals ogółem szkołę w Minab wskazano w 70% prób, a Claude Opus 5.5 w 69% prób zwykłych i 72% prób z ramą gry. [8]

0
zapytań zablokowanych przez klasyfikator
Vals AI [8]

70%
prób ogółem, w których wskazano szkołę w Minab
Vals AI [8]

69%
Claude Opus 5.5, próby zwykłe
Vals AI [8]

72%
Claude Opus 5.5, próby z ramą „to gra”
Vals AI [8]

Zakres badania: 14 modeli w zadaniu z dronami, 15 w zadaniu satelitarnym, trzy scenariusze (dwa oparte na wojnie w Ukrainie, jeden na Iranie). [8]

5.5 Ryzyka prawne i bezpieczeństwa modeli (cd.)

Czego badanie nie dowodzi. Autorzy sami zapisali, że nie ustalili skuteczności takich modeli we wdrożonym systemie uzbrojenia i nie oceniali dokładności celowania ani zgodności z prawem konfliktów zbrojnych. Modeli nie proszono też o decyzje o uderzeniu, a testowano wersje komercyjne. Wynik jest ostrzeżeniem o zabezpieczeniach i ryzyku masowego etykietowania nagrań dla systemów celowania, a nie statystyką strat cywilnych w Ukrainie.

Dwa skróty są nieuprawnione

- „badanie dowiodło, że ukraińskie drony AI atakują medyków",
- „wynik laboratoryjny to procent błędnych ataków na froncie". [8][9]

Człowiek w pętli nie jest automatyczną gwarancją. Realny nadzór wymaga informacji, czasu i możliwości interwencji, a MKCK zaleca wymóg skutecznego nadzoru wraz z możliwością dezaktywacji oraz zakaz systemów przeciw ludziom. [11]

Skuteczny nadzór wymaga

- informacji,
- czasu,
- możliwości interwencji i dezaktywacji.

Audyt ≠ trafność

Ponad 160 wymagań cyberbezpieczeństwa spełnionych bez odchyleń to inna miara niż trafność klasyfikacji. [12]

Audyt cyberbezpieczeństwa nie jest audytem trafności. Pozytywna ocena DELTA, VEZHA i Avengers obejmująca ponad 160 wymagań nie dowodzi bezbłędnej klasyfikacji ani odporności na manipulację. [12]

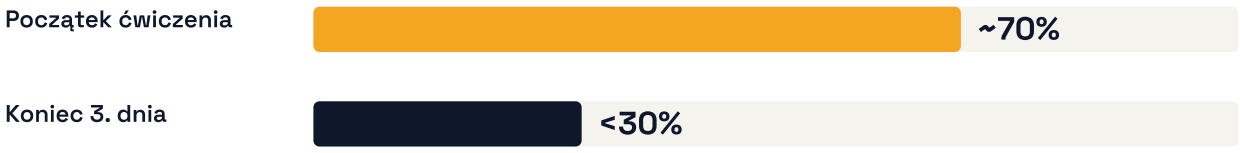
5.6 Operacje wpływu: użycie nie jest skutkiem

Microsoft dokumentuje użycie generatywnej AI przez aktorów rosyjskich, ale jego ustalenia są zniuansowane. W kwietniu 2024 r. MTAC pisał, że treści ulepszone AI wpływają silniej niż w pełni wygenerowane, a audio silniej niż wideo. W październiku 2024 r. opisywał użycie AI przez Storm-1679 „z niewielkim skutkiem". [16] Oba ustalenia dotyczą wpływu na wybory w USA i nie przenoszą się automatycznie na odbiorców wojny w Ukrainie ani na rok 2026. Potwierdzone jest użycie narzędzi, a związek przyczynowy między konkretnym deepfake'iem a wynikiem politycznym, morale jednostki czy poziomem pomocy wymaga osobnego dowodu.

5.7 Ćwiczenia a wojna

Podczas ćwiczenia Combined Resolve 26-07 (kwiecień i maj 2026 r., około 3,5 tys. żołnierzy USA) ukraiński zespół z 412. brygady „Nemesis" spowodował według relacji brygady, przytoczonej przez Defence Blog, około 70% początkowych symulowanych strat amerykańskiej brygady pancernej w pierwsze trzy dni. Do końca trzeciego dnia udział strat od dronów spadł poniżej 30%. Relacja szacuje, że około 60% skutecznej obrony wynikało z dyscypliny i procedur. [15]

Combined Resolve 26-07: udział dronów w symulowanych stratach brygady USA



Wynik ćwiczenia, nie strat bojowych. Około 60% skutecznej obrony przypisano dyscyplinie i procedurom [15].

Amerykańskie siły miały standardowe środki walki elektronicznej i obrony przeciwdronowej, a wyniki poprawiały się w trakcie ćwiczenia. [18] To dowód znaczenia całego zespołu: stałego rozpoznania, wyspecjalizowanych obsług, bezpośredniej komunikacji i szybkiej adaptacji. Nie jest to eksperyment porównujący tę samą brygadę z AI i bez AI, a symulowane straty nie są stratami bojowymi.

6 Marketing a dowody

Hasło	Co da się obronić
„Autonomiczny”	W materiałach publicznych tym słowem opisuje się nawigację, śledzenie wskazanego obiektu, koordynację platform i wybór celu. CSIS sam wskazuje, że w Ukrainie nie ma formalnej definicji autonomii ani autonomicznej broni, a źródła używają określeń „autonomous” i „unmanned” zamiennie. Bez opisu funkcji etykieta nie ma wartości analitycznej. [2]
„Trzy–cztery razy skuteczniejszy”	Poprawa w określonych warunkach jest wiarygodna. Stały mnożnik niezależny od pogody, obsługi i przeciwnika nie został wykazany. Wartości CSIS należy podawać jako raportowane szacunki. [2]
„10 tys. razy skuteczniejszy”	Wypowiedź założyciela firmy przytoczona przez NPR, bez zdefiniowanego miernika. [6]
„AI odporna na zagłuszanie”	Określona funkcja pokładowa może umożliwić kontynuację określonej fazy lotu po utracie określonego łącza. Twierdzenie, że drona nie da się zakłócić, wykracza poza dowody. [5][10]
„Rój”	Wiele dronów użytych naraz nie dowodzi kolektywnego podejmowania decyzji. Dzisiejsza technologia częściej odpowiada sterowaniu wieloma platformami przez jednego operatora. [7]
„Tani dron zniszczył drogi sprzęt”	Może być prawdziwym opisem pojedynczego zdarzenia, ale nie bilansem ekonomicznym zdolności. Trzeba doliczyć nieudane misje, rozpoznanie, ludzi, łączność, serwis i utrzymanie. [10]
„Raport think tanku dowodzi skuteczności”	Nie zawsze. Raport może prawidłowo przytoczyć niezweryfikowane twierdzenie rozmówcy. Trzeba sprawdzić, czy autor sam mierzył, czy zebrał relacje.

7 Tezy z panelu wobec dowodów

Zestawienie dotyczy tez wygłoszonych na panelu „SI na polu walki" (Dell Technologies, Łódź, 24.11.2026) i pokazuje, które mają oparcie w sprawdzonych źródłach. Atrybucję tez ustalono z transkryptu nagrania, który nie ma podziału na mówców.

Teza	Oparcie w źródłach	Ocena
Problemem są dane treningowe, a nie same modele	CSIS: standardy etykietowania, zbiór walidacyjny, dryf modelu po zmianie sensora. Ifri: AI jako akcelerator procesu. [2][10]	Poparte
Cel zatwierdza człowiek, autonomii wyboru celu nikt jeszcze nie oddał	Zgodne z Reuters i NPR dla opisanych ukraińskich przykładów. Wymaga zastrzeżenia o rosyjskim V2U (CSIS: prawdopodobnie w pełni autonomiczny) i raporcie Anthropic. [3][5][6][17]	Poparte z zastrzeżeniem
Operatorzy pierwszej linii nie rozumieją, jak działa AI	Brak badania w sprawdzonych źródłach.	Obserwacja własna
Na jedno trafienie przypada 15 lotów, które nie dolatują	Oznacza około 6% skuteczności, poniżej przedziałów podawanych przez CSIS (10–15% zwykłe FPV, 30–50% doświadczeni operatorzy). Źródła nie podają takiego wskaźnika. [2]	Niepotwierdzone Oznaczyć jako szacunek własny
Rosjanie zatruwają dane i modele	W sprawdzonych źródłach nie znaleziono potwierdzenia zatruwania modeli rosyjskimi danymi. Udokumentowano natomiast użycie komercyjnych modeli przez rosyjskich aktorów (raport Anthropic, wrzesień 2026). [17]	Niepotwierdzone w tej formie

7 Tezy z panelu wobec dowodów CD.

Teza	Oparcie w źródłach	Ocena
Analiza danych o serwisie toalet przenośnych: trzy tygodnie pracy analityka wobec 15 minut z AI	Brak niezależnego pomiaru w sprawdzonych źródłach. Przykład ilustruje skrócenie czasu analizy, nie jej trafność.	Anegdota, bez źródła
Dochodzimy do fizyki, której AI nie oszuka	Ifri: EW, światłowód, spadek skuteczności Excalibur z 70% do 6%. Reuters: zależność od warunków pola walki. [5][10]	Poparte
Polska sama nie zbuduje dużego modelu, Unia Europejska mogłaby	Ocena strategiczna, poza zakresem weryfikacji.	Opinia

Bilans ośmiu tez



Poparte 2 · Poparte z zastrzeżeniem 1 · Niepotwierdzone 2 · Obserwacja / anegdota / opinia 3

8 Rekomendacje dla Polski i NATO

Poniższe punkty są rekomendacjami analitycznymi wynikającymi z materiału, nie deklaracją, że istnieje jeden sprawdzony model do skopiowania.

1 **Najpierw dane i integracja.** Spójne oznaczanie i archiwizowanie danych, rejestrowanie również niepowodzeń, wspólne formaty wymiany, możliwość ustalenia pochodzenia wskazania, bezpieczne środowiska trenowania i walidacji oraz możliwość zmiany dostawcy bez utraty danych. Podstawa: doświadczenia Avengers i rozwój DELTA jako ekosystemu. [2][10]

2 **Zamawiać wyniki w zdefiniowanych warunkach, nie etykietę „AI".** Protokół odbioru powinien obejmować skuteczność wobec określonych klas obiektów, liczbę fałszywych alarmów, zachowanie przy braku pewności, obciążenie operatora, pracę przy degradacji łączności, wyniki w różnych porach roku i koszt utrzymania. To proponowane kryteria, uzasadnione dryfem danych i szybkim starzeniem się rozwiązań. [2][10]

3 **Opisywać autonomię funkcjami.** W wymaganiach i raportach rozdzielać nawigację, śledzenie celu, wybór celu i autoryzację użycia siły, zgodnie z podejściem MKCK, oraz wymagać możliwości interwencji i dezaktywacji. [11]

4 **Nie budować obrony przeciw dronom na jednym typie sensora.** Ifri opisuje ekosystem detekcji obejmujący akustykę, termikę, radar i fuzję danych oraz wskazuje, że wobec dronów światłowodowych i autonomicznych EW traci skuteczność, a wraca przechwytywanie fizyczne. Wyniki każdego detektora trzeba więc oceniać dla konkretnych klas zagrożeń. [10]

8 Rekomendacje dla Polski i NATO CD.

5 **Traktować modele ogólnego przeznaczenia jako ryzyko łańcucha dostaw i nadużyć.** Wyniki Vals pokazują, że zabezpieczenia dostawców nie gwarantują odmowy w zadaniach zbliżonych do celowania, więc procedury powinny zakładać weryfikację wyników i ograniczenie ich roli w łańcuchu decyzyjnym. [8][9]

6 **Nie kopiować statystyk w oderwaniu od warunków.** Przenośne są zasady: integracja, szybka informacja zwrotna, testy z przeciwnikiem adaptacyjnym, odporność organizacyjna i utrzymanie zdolności. Nieprzenośne bez dodatkowych badań są lokalne odsetki trafień, ekonomika odcinka frontu i założenia o obecności cywilów. [10]

7 **Skalować etapowo, bez jednej daty „gotowości".** Pilotaże funkcji analitycznych, walidacja z użytkownikami i rejestracja błędów, integracja z procedurami i szkoleniem, skalowanie po wykazaniu powtarzalnej korzyści, stała ponowna ocena po zmianach modeli i środowiska. To rekomendowana kolejność, nie prognoza kalendarzowa.



Rekomendowana kolejność wdrażania (punkt 7). Kolejność, nie kalendarz.

9 Dziesięć pytań bez rzetelnej odpowiedzi publicznej

1. Jaki odsetek misji dronowych po obu stronach rzeczywiście wykorzystuje ML, a nie tylko autopilota lub klasyczne śledzenie?
2. Jak zmienia się skuteczność tego samego zespołu i platformy po dodaniu AI w porównywalnych warunkach?
3. Jakie są pełne statystyki błędnych i pominiętych wskazań Avengers według sensorów, pogody i klas obiektów?
4. Ile misji z automatycznym naprowadzaniem kończy się wykonaniem zadania, a nie tylko kontaktem z obiektem?
5. Jak często po utracie łączności system zachowuje się inaczej, niż oczekiwał operator?
6. W jakiej części rosyjskich misji V2U cel wybiera system, a w jakiej został określony wcześniej?
7. Czy istnieje niezależnie zweryfikowany bilans szkód cywilnych wynikających z autonomicznego wyboru celu w tej wojnie?
8. Jaki jest rzeczywisty koszt skutecznie wykonanego zadania po uwzględnieniu prób, obsług, danych, szkolenia i utrzymania?
9. Ile deklarowanych oszczędności pracy operatorów pozostaje po doliczeniu nadzoru, kontroli jakości i ponownego trenowania?
10. Jak szybko przewaga danej wersji modelu zanika po zmianie taktyki i środków przeciwdziałania przeciwnika?

10 Zakres weryfikacji i ograniczenia

Sprawdzone w źródłach

MON (Avengers, DELTA), CSIS (marzec 2025, kwiecień 2026, opis czerwcowego), Reuters przez The Star, NPR przez KPBS, RUSI (rój), Vals AI i TechCrunch, Ifri (w streszczeniu fragmentów), MKCK, relacje o kontrakcie Auterion, relacje o Combined Resolve, strony Microsoft MTAC oraz relacje RUSI, Euronews i Defense One o raporcie Anthropic.

Nie zweryfikowano

Artykułu Modern War Institute (liczby 43% i 20–30%), raportu Microsoft Digital Defense Report 2025, artykułu Military Review o integracji broni autonomicznej oraz analiz RBC-Ukraine. Pełnego tekstu CSIS z czerwca 2026 r. nie udało się pobrać, więc jego tezy podano według opisu na stronie i omówienia Small Wars Journal.

Narzędzia AI i zastrzeżenie o dostawcy

Opracowanie przygotowano z pomocą narzędzi AI. Dwa źródła dotyczą modeli dostawcy jednego z tych narzędzi: badanie Vals AI i raport Anthropic z września 2026 r. Potraktowano je tak jak pozostałe i podano także wyniki niekorzystne dla tego dostawcy.

Pochodzenie liczb

Kilka opisów badania Vals pochodzi z relacji wtórnych (TechCrunch, opracowania w mediach). Tam, gdzie pierwotny tekst Vals podawał dane, użyto jego sformułowań. Liczby z Ifri podano według streszczenia fragmentów raportu.

Źródła

[1] Ministerstwo Obrony Ukrainy, komunikat o 12 000 celów wykrywanych tygodniowo, 23.09.2024.

[2] CSIS, „Ukraine's Future Vision and Current Capabilities for Waging AI-Enabled Autonomous Warfare", marzec 2025. https://www.csis.org/analysis/ukraines-future-vision-and-current-capabilities-waging-ai-enabled-autonomous-warfare

[3] CSIS, analiza rosyjskiego systemu V2U, kwiecień 2026.

[4] K. Bondar, M. Mande, CSIS, „Defining Autonomy: Why Software, Not Drones, Will Decide the Next War", czerwiec 2026 (według strony CSIS i omówienia Small Wars Journal z 16.06.2026). https://www.csis.org/analysis/defining-autonomy-why-software-not-drones-will-decide-next-war

[5] Reuters, „Ukrainian drone pilots look to AI for battlefield edge", 29.11.2025 (wersja The Star).

[6] NPR, relacja o dronach AI w wojnie w Ukrainie, 29.10.2026 (wersja KPBS).

[7] R. Tollast, RUSI, komentarz o rojach dronów, 16.07.2026.

[8] G. Jaff, A. Ozerov, Vals AI, „Frontier models have few guardrails around autonomous weapons", 17.11.2026. https://www.vals.ai/blogs/autonomous-warfare

[9] TechCrunch, relacja o raporcie Vals AI. https://techcrunch.com/2026/11/17/ai-models-can-be-tricked-into-identifying-civilians-as-military-targets-by-telling-them-its-a-game/

[10] Ifri, É. Tenenbaum i in., raport o MilTech w wojnie w Ukrainie, luty 2026. https://www.ifri.org/sites/default/files/2026-02/ifri_tenenbaum_et_al_miltech_war_ukraine_2026.pdf

[11] MKCK, „Autonomous Weapon Systems and International Humanitarian Law: Selected Issues", październik 2025. https://www.icrc.org/sites/default/files/media_file/2025-10/ICRC-Position_Paper-Autonomous_Weapon_Systems_and_IHL-Selected_issues_Oct2025.pdf

Źródła CD.

[12] Ministerstwo Obrony Ukrainy, komunikat o niezależnej ocenie cyberbezpieczeństwa DELTA, 09.03.2026.

[13] The Register, FT i DroneLife, relacje o dostawie 33 tys. zestawów Auterion, lipiec 2025.

[14] Jamestown Foundation, „Ukrainian Military Offers Lessons Learned to NATO, Part Three".
https://jamestown.org/ukrainian-military-offers-lessons-learned-to-nato-part-three/

[15] United24 Media, relacja o Combined Resolve 26-07 (za Defence Blog, 20.10.2026).
https://united24media.com/world/ukraines-drone-veterans-hit-a-us-tank-brigade-with-a-70-casualty-lesson-in-modern-warfare-23646

[16] Microsoft MTAC, 17.04.2024 oraz 23.10.2024.
https://blogs.microsoft.com/on-the-issues/2024/04/17/russia-us-election-interference-deepfakes-ai/

[17] RUSI, „From Human Proxies to Autonomous Adaptation"; Euronews, 16.09.2026; Defense One, wrzesień 2026 (o raporcie Anthropic).
https://www.rusi.org/explore-our-research/publications/commentary/human-proxies-autonomous-adaptation-next-phase-russias-hybrid-activity

[18] SAN, relacja o Combined Resolve (za Wall Street Journal).
https://san.com/cc/ukraines-drone-war-offers-hard-lesson-for-us-armory/
Stan na 25.11.2026: adres przekierowuje na stronę główną serwisu.

Numeracja źródeł w tym wydaniu jest ciągła (1–18); w wersji roboczej pozycje 14–18 miały numery 15–19. Pozycje bez adresu podano tak, jak w materiale źródłowym.

MATTHEW HALABA.

AI na polu walki w Ukrainie. Co potwierdzają jawne dane, a czego z nich nie da się wywnioskować. Raport analityczny, stan na 25.11.2026.

Matthew Halaba · halaba.online · matthew@halaba.online