

ISS GLOBAL / STRATEGIC ASSESSMENT



UAS, autonomy & allied interoperability

A twelve-month synopsis against the UK–US AI and Autonomy partnership

REVIEW PERIOD

26 September 2025 – 25 September 2026

ASSESSMENT DATE

26 September 2026

The emerging requirement is not merely for more autonomy, but for demonstrably controlled cooperation between autonomous functions, people and organisations.

Principal assessment

The partnership is a material signal, but its significance is broader than the torpedo demonstration. The evidence reviewed shows a shift towards connecting uncrewed platforms, sensors, AI models and human decision-makers into coordinated mission systems. Operational drone use is already extensive; the maturity of autonomous decision-making, multinational integration and assurance remains uneven. ^{[1],[6],[9],[11]}

For ISS Global, this supports strengthening **WS01 validation and WS03 assurance**, and testing the governed control-plane positioning. It does not, by itself, justify a separate roadmap item or claims that Dfuze is an autonomous mission-control system.

SCOPE DISTINCTION

UAS are aerial systems. Excalibur is an uncrewed underwater vehicle (UUV). The connection is cross-domain autonomy and governance, not identical operating requirements.

02 / The signal

04–06 / Operational synthesis

08–09 / Workstream implications

03 / Twelve-month progression

07 / Harm, confidence & limits

10–11 / Source register

What the partnership establishes

The UK announcement of 22 September 2026 describes the launch of work between the MOD’s Rapid AI Delivery Taskforce and the US Chief Digital and Artificial Intelligence Office. Its stated objectives connect AI and autonomy with critical-infrastructure protection, deterrence and trusted interoperability. It is strong evidence of official programme direction, but does not publish a detailed delivery schedule, assurance specification or procurement opportunity. ^[1]

A tangible integration milestone

The associated Excalibur demonstration provides a more tangible integration milestone. The US Navy’s public account specifies 13 September 2026, at the British Underwater Test & Evaluation Centre in Scotland, and identifies an exercise Mk 48 torpedo. The Navy’s Rapid Capabilities Office describes integrating management and command-and-control functions across systems not originally designed to work together. ^[2]

This is evidence of a particular allied platform–payload integration, not proof of autonomous target selection or weapon-release authority.

CHRONOLOGY AND TERMINOLOGY

The UK announcement uses “last week”; the US account supplies 13 September. The explicit date is preferable in a chronology. “Live firing” should not be expanded into an unsupported claim that a live warhead was used. ^{[1],[2]}

Evidence boundaries

SUPPORTED BY THE PUBLIC RECORD	NOT ESTABLISHED
Official bilateral programme direction	A detailed jointly approved assurance specification
A reported allied platform–payload trial	Autonomous selection and engagement of a target
Critical-infrastructure and deterrence objectives	Operational fleet readiness or universal compatibility
A material validation context	A procurement requirement or accreditation for Dfuze

ISS GLOBAL ASSESSMENT

Allied autonomy is increasingly an integration and assurance problem, not simply a platform-development problem. This is an analytical conclusion, not a published requirement for any particular commercial product.

This synopsis is selective: it examines defence and security developments most relevant to the signal. It is not a comprehensive global census of UAS operations.

02 / REPORTING CHRONOLOGY

The twelve-month progression

Dates below are publication dates unless otherwise stated. Each milestone is labelled by maturity to prevent trials, operational claims and programme intentions being conflated.

17 OCT 2025	Digital foundations under stress Trident Sprint tested uncrewed systems, surveillance-data exchange and communications in disrupted, intermittent and low-bandwidth conditions. Demonstration: digital integration and degraded connectivity were explicit requirements. ^[3]
DEC 2025 – JAN 2026	Proteus progresses to flight Ground-running trials preceded a first flight announced on 16 January. Aerial demonstrator: autonomous flight controls operated under continuous test-pilot supervision; future maritime missions were not operationally validated. ^{[4],[5]}
12 FEB 2026	Architecture and multinational adoption The US Air Force described a government-owned autonomy architecture across multiple aircraft and suppliers. Eight NATO allies separately agreed to accelerate maritime capability acquisition and integration. Testing and programme commitments. ^{[6],[7]}
APRIL 2026	Protective and combat applications Dstl reported AI-assisted explosive-hazard trials. Ukraine described organised Drone Line employment and procurement of 8,000 Octopus interceptors. Controlled trial; reported operational use; procurement. ^{[8],[9],[10]}
SEPTEMBER 2026	Coalition mission coordination NATO reported Task Force X-Arctic experimentation at REPMUS, connecting systems through shared information and tasking under human command. Coalition experimentation. ^[11]
22–25 SEP 2026	Partnership and data development The UK announced the US partnership, followed by a competition to exploit Ukrainian battlefield data for AI-enabled drone development. Programme and competition announcements, not fielded swarms. ^{[1],[12]}

From sorties to mission systems

A / Sustained, organised battlefield functions

Ukraine’s April account of Drone Line describes a unified approach combining reconnaissance, strike systems, analytics, training and centrally supported units. It reports more than 1,000 participating crews. The important organisational development is sustained integration of unmanned systems into the force, rather than isolated use by individual operators. Its battlefield-effectiveness claims remain Ukrainian MOD claims, not independently audited results. ^[9]

Assessment: the relevant unit of analysis is increasingly the mission and its information chain, not the aircraft alone. An alert, a classified object, an approved action and a confirmed result are different records, not interchangeable descriptions of one event.

Sensor observation	Software inference	Corroboration
Human review	Authorised action	Outcome evidence

For Dfuze, that distinction is the strongest connection to an intelligence-integrity role. A useful record preserves what was observed, inferred, corroborated, accepted or rejected, authorised and subsequently established.

B / Resilience does not necessarily mean autonomy

The Ukrainian MOD’s February authorisation of an upgraded Baton Optik system identifies fibre-optic control and video transmission. This illustrates an alternative to radio-dependent control. It does not establish AI decision-making: changing the communications medium is different from delegating decisions to software. ^[13]

Proteus illustrates another distinction. Its first flight involved independently operated flight controls, but within a short test routine and under continuous supervision. That supports bounded flight autonomy, not an unrestricted ability to conduct every intended mission. ^[5]

VALIDATION CONSEQUENCE

Avoid a single “autonomous/not autonomous” field. Record which function is automated, its permitted operating limits, the supervising authority and the response to loss of communications.

Bounded functions, protective uses

FUNCTION	QUESTION TO ESTABLISH
Navigation	Who or what determines movement within the permitted operating area?
Detection / classification	Is the label machine-generated, human-confirmed or independently corroborated?
Mission adaptation	Can the system change tasks, and within what limits?
Action authority	Which decisions remain reserved to an authorised person?
Communications loss	What remains permitted, and when does authority expire?

C / Counter-UAS includes drone-on-drone interception

Ukraine’s April Octopus announcement describes an interceptor with automatic terminal guidance, intended to counter Shahed-type attack drones. It reports licensing and production arrangements involving Ukrainian manufacturers and the UK government. The source states that the system has been effective in combat, but provides no independently auditable performance dataset. ^[10]

Assessment: counter-UAS comprises separate judgments: detection, identification, tracking, authorisation, response and outcome assessment. A disappearing track is not necessarily a confirmed interception; detector confidence is not equivalent to confidence in identity or responsibility. WS01 should test missed threats and erroneous escalation, not only successful detections.

D / Protective and investigative uses

Dstl’s trial with 33 Engineer Regiment used small-UAS sensor data and AI to help operators locate and identify replica mines and ordnance. It demonstrated model retraining against new threat types and environments. Successful detection of prepared replicas does not establish reliable clearance of an operational site. ^[8]

DFUZE RELEVANCE

Suspected object → supporting imagery → assessed identification → qualified human review → recorded disposition. An AI label must remain linked to imagery, model version and review history; it must not silently become a confirmed device identification or declaration that an area is safe.

05 / OPERATIONAL SYNTHESIS

Software, coalition systems & data

E / Value increasingly lies in integration

The US Collaborative Combat Aircraft programme's February announcement describes government-owned architecture intended to allow mission-autonomy software from different suppliers to operate across different aircraft. It evidences deliberate modularity and reduced dependence on one platform–software combination, not effortless integration or automatic satisfaction of coalition requirements. ^[6]

Assessment: interoperability requires three distinct tests: *technical* exchange and interpretation; *operational* understanding of tasks and constraints; and *authority* to see, use or act on information. Receiving allied data does not automatically permit redistribution, model training or action.

F / Infrastructure protection is cross-domain

NATO's Baltic announcement links multinational maritime capabilities to undersea infrastructure security. It follows deployment and testing of 70 air and maritime drones during March–October 2025. That period only partly overlaps this review and is not a twelve-month total. ^[7]

Task Force X-Arctic's September account describes a shared data layer, digital command architecture and automated tasking under human command. NATO reports nearly 300 connected capabilities, not necessarily 300 drones. Further remote-infrastructure experiments and later demonstrations remained planned. ^[11]

Assessment: an undersea scenario should test cross-domain, multinational evidence exchange without losing provenance, restrictions, uncertainty or command responsibility—not merely replace an aircraft icon with a submarine.

G / Operational data becomes part of capability

The UK's 25 September announcement proposes initial access for up to 12 companies to Ukrainian daylight and thermal UAS imagery, including sensor information from over six million object detections. The competition covers recognition, distributed decisions, adaptive missions and collaborative sensing, including constrained communications. These are development objectives, not deployed British swarms. ^[12]

Assessment: governance must cover training-data origin, verified or disputed labels, reuse permissions, model versions and later corrections. Six million detections are not six million verified targets, engagements or independent training examples.

06 / EVIDENCE ASSESSMENT

Harm, confidence & remaining gaps

More sensing does not guarantee safer decisions

UN human-rights monitors recorded 66 civilians killed and 369 injured by short-range drones in Ukraine in March 2026. Combined casualties were 70% above March 2025. This is independent evidence of increased harm in that comparison, not evidence that attacks were autonomous. ^[14]

In September, the monitoring mission documented increased attacks on commercial infrastructure and specific drone strikes affecting shopping centres. It also recorded Ukrainian attacks against Russian commercial and refinery facilities, while explaining limitations in verifying casualties inside Russia. ^[15]

Reuters' September account of the UN Sudan fact-finding mission describes drone warfare extending attacks beyond immediate front lines and damaging civilian services. This corroborates reporting of UN findings; it is not a technical determination of autonomy in individual attacks. ^[16]

ISS GLOBAL ASSESSMENT

"Trusted" cannot mean simply accurate object recognition or successful mission completion. Validation must examine uncertainty, inappropriate recommendations, operator workload, rejected actions and evidence preservation for investigation of failures.

Confidence judgments

High confidence: official announcements establish substantial allied interest in autonomous systems, modular integration, battlefield data and cross-domain infrastructure protection.

Moderate confidence: these developments indicate growing requirements for provenance, bounded authority and auditable integration. That is an analytical inference, not a published common procurement specification.

Not established by this review

- The share of global UAS missions conducted autonomously during the review period.
- Comparable, independently verified performance across the cited systems.
- Autonomous lethal decision-making in the Excalibur trial.
- A fully operational UK–US joint autonomy architecture.
- A partnership requirement, accreditation or opportunity specifically for Dfuze.

Some US military pages blocked direct retrieval; indexed official publications and official organisational posts were used, with limitations recorded. NATO's September article has a publication/end-date inconsistency, so it is treated as September reporting.

Autonomous mission evidence

STATUS

The following are proposed validation requirements—not claims about current Dfuze functionality or published requirements of the partnership.

Add one bounded allied undersea infrastructure-protection scenario, using synthetic or appropriately releasable material. Combine a UK-origin undersea observation, an aerial observation and an allied analytical contribution. A human reviewer assesses whether the evidence warrants further investigation. There is no need to simulate weapon control.

Five deliberate complications

- 1. **Conflicting classifications.** Different sources assess the same object differently; retain both assessments and their evidential basis.
- 2. **Delayed information.** Uncertain timestamps and late arrivals must remain visible rather than being silently normalised.
- 3. **Connectivity loss.** Interrupt the review and preserve the decision state and applicable restrictions.
- 4. **Changed permissions.** Alter the receiving organisation’s access rights and test the agreed enforcement behaviour.
- 5. **Model update.** Introduce a version that changes an earlier classification without overwriting the original assessment.

Acceptance criteria

The record must distinguish observation from inference; preserve original evidence; identify relevant model and policy versions; record human decisions and overrides; and export a reconstructable account without presenting missing information as certainty.

EVIDENCE STATE	REQUIRED DISTINCTION
Observed	Original sensor contribution and acquisition context
Inferred	Derived interpretation, model version and uncertainty
Reviewed	Human acceptance, rejection or request for corroboration
Authorised	Named authority and permitted scope
Established afterwards	Outcome evidence, corrections and unresolved gaps

These tests strengthen the existing Autonomous Mission Evidence workstream. They do not imply a new platform-control capability or separate roadmap commitment.

Make trusted interoperability testable

CONTROL AREA	EVIDENCE TO REQUIRE
Human and machine identity	Attribution of each contribution, recommendation and authorised action
National disclosure restrictions	Enforcement of releasability and purpose limits
Evidence provenance	Links between original material, transformations and derived assessments
Model / configuration integrity	Identifiable versions, approved changes and rollback records
Human authority	Boundaries between viewing, recommending and executing
Disconnected operation	Cached permissions, expiry behaviour and reconciliation on reconnection
Audit and investigation	Protected records sufficient to reconstruct material decisions
Sovereign deployment	Actual hosting, administrative access, key control and external dependencies

Interoperability does not require unrestricted data sharing. Sovereignty is not established solely by server location. A disconnected system cannot receive immediate remote revocation: agree an expiry or bounded-authority mechanism rather than claiming instantaneous enforcement.

Governed control-plane positioning

PROPOSED POSITIONING

Dfuze should be evaluated as an evidence and assurance layer around specialist human–machine workflows, preserving provenance, permissions, human authority and reconstructable decisions across organisational boundaries.

This is narrower and more credible than claiming to coordinate autonomous weapons or provide universal military interoperability. Test it through demonstrable customer questions: can an analyst distinguish inference from verified evidence; can disclosure limits survive an exchange; and can an investigator reconstruct which information and model informed a decision?

Decision

Keep this inside WS01, WS03 and existing positioning work. No separate roadmap item is warranted. Prove that evidence, restrictions and responsibility remain intelligible when systems connect, models change, communications fail and allies exchange information.

REFERENCE REGISTER

Sources 01–08

Numbered citations link to these records; titles link to the original publications. Sources accessed 26 September 2026. Multiple official reposts are not independent corroboration.

-
- 01 **UK–US AI and Autonomy partnership announcement**
UK Prime Minister's Office · 22 Sep 2026
Primary announcement; full text reviewed. Programme intent and UK account of trial, not an assurance specification.
-
- 02 **Excalibur / Project Broadsword public account**
US Navy Rapid Capabilities Office / Chief of Naval Operations · September 2026; event 13 Sep
Official organisational post and embedded CNO account retrieved through search. Navy website article blocked direct access; not an independent trial evaluation.
-
- 03 **Technology demonstration boosts information warfare abilities**
Royal Navy · 17 Oct 2025
Primary exercise account; full text reviewed. Demonstration, not fleet-wide operational validation.
-
- 04 **Crewless helicopter one step from maiden flight**
Royal Navy · 2 Dec 2025
Primary report retrieved through indexed text. Ground-running milestone; intended missions distinguished from demonstrated capability.
-
- 05 **Autonomous helicopter makes first flight**
Royal Navy · 16 Jan 2026
Primary account; full text reviewed. Short supervised test routine.
-
- 06 **Open architecture and Collaborative Combat Aircraft ecosystem**
US Air Force Public Affairs · 12 Feb 2026
Official publication retrieved through indexed text; direct page returned HTTP 403. Reposts on USAF sites are one source family.
-
- 07 **Allies expedite innovation adoption for Baltic Sea security**
NATO · 12 Feb 2026
Primary programme announcement; full text reviewed. Historical March–October 2025 activity only partly overlaps review window.
-
- 08 **Drones using AI to spot explosive dangers**
Dstl / UK MOD · 2 Apr 2026
Primary trial account; full text reviewed. Replica hazards in a controlled trial, not operational clearance certification.
-

REFERENCE REGISTER

Sources 09–16

Numbered citations link to these records; titles link to the original publications. Sources accessed 26 September 2026. Multiple official reposts are not independent corroboration.

09	Drone Line: implementing a new warfare doctrine Ukrainian MOD · 9 Apr 2026 Primary belligerent-government account; full text reviewed. Reported scale and effectiveness are not independently audited.
10	Procurement of 8,000 Octopus interceptors Ukrainian MOD · 30 Apr 2026 Primary procurement and performance claims; full text reviewed. Procurement is not a confirmed delivery or interception total.
11	Task Force X-Arctic at REPMUS 2026 NATO Allied Command Transformation · 24 Sep 2026 page date Primary experimentation account; full text reviewed. Page dated 24 September describes exercise ending 25 September: treated as September reporting, not exact daily chronology.
12	British companies to access Ukrainian data for AI drone swarms UK MOD · 25 Sep 2026 Primary competition announcement; full text reviewed. Objectives and future access do not establish fielded capability.
13	Baton Optik fibre-optic-controlled UAS authorisation Ukrainian MOD · 5 Feb 2026 Primary belligerent-government account; full text reviewed. No independent acceptance of absolute electronic-warfare protection claims.
14	Short-range drones and civilian casualties in March UN Human Rights Monitoring Mission in Ukraine · 10 Apr 2026 Independent monitoring; full text reviewed. Verified minimums and monthly comparison, not a global or rolling-year total.
15	Attacks against retail, food and logistics companies UN Human Rights Monitoring Mission in Ukraine · 17 Sep 2026 Independent monitoring; full text reviewed. Explains verification limits for casualties inside the Russian Federation.
16	Foreign support and drones fuel Sudan war: UN probe Reuters · 3 Sep 2026 Retrieved reporting of UN findings, not a directly examined UN report or technical autonomy assessment. One secondary source family.

Production note. Self-contained HTML; A4 portrait; 12 mm content boundaries; original 30 mm coin; full-page ivory wash; embedded Nimbus Roman / Nimbus Sans fallback typography. The saved catalogue font package was unavailable during this export. This strategic synopsis retains the preceding analysis; no new incident investigation or email dispatch is implied.