Enhancing Naval ISTAR using Secure COTS Drone Swarms

Lt Morgan Colbeck RN MSci IEng MIET GCGI

EAAW XI, IMarEST Conference, November 2025

Royal Navy

Outline

Introduction

Disclaimer

I am presenting this as Open Source research independently from any Royal Navy projects in this area. My views do not necessarily reflect the Royal Navy's views on these topics.

Motivation

Figure 1: Type 45 Destroyer

[BAE Systems, 2025]

Figure 2: Conventional Fast Inshore Attack Craft (FIAC) Swarm

[GlobalSecurity.org, 2022]

Motivation

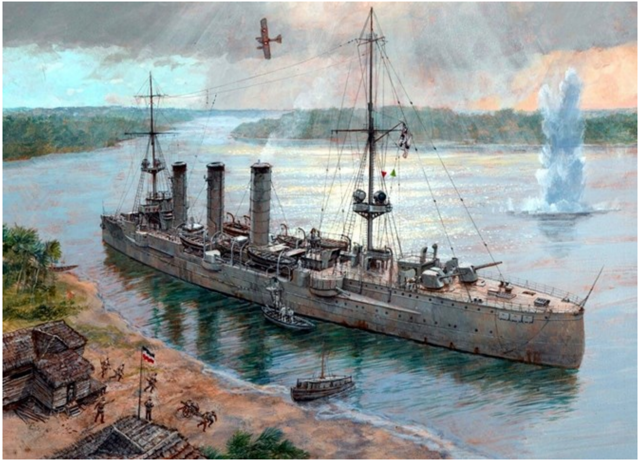


Figure 3: Rufiji Delta (1915) by Paul Wright

[The Western Front Association, 2025]

Motivation

Figure 4: Wildcat with Martlet equipped

[Navy Lookout, 2020]

Motivation

- Maritime domain: asymmetric threats (FIACs, small-boat swarms, drone swarms) demand low-cost Intelligence, Surveillance, Targeting, and Reconnaissance (ISTAR) solutions.
- Rapid evolution of Commercial Off The Shelf (COTS) drones reshaping modern warfare; demonstrated impact in Ukraine.
- Central question: How can COTS drones be used in maritime warfare without compromising security or real-time data flow for operations?

Network Centric Warfare

Network Centric Warfare

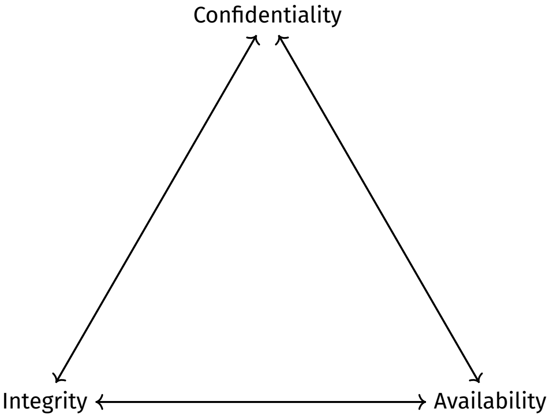
- Information dominance is and has always been a force multiplier.
- Modern Network Centric Warfare is provided by sensors, communications, command & control (C2), and precision weapons.
- Tactical Data Links (TDLs) provide backbone.
- Direct integration into the TDLs increases the cyber attack surface and potentially derails the way we fight.
- Use of non-military assets requires pragmatic security and interoperability measures.

Balancing the Confidentiality, Integrity, Availability Triad

Balancing Confidentiality, Integrity, Availability (CIA)

- **Confidentiality:** prevent adversary interception of sensitive data.
- **Integrity:** ensure targeting and C2 data are untampered.
- **Availability:** maintain timely data flow, even under attack.

The Trade Off



The Trade Off

If you prioritise...	You constrain...	Why
Confidentiality	Availability & Integrity	Strong access control and encryption can make systems harder to access or verify.
Integrity	Availability & Confidentiality	Verification layers (hashing, audits, validation) introduce overhead and delay.
Availability	Confidentiality & Integrity	Fewer access barriers and reduced checks maintain uptime but weaken protections.

Drones in the Maritime Domain

Drone use for ISTAR

- Command will have a higher risk appetite with uncrewed drones allowing higher risk operations to be carried out.
- High quantities of drones provide mass and persistence.
- Use-case: feeding targeting data to naval guns (e.g. 5” guided projectiles).
- Multiple cheap drones reduce cumulative error (GPS-like error correction).

Error Correction

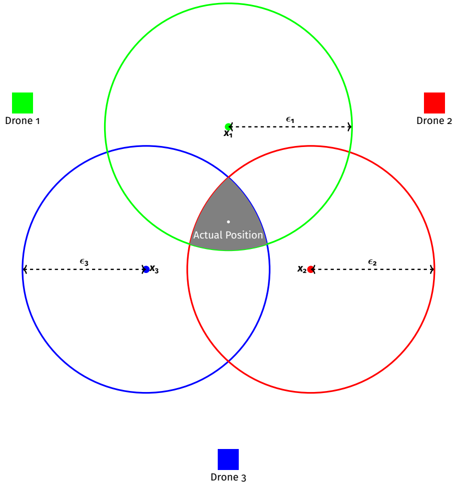


Figure 5: Multiple data sources reduce overall error

Resilience in Contested Spectrum

Resilience: RF DEWs, Jamming, and Hardening

- Radio Frequency (RF) Directed Energy Weapons (DEWs) and Global Navigation Satellite System (GNSS) jamming threaten COTS survivability.
- Options: Electromagnetic shielding against RF DEWS; Inertial Navigation Systems (INS) for GNSS-denied ops.
- Increases in resilience corresponds to an increase in cost.
- Tiered fleet: mass-produced “disposable” drones vs hardened persistent drones.
- Options to Command, allowing a threat appropriate drone to be used in each scenario.

Authentication and Trust Models

Authentication and Trust Models

- **Public Key Infrastructure:** strong integrity and confidentiality, familiar civilian tooling (Transport Layer Security, TLS; Secure Socket Layer, SSL; Secure Shell Hashing, SSH).
- **Centralised:** central authorities, no local authentication, less flexible, provides excellent top down security.
- **Decentralised:** no central authority, flexible for ad-hoc coalition partners; suitable for local vouched trust.
- **Hybrid:** central authorities with local verification permitted for operational flexibility.

Centralised Certificate Authority

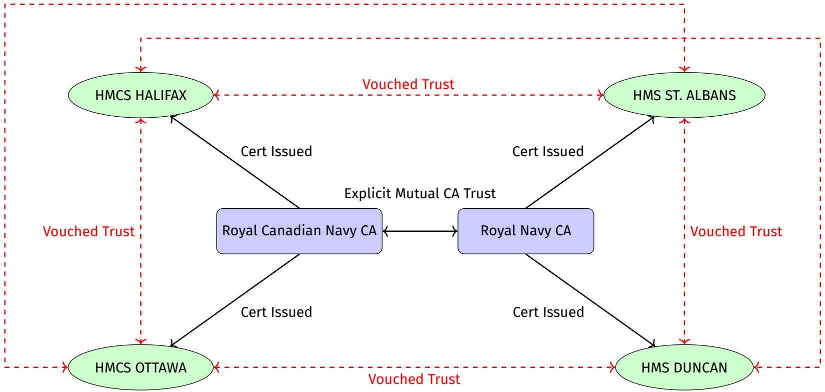


Figure 6: Web of trust with only centralised authorities permitted to authenticate.

Decentralised Certificate Authority

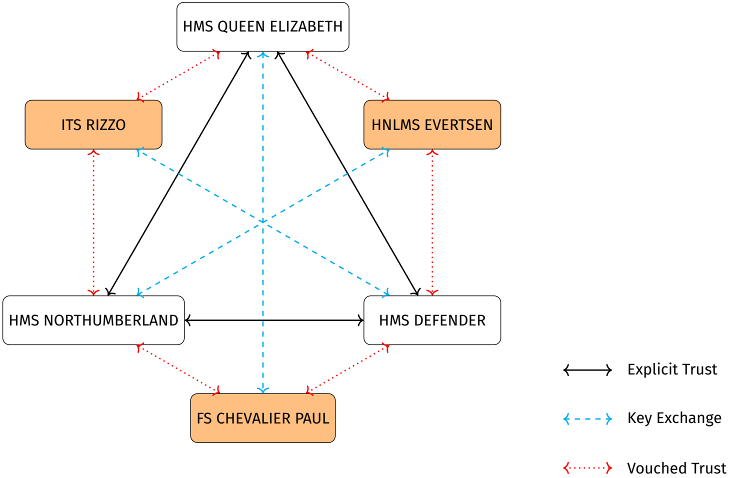


Figure 7: Web of trust with anyone permitted to authenticate. Though vouched trust exists between all parties the additional vouched trust lines have been omitted for clarity.

Secure Network Topology

Proposed Topology: Vouched Trust

- A full zero trust model cannot be used due to requirement for interoperability.
- Zero-trust principles applied pragmatically with a vouched-trust model for coalition ops.
- Sandbox picture compiler aggregates, filters, rate-limits COTS inputs.
- Hardware unidirectional data diode moves curated picture into the combat system.

Proposed Network Topology

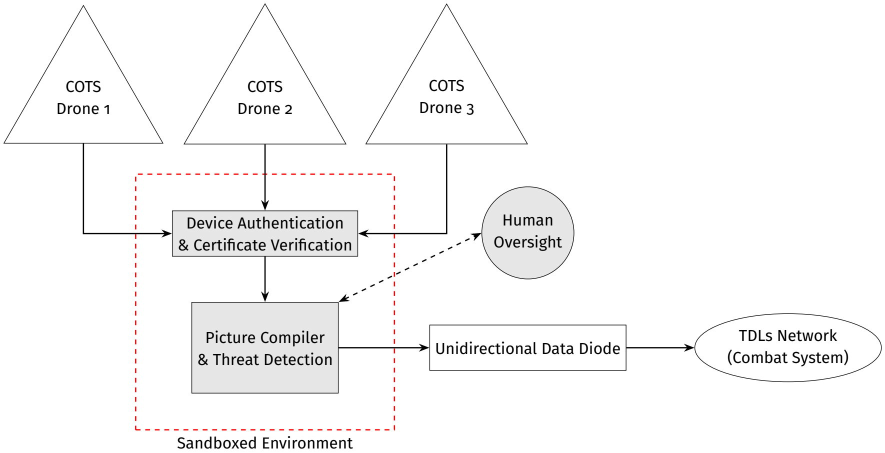


Figure 8: Proposed network topology with three drones as an example

Operational Trade-offs

Costs, Survivability, and Force Design

- Command can consider the mission threat profile.
- Evaluate cost-per-mission vs survivability (e.g. 3 cheap drones vs 1 hardened drone).
- Heterogeneous fleet design enables appropriate asset selection per mission profile.
- Net effect: restore cost-parity against asymmetric threats and reduce personnel risk.

Responding to the Quantum Threat

Quantum Threats and Post-Quantum Cryptography

- Quantum computing will eventually break today's asymmetric algorithms (e.g., RSA) on strategic timescales.
- To prepare, we adopt a hybrid cryptographic model combining conventional and post-quantum algorithms.
- NIST (2024) standardised CRYSTALS family (Kyber/Dilithium) enables a quantum-resistant Web of Trust.
- The tactical risk today is low so COTS drones are unlikely to incorporate quantum-relevant attacks.
- For resource-constrained drones, computationally heavy PQC operations should be kept off-device to preserve performance.

Conclusion

Conclusion and Next Steps

- Secure use of COTS drone swarms yields significant operational advantage at low cost.
- Enables our people to be kept out of harm's way.
- Implement hybrid trust architectures, sandboxing, and data diodes for safe integration.
- Opportunity to exploit COTS drones in the maritime domain through Royal Navy Task Groups in lieu of crewed air assets.

Questions

Thank You.

Bibliography

BAE Systems (2025).
Type 45 destroyers.
https://www.baesystems.com/en-uk/product/destroyers.

GlobalSecurity.org (2022).
Swarming small surface craft.
https://www.globalsecurity.org/military/world/iran/swarming.htm.

National Institute of Standards and Technology (2024).
Announcing approval of three federal information processing standards (fips) for post-quantum cryptography.
https://csrc.nist.gov/news/2024/postquantum-cryptography-fips-approved.

Navy Lookout (2020).
The martlet missile – the wildcat helicopter gets its claws.
https://www.navylookout.com/the-martlet-missile-wildcat-helicopter-gets-its-claws/.

The Western Front Association (2025).
Running the Rufiji gauntlet: The destruction of SMS Königsberg.
https://www.westernfrontassociation.com/world-war-i-articles/running-the-rufiji-gauntlet-the-destruction-of-sms-konigsberg/.