



Droni navali britannici inviavano dati in Cina: il caso che coinvolge Royal Navy e forze speciali SBS

Pubblicato il 11/08/2026

Una vulnerabilità scoperta a bordo di alcuni dei più moderni mezzi navali senza equipaggio britannici riporta al centro dell'attenzione un problema sempre più importante per le Forze Armate occidentali: la sicurezza della catena di approvvigionamento dei sistemi autonomi.

Secondo quanto rivelato il 9 agosto dal [*Telegraph*](#), le telecamere installate sui **K3 Scout**, imbarcazioni veloci senza equipaggio utilizzate dalla Royal Navy e dai Royal Marines, stabilivano autonomamente comunicazioni con un **indirizzo IP situato in Cina**.

La scoperta è avvenuta durante una normale attività di verifica delle vulnerabilità informatiche condotta dal Ministero della Difesa britannico.

Il problema non riguardava direttamente il sistema di navigazione o di controllo del K3 Scout, ma alcune telecamere acquistate dal costruttore britannico Kraken Technology Group attraverso

un fornitore terzo. All'interno dei dispositivi erano presenti componenti di origine cinese.

Una volta rilevato il collegamento verso la Cina, il Ministero della Difesa ha disposto la rimozione della connettività Internet dalle telecamere interessate.

Cosa veniva realmente trasmesso

È questo l'aspetto sul quale occorre distinguere tra il titolo particolarmente forte dell'inchiesta britannica e quanto finora accertato.

Le comunicazioni rilevate vengono descritte come **“heartbeat communications”**, piccoli messaggi automatici attraverso i quali un dispositivo connesso segnala a un server di essere acceso, raggiungibile e correttamente funzionante.

Non è quindi stato dimostrato che le telecamere abbiano trasmesso in Cina immagini, filmati, coordinate, dati tattici o informazioni riguardanti operazioni militari.

Il Ministero della Difesa britannico ha affermato che l'indagine condotta dopo la scoperta non ha trovato prove che dati o sistemi del MoD siano stati consultati, compromessi o trasmessi all'esterno.

La vicenda rimane tuttavia particolarmente delicata proprio per la natura delle piattaforme coinvolte e per gli ambienti nei quali sarebbero state utilizzate.

I K3 Scout e le forze speciali britanniche

Secondo il *Telegraph*, i K3 Scout erano stati impiegati anche nell'ambito di attività riconducibili alle **forze speciali britanniche**, compreso lo **Special Boat Service**, l'unità delle UK Special Forces specializzata nelle operazioni marittime.

Il quotidiano britannico riferisce inoltre che alcune delle imbarcazioni erano state predisposte in vista di possibili missioni nel Golfo.

Questo elemento rende il problema della sicurezza delle telecamere particolarmente significativo: anche una periferica apparentemente secondaria, se collegata a una rete e installata su una piattaforma impiegata in contesti sensibili, può trasformarsi in un potenziale punto di accesso o di raccolta delle informazioni.

Secondo quanto riportato dalla stampa britannica, sui dispositivi sarebbero inoltre state registrate attività connesse alla preparazione di operazioni nel Golfo. Anche in questo caso, tuttavia, **non vi sono prove pubbliche che tali registrazioni siano state effettivamente trasferite verso la Cina.**

Project Beehive: 20 mezzi per 12,3 milioni di sterline

La presenza dei K3 Scout nella Royal Navy non è marginale.

L'11 marzo 2026 la Royal Navy ha annunciato ufficialmente l'acquisto di **20 imbarcazioni senza equipaggio prodotte da Kraken Technology Group**, nell'ambito di un contratto del valore di **12,3 milioni di sterline.**

Il programma prende il nome di **Project Beehive** e rappresenta uno degli elementi della trasformazione della Royal Navy verso quella che Londra definisce una **Hybrid Navy**, nella quale unità tradizionali con equipaggio dovranno operare insieme a sistemi autonomi e senza equipaggio.

Secondo la Royal Navy, i 20 mezzi sono destinati al **Coastal Forces Squadron** e al **47 Commando Royal Marines** per attività operative, addestrative e di sperimentazione.

Il K3 Scout è stato concepito inoltre con un'architettura aperta, proprio per consentire la rapida integrazione di nuovi sensori e capacità.

Una caratteristica che offre una notevole flessibilità operativa, ma che rende ancora più importante conoscere esattamente provenienza, software e comportamento di ogni componente integrato nella piattaforma.

Sorveglianza, protezione delle forze e attacchi di precisione

Le potenzialità del K3 Scout vanno ben oltre quelle di un semplice motoscafo radiocomandato.

La stessa Royal Navy indica tra i possibili impieghi della piattaforma la **sorveglianza**, la **protezione delle forze** e persino gli **attacchi di precisione.**

Nel luglio scorso un K3 Scout configurato secondo le specifiche del Project Beehive è stato protagonista di un'importante sperimentazione: il mezzo è stato aviolanciato per quattro volte da un **A400M**, da una quota di circa 1.300 piedi, sopra il Mare del Nord.

La prova aveva l'obiettivo di dimostrare la possibilità di proiettare rapidamente un sistema navale senza equipaggio in un'area operativa senza dipendere dalla presenza di una nave madre o di un porto nelle vicinanze.

Per la Royal Navy questa capacità potrebbe consentire, in futuro, di trasportare rapidamente i K3 Scout anche in acque contestate o difficilmente accessibili.

È proprio la crescente importanza operativa di queste piattaforme a rendere il caso delle telecamere particolarmente significativo.

Il vero problema è la supply chain

La vicenda britannica evidenzia infatti una vulnerabilità che riguarda ormai l'intero settore dei sistemi senza equipaggio.

Un drone può essere progettato e assemblato nel Regno Unito, negli Stati Uniti o in un altro Paese NATO, ma contenere al proprio interno **telecamere, circuiti elettronici, antenne, motori, batterie e altri componenti provenienti da catene di fornitura internazionali**.

Il rischio non consiste necessariamente nella presenza intenzionale di uno strumento di spionaggio.

Un componente commerciale può semplicemente essere progettato per comunicare automaticamente con server del produttore per aggiornamenti, diagnostica, telemetria o gestione remota.

Un comportamento perfettamente normale in un prodotto civile può però diventare inaccettabile quando lo stesso componente viene installato su un sistema militare impiegato per sorveglianza, intelligence o operazioni speciali.

Ed è probabilmente questa la lezione più importante del caso K3 Scout.

Nessuna prova di spionaggio, ma un campanello d'allarme

Parlare oggi di “droni britannici che inviavano segreti militari alla Cina” sarebbe quindi eccessivo rispetto alle informazioni disponibili.

Ciò che risulta è che **telecamere installate sulle piattaforme comunicavano autonomamente con un indirizzo IP cinese** e che il Ministero della Difesa, una volta individuato il comportamento, ne ha eliminato la connettività.

Il MoD sostiene che non esistano prove della compromissione o della trasmissione di proprie informazioni.

Resta tuttavia un interrogativo difficilmente ignorabile: **come è stato possibile che componenti installati su mezzi destinati anche a impieghi operativi e utilizzati in ambienti estremamente sensibili conservassero la capacità di comunicare con infrastrutture informatiche esterne?**

In un'epoca nella quale droni e sistemi autonomi stanno diventando nodi permanenti delle reti militari, la sicurezza non può più riguardare soltanto la piattaforma nel suo complesso.

Dovrà arrivare fino all'ultima telecamera, all'ultimo chip e all'ultima riga di software.

Link notizia: <https://www.telegraph.co.uk/news/2026/08/09/spy-cameras-on-navy-drones-secretly-sent-data-to-china/>