Stowarzyszenie Producentów Technologii Podwójnego Zastosowania DUALTEC
Jasionka 954E, 36 – 002 Jasionka, Polska
Tel. :(0-48) 692 187 012, mail: stowarzyszenie@dualtec.com.pl
NIP: 5170449575, Regon: 529100746, KRS: 0001114630

Szczecin 12..08.2025 r.

INFORMACJA NA TEMAT ZAGROŻEŃ PŁYNĄCYCH Z UŻYTKOWANIA CHIŃSKICH DRONÓW

1. Zagrożenie wyciekiem informacji

Drony produkcji chińskiej, nawet w wersjach eksportowych, mogą przeskład dane telemetryczne, obrazy wideo, lokalizację GPS oraz inne informacje operacyjne do chmur danych lub serwerów producenta. Dotyczy to zarówno transmisji w czasie rzeczywistym, jak i danych przechowywanych tymczasowo w urządzeniu (np. ciche aplikacji mobilnej).

W warunkach operacyjnych może to skutkować nieautoryzowanym dostępem do:

- lokalizacji wojskowych/wrażliwych obiektów,
- tras patrolowych,
- informacji o rozmieszczeniu sił/patroli/pozycji własnych,
- sposobu prowadzenia operacji/działań.

Nawet jeśli dane nie są bezpośrednio przesyłane do serwerów zlokalizowanych w ChRL, producent może dysponować zdalnym dostępem do urządzenia poprzez aktualizacje oprogramowania lub komunikację zakodowaną w tle.

2. Zagrożenie utajnionym pozyskiwaniem danych przestrzennych (fotogrametria)

Wiele chińskich dronów jest wyposażonych w zaawansowane czujniki wizyjne służące do autonomicznego wykrywania przeszkód (np. systemy stereowizyjne, lidar, kamery ToF). Dane te, zebrane z wielu kierunków i w wysokiej rozdzielczości, mogą być wykorzystane do zbudowania trójwymiarowych modeli obiektów wrażliwych/wojskowych i np. infrastruktury krytycznej.

Dzięki nowoczesnym technikom rekonstrukcji 3D opartym na splatach gaussowskich (Gaussian Splatting), możliwe jest szybkie utworzenie bardzo precyzyjnych modeli 3D np. stanowisk dowodzenia, pojazdów, wyrzutni rakiet itp., bez konieczności planowego fotografowania danego obiektu. Dron zbiera te dane niejako „przy okazji", pod pozorem nawigacji lub unikania przeszkód.

Istnieje także zagrożenie nieautoryzowanego przesyłania plików w postaci obrazów twarzy czy sylwetek ludzkich, zarówno w postaci mini obrazów jak i (przy sprzyjających warunkach) pojedynczych zdjęd.

3. Potencjalne zastosowanie ukrytego mechanizmu „kill switch"

Sprzęt i oprogramowanie o zamkniętym kodzie, nad którym użytkownik nie ma pełnej kontroli, może zawierać mechanizmy umożliwiające producentowi (lub osobom trzecim) dezaktywację urządzenia w sposób zdalny – tzw. kill switch. Może on być aktywowany na żądanie lub po spełnieniu określonych warunków (np. wykrycie działania w niedozwolonym regionie, brak połączenia z serwerem producenta, zmiana daty systemowej itp.).

Konsekwencją może być utrata BSP podczas misji, utrudnienie ewakuacji sprzętu, a w skrajnych przypadkach – dezaktywacja całej floty dronów danego typu.

Jasionka 954E, 36 – 002 Jasionka, Polska
Tel. :(0-48) 692 187 012, mail: stowarzyszenie@dualtec.com.pl
NIP: 5170449575, Regon: 529100746, KRS: 0001114630

4. Brak kompatybilności z zachodnimi i krajowymi systemami zarządzania lotem

Chińskie drony bardzo często wykorzystują zamknięte, autorskie rozwiązania do zarządzania lotem i konfiguracji misji. Interfejsy te są całkowicie odmienne od powszechnie używanych w NATO i krajowych systemów, takich jak QGroundControl, Mission Planner czy MAVProxy. Brak standaryzacji uniemożliwia:

- integrację z innymi systemami C4ISR,
- szybkie szkolenie operatorów,
- adaptację narzędzi do specyfiki misji wojskowych,
- przeprowadzenie zautomatyzowanych testów zgodności lub interoperacyjności.

5. Brak wartości szkoleniowej w kontekście wdrażania dronów polskiej produkcji

Z uwagi na zamkniętą architekturę oprogramowania i sprzętu, obsługa chińskich dronów znacząco różni się od operowania systemami wykorzystywanymi w krajowych lub sojuszniczych rozwiązaniach. Interfejsy użytkownika, logika działania, struktura menu, sposób definiowania misji oraz filozofia konfiguracji parametrów lotu są całkowicie odmienne.

W związku z tym:

- szkolenie operatorów wojskowych na dronach chińskich nie przekłada się na umiejętności
- przydatne przy obsłudze dronów polskiej/europejskiej produkcji, nie buduje to kompetencji w zakresie stosowania standardów NATO (np. MAVLink, otwarte interfejsy GCS),
- w praktyce prowadzi do powstania równoległego i niekompatybilnego toru szkoleniowego, który w żaden sposób nie wspiera rozwoju krajowych zdolności technologicznych ani operacyjnych.

6. Zamknięty charakter oprogramowania i sprzętu

Drony produkcji chińskiej są w większości przypadków urządzeniami o zamkniętej architekturze – zarówno sprzętowo, jak i programowo. Oznacza to, że użytkownik nie ma możliwości:

- wgrania własnego oprogramowania autopilota,
- zmodyfikowania firmware'u pod kątem wymogów wojskowych (np. szyfrowanie transmisji, ograniczenia przestrzenne),
- dostosowania algorytmów autonomicznego lotu do charakterystyki danego środowiska (np. operacje w obszarze zurbanizowanym lub leśnym),
- wymiany podzespołów bez ryzyka utraty gwarancji lub sprawności urządzenia.

W kontekście wymagań operacyjnych Sił Zbrojnych RP, czy innych służb, ogranicza to możliwość wdrażania krajowych technologii, modernizacji sprzętu oraz rozwijania własnych kompetencji w zakresie BSP.

Podsumowanie

Z punktu widzenia bezpieczeństwa narodowego, suwerenności technologicznej oraz interoperacyjności z sojusznikami, wykorzystanie chińskich dronów w siłach zbrojnych oraz służbach niesie ze sobą szereg istotnych zagrożeń. Rekomenduje się ostrożność w zakresie ich wdrażania do struktur operacyjnych oraz dążenie do rozwijania i stosowania rozwiązań krajowych lub sojuszniczych, opartych na otwartych standardach i umożliwiających pełną kontrolę nad oprogramowaniem oraz przepływem danych.

Opracował dla Klastra Dualtec: Paweł Śmiałek