

Resilience-First Secure Communications for Maritime Critical Infrastructure

Early QuStream/DQSP Field-Trial Results for Multi-Domain Operations in Contested Environments

Adrian Neal *MSc. Soft. Eng. (Oxon)*

Chief Scientist at Oxford Scientific

Chief Technical Officer at Delatr Technologies

Chief Executive Officer at QuStream

Senior Director & Global Lead for Post-Quantum Cryptography at Capgemini

Two-time Winner of the NATO NCIA Defence Innovation Challenge



Introduction - Who We Are



Created & Published QuStream Encryption Protocol having Information Theoretic Security



Commercialised QuStream for high-value and Post-Quantum long-life information assets



Partnered to develop EW resilient **QuStream** in hardware as **DQSP** – Delatr-QuStream-Protocol



Established JV to build **QuStream/DQSP** to NATO standards for field deployment



Introduction - What is QuStream/DQSP



Published and Presented in
November 2025 at FTC
Munich, Germany

QuStream — A secure-communications method in which both endpoints independently derive a continuous stream of fresh, cryptographically independent keys from a single pre-distributed seed, without key servers, certificate authorities, or live key-exchange infrastructure.

DQSP — QuStream hardened for electronic warfare: each packet is independently keyed and authenticated, forged traffic is rejected at negligible cost, and no handshake or session state exists for an adversary to attack — sustaining usable throughput under jamming conditions in which conventional schemes degrade sharply or fail to establish.



The Current Situation

- ⚠ Communications in contested domains are problematic
- ⚠ Encryption algorithms were never designed for EW
- ⚠ New post-quantum algorithms only make things worse
- ⚠ AI is making EW much more adaptive and effective

Communications Security Decides Military Outcomes



Encryption wasn't designed to withstand EW

AES	Key distribution	Static keys	Fleet-wide exposure
RSA	Quantum-broken	PKI-dependent	Heavyweight
ECDH	Quantum-broken	Handshake-fragile	Jamming-vulnerable
ML-KEM	Bandwidth-heavy	Handshake-fragile	Large overhead
DQSP	No handshake	Per-message keys	Tiny overhead



What we did – Field-Trials + AI Simulation

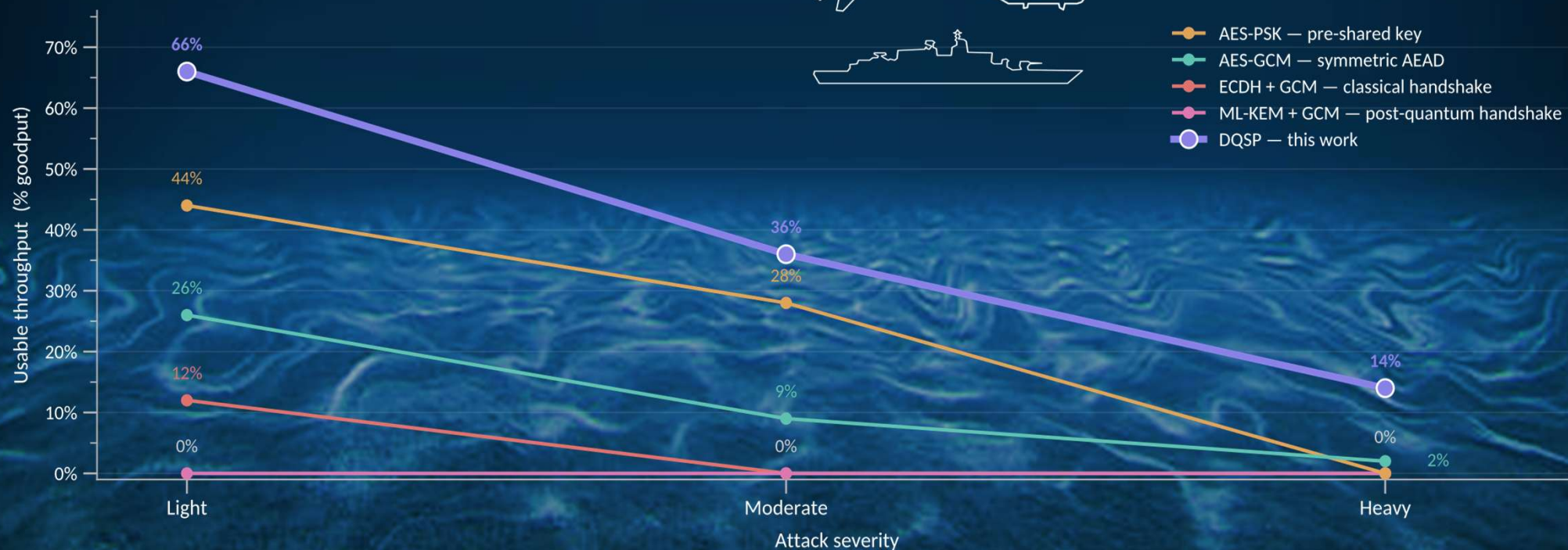
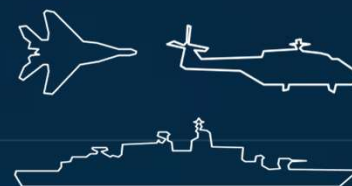
LLM-orchestrated multi-agent red team — a reasoning commander directing jammers, adapting strategy across episodes

- **Three threat tiers, scaled in difficulty** — wideband barrage jamming, reactive/follower jammers, and an adaptive AI adversary.
- **An adaptive, reasoning adversary** — built to observe the link's externally visible behaviour (timing, bandwidth, packet size) and re-tune its strategy across episodes.
- **Identical conditions for every scheme** — DQSP and all conventional baselines faced the same adversary, channel, and power budget.
- **Attacks on structure, not just signal** — the adversary chose where, when, and how to disrupt (jamming, forgery injection, timing against key events), testing each scheme precisely where it is weakest.



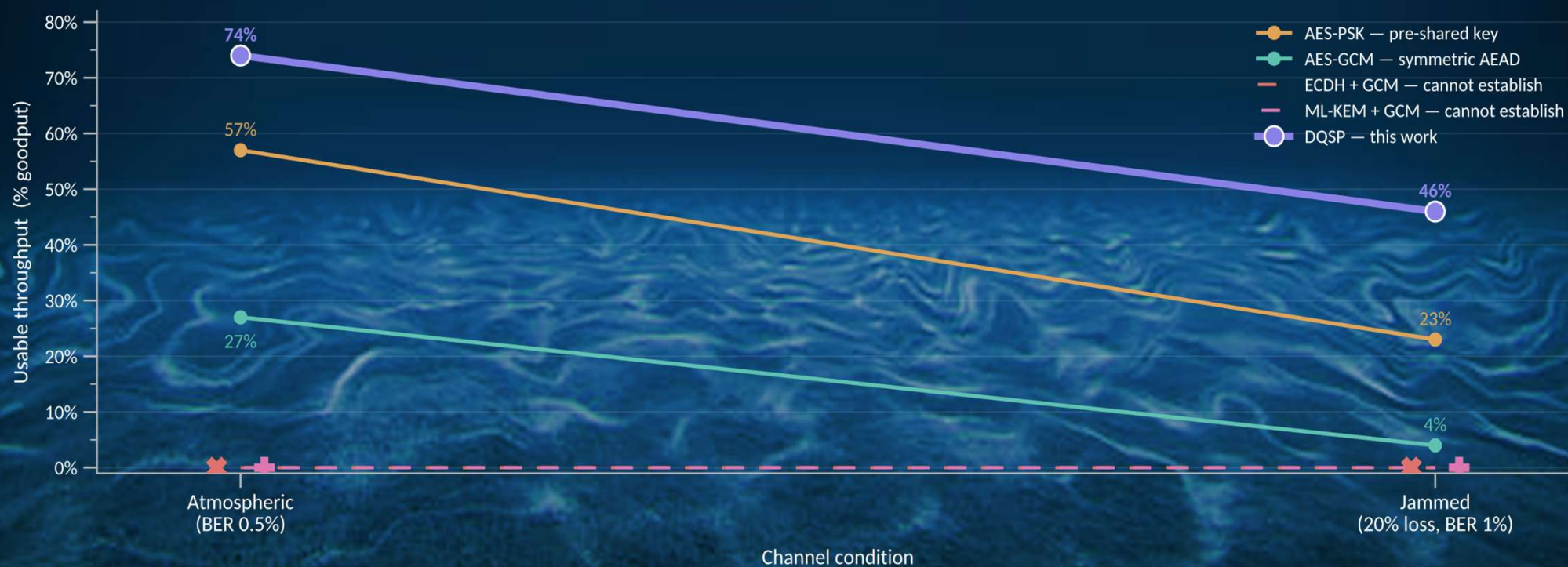
EW LLM-Orchestrated Multi-Agent Red Team

Surface RF — Graceful Degradation Under Mixed Attack



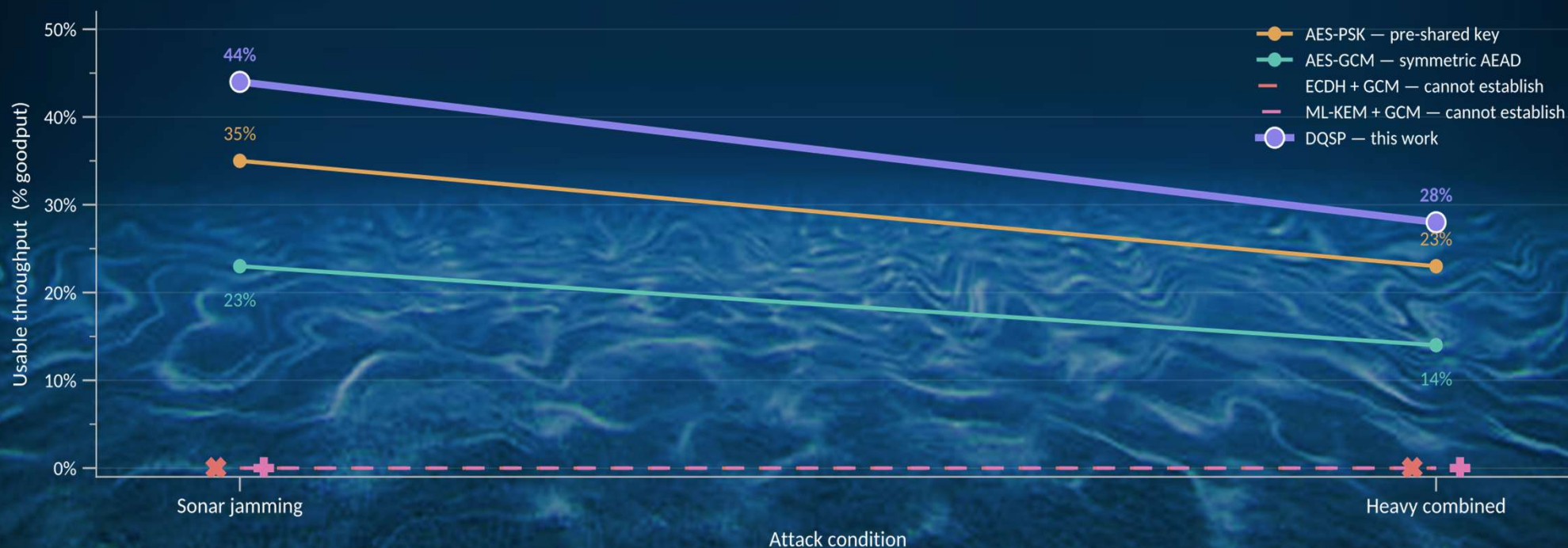
EW LLM-Orchestrated Multi-Agent Red Team

Submarine VLF — Robustness Under Jamming



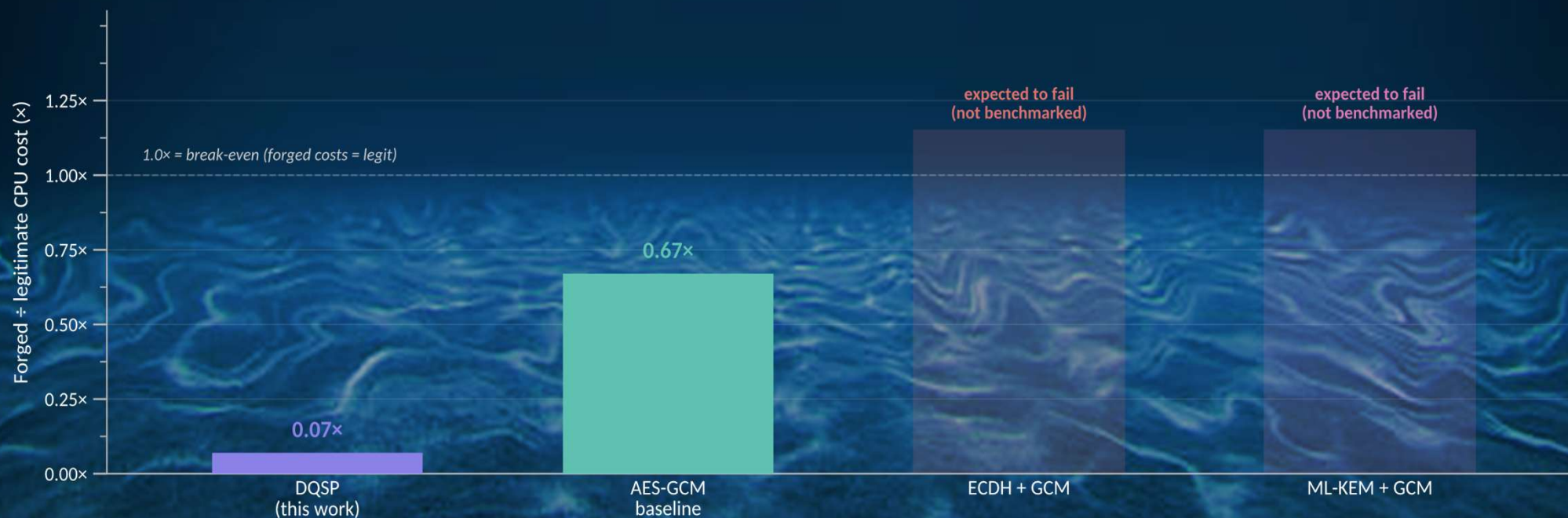
EW LLM-Orchestrated Multi-Agent Red Team

Subsurface Acoustic UUV — Robustness Under Sonar Jamming



EW LLM-Orchestrated Multi-Agent Red Team

Forgery DoS — cost to reject a forged packet (lower is better)



EW LLM-Orchestrated Multi-Agent Red Team

Property	AES-PSK	AES-GCM	ECDH + GCM	MLKEM + GCM	DQSP
Surface RF — light mixed attack ²	44%	26%	12% ¹	0% ¹	66%
Surface RF — moderate mixed attack ²	28%	9%	0% ¹	0% ¹	36%
Surface RF — heavy mixed attack ²	0%	2%	0% ¹	0% ¹	14%
Subsurface acoustic UUV (sonar jamming) ³	35%	23%	—	—	44%
Subsurface acoustic UUV (heavy combined) ³	23%	14%	—	—	28%
Submarine VLF atmospheric (BER 0.5%) ³	57%	27%	—	—	74%
Submarine VLF jammed (20% loss + BER 1%) ³	23%	4%	—	—	46%
Underwater optical (high turbidity) ³	30%	22%	—	—	34%
Per-message forward secrecy	No	No	Session	Session	Yes
Post-quantum secure	Yes	Yes	No	Yes	Yes
Capture exposure	Fleet	Fleet	Session	Session	Message
Wire overhead per packet	8 B	28 B	29 B + HDSK	29 B + 2.3 KB	8 B
Forgery DoS amplification	1.0×	1.1×	n/a (dies)	n/a (dies)	0.07×

¹ Session declared dead during the run; protocol unable to deliver further commands without operator intervention. ² Surface RF mixed-attack scenarios apply random packet loss, per-bit corruption, burst jamming, and reorder simultaneously, scaled from light (10% loss, 0.1% BER) through severe (55% loss, 1.5% BER). ³ Subsurface scenarios use channel-appropriate dictionaries (acoustic 32B AUV command, VLF 6B fleet broadcast, optical 64B sensor frame) and post-FEC BER ranges representative of the medium; ECDH and ML-KEM omitted as their multi-packet handshakes are not feasible at subsurface bandwidths and latencies. Numbers measured, reproducible from the published reference implementation.

Next Steps

