Enhancing Naval Combat Systems with Secure COTS Drone Swarms

Lt. M J L Colbeck RN MSci IEng MIET
Royal Navy

Synopsis

The rapid proliferation of Commercial Off-The-Shelf (COTS) technology has transformed modern warfare, particularly in network-centric operations. Maritime forces must now integrate low-cost, high-impact solutions to counter asymmetric threats, including Fast In-Shore Attack Crafts (FIACs) and drone swarms. This study examines how COTS drones and other commercially available technologies can enhance networked targeting, intelligence gathering, and operational resilience in naval combat scenarios.

Recent conflicts, particularly in Ukraine, have demonstrated the effectiveness of COTS drones for reconnaissance, fire control, and direct attack roles. Applying these concepts to naval operations, this paper proposes a framework for integrating COTS-based sensor networks into Tactical Data Links (TDLs) while maintaining cybersecurity, interoperability, and real-time operational capability.

A primary challenge in this integration is balancing the Confidentiality, Integrity, and Availability (CIA) Triad to ensure secure data exchange without compromising real-time decision-making. This paper explores Public Key Infrastructure (PKI), Web of Trust authentication models, and post-quantum cryptography solutions to mitigate cyber vulnerabilities while maintaining tactical flexibility. Additionally, it discusses network topology enhancements, including hardware-based data diodes and sandboxed computing environments, which are currently being implemented within the Royal Navy's Shared Infrastructure (SI) approach to Combat Management Systems.

A COTS-enhanced targeting solution is proposed, utilising drone swarms to feed targeting data into naval gun systems. By leveraging error correction algorithms akin to GPS positioning, multiple low-cost drones can enhance accuracy, reduce targeting errors, and mitigate adversary countermeasures. The study further outlines a cost-effective approach to restoring parity between naval forces and asymmetric threats by integrating low-cost ISTAR platforms with long-range naval artillery and missile systems.

Finally, the challenges posed by quantum computing threats to military cryptographic protocols are addressed, focusing on hybrid post-quantum encryption frameworks to ensure secure tactical communications in a rapidly evolving cyber landscape.

Keywords: COTS (Commercial Off-The-Shelf) Devices; Network Centric Warfare; Drone Swarms; Tactical Data Links; PKI (Public Key Infrastructure); Post-Quantum Cryptography; Asymmetric Warfare

1 Introduction

As Bill Gates said about business, "How you gather, manage, and use information will determine whether you win or lose" (Gates and Hemingway, 2000, p.1). This fundamental principle, and the need for information to enable it, is the driving force behind many great technological revolutions, from the telegraph to radar. In this vein, observation balloons were first deployed in the American Civil War to inform the artillery where the enemy's forces were (Hoehling, 1958, p.116). This evolved during the First World War to the deployment of observation aircraft and the use of photography to allow coordination of artillery and create weak points in the enemy's line (Finnegan, 2006, p.3). In the maritime domain, this was used significantly in the Battle of Rufiji Delta and the sinking of *SMS Königsberg* (Pollen, 2016).

The accurate identification of where to strike was developed further in the Second World War, with an identified need to know when to strike. In the North African Campaign, the observation that most casualties are caused in the first few seconds of an artillery strike led to the development of Time on Target (Pemberton, 2022). This theory sought to maximise firepower brought to bear at a single point in time and space, which was used to have a devastating effect in this theatre. Combining this with developments in communication technology has led to the development of Network Centric Warfare, enabling precision-guided munitions and effective coordination of units.

The potential of revolutions in commercial off-the-shelf (COTS) drone technology and 3D printing to enhance military capabilities has been vividly demonstrated in Ukraine (The Economist, 2024a). Though drones are increasingly used in air-to-air combat (Jennings, 2024) or logistics (The Boeing Company, 2024), this paper will focus on using drones in an observation and target acquisition role. Military strategists have seen the benefits of integrating these data sources into networks, as shown in Ukraine. This paper justifies the tactical necessity and explores how these data sources, both allied and self-supplied, can be securely added to modern military tactical data networks, inspiring optimism for the future of military technology.

Author's Biography
Lt Morgan Colbeck currently works within the Combat System Design Authority at Defence Equipment & Support while studying for an MSc in Cyber Defence and Information Assurance at Cranfield University. He has previously served as DWEO on *HMS Duncan*.

2 Network Centric Warfare

Network Centric Warfare, a system that leverages sensors, command and control, and precision weapons to achieve and exploit information dominance, is a powerful strategy (Alberts et al., 1999, p.88). Its key advantage lies in shared situational awareness, which enables commanders to make effective decisions and enhance operational efficiency. The real-time data distribution across military units allows them to operate with a shared understanding of the battlespace. This shared situational awareness enables units to make well-informed decisions based on real-time intelligence, surveillance, target acquisition, and reconnaissance (ISTAR) data. These elements combine to act as a force multiplier, improving resource utilisation and enabling units to operate with greater precision and agility.

Despite these advantages, Network Centric Warfare presents significant challenges. The heavy reliance on tactical data networks presents a large cyber attack surface, introducing significant cybersecurity risks (Koch and Golling, 2015). This requires strong encryption, which exposes interoperability problems when integrating external devices, either acquired outside standard military supply channels or while cooperating with coalition partners. This is mainly achieved in the military maritime environment through Tactical Data Links (TDLs) such as Link 16 (BAE Systems, 2016).

As shown in the Ukraine conflict, small, inexpensive COTS and 3D printed drones have been used for reconnaissance, targeting, and even direct attacks (Zafra et al., 2024; The Economist, 2024b). These devices have leveraged the advantages afforded by networked COTS drones to deliver significantly improved targeting accuracy at a low cost (The Economist, 2025). Since the devices are low-cost and un-crewed, there is an increased risk appetite to move the drone closer to the enemy than an expensive military or crewed aircraft. Additionally, these devices can be integrated into existing doctrine, negating the need to alter the conceptual component of fighting power (UK Ministry of Defence, 2022). Once these devices are integrated, they can be used similarly to the operators' existing equipment. This requires either modifying COTS devices to accommodate military encryption or finding another encryption method that can be easily applied to a commercial device. Any solution to this problem must find an acceptable compromise across the CIA triad while minimising additional overhead costs.

3 Maximising CIA

The CIA triad, Confidentiality, Integrity, and Availability, is the foundation of network security (Nieles et al., 2017). In a military context, these principles hold specific significance:

- **Confidentiality**: Protecting communication between naval assets, including voice and data, from unauthorised access. If enemy forces intercept critical data, such as their known positions, they can adjust and render intelligence useless. The Battle of Matapan, where Ultra intelligence intercepts enabled Admiral Cunningham to execute a counter, demonstrated that revealing operational plans allows adversaries to counter strategically. Ensuring secrecy through robust encryption and secure communication channels is essential (Carson and Yarhi-Milo, 2017).
- **Integrity**: Ensuring that transmitted data remains unaltered. In a naval environment, tampering with targeting orders or enemy position reports could lead to severe disruption, potentially causing friendly fire incidents. Cryptographic hash functions and digital signatures help maintain data integrity.
- **Availability**: Ensuring prompt access to data enables decision superiority. Military forces rely on fast and informed decision-making, supported by redundancy, failover mechanisms, and distributed architectures to maintain operations even under cyberattacks.

However, achieving a balance between these three principles presents significant challenges. Strengthening confidentiality through encryption may reduce availability due to access delays while enforcing rigorous integrity controls can slow data transmission in time-sensitive situations. Likewise, prioritising availability through redundancy increases the attack surface, potentially compromising confidentiality and integrity. This complexity underscores the difficulty of maintaining a secure and efficient network, highlighting the intricate nature of the task.

The strategic importance of this balance cannot be overstated. The longevity of the information's value to an adversary dictates the level of security required. For example, missile strike coordinates remain relevant only until the strike is executed, making ultra-secure encryption unnecessary. In contrast, long-term strategic plans require high confidentiality, even at the expense of integrity and availability. Implementing these principles is crucial to maintaining operational advantage.

While downlink protection is vital, C2 uplink integrity and availability are equally critical. A nearby adversary can jam or spoof C2 signals, overpowering the uplink and causing a loss of control or inserting malicious commands (Mitre Engenuity, 2023). Denial or manipulation of the uplink may not only ground the drone but also induce it to carry out hostile actions, turning a reconnaissance asset into a weaponised liability. Although many UAS

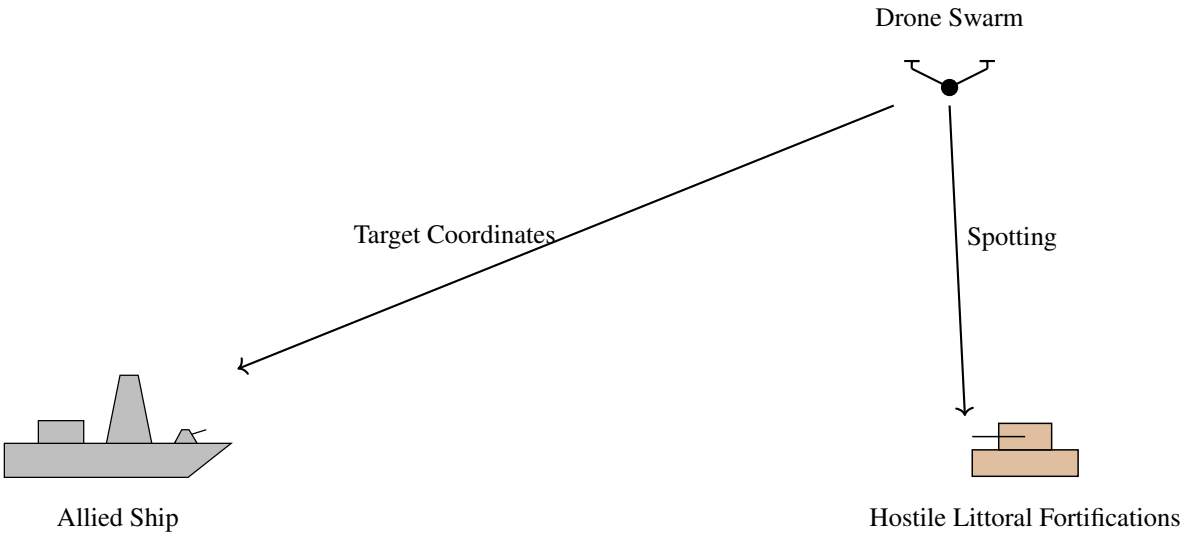

Figure 1: Diagram showing a ship and a drone swarm working to target hostile fortifications. The drone swarm provides target spotting and fire corrections to enhance the accuracy of the gun turret.

carry autonomy routines to "keep flying" when C2 is lost, these routines can be subverted via adversarial-example attacks on onboard machine-learning classifiers, causing mis-identification of obstacles or targets and creating new attack surfaces (Lu et al., 2023).

4 Maritime Drone Swarms and Saturation Attacks

The increasing use of FIACs in the Middle East highlights the asymmetric threat developing against modern warships (Thornton, 2007, p.120). With a low profile, small radar cross-section, and composed of highly radar absorbent materials such as fibreglass, it is challenging to detect these boats at range with modern radar technology. Instead, using an aerial observer, such as a helicopter, is much more reasonable for spotting these fast attack crafts. This is a weakness: helicopters are expensive in terms of both equipment and personnel. In this asymmetric environment, a single, low-cost munition, such as an RPG from the FIACs, could cause a large amount of damage to allied forces.

Translating the lessons from the Ukraine war to the maritime domain, similar tactics can be used against a FIAC swarm. A well-coordinated swarm of inexpensive COTS drones equipped with ISTAR capabilities could feed into a tactical data network and provide a cost-effective solution for identifying hostile targets. In particular, LIDAR (laser imaging, detection, and ranging) has been used effectively in direct sprays in farming (Gil et al., 2013). These advancements could be used with conventional guns, allowing them to target approaching vessels and engage them before the target can effectively engage.

The new standard medium calibre five-inch gun to be mounted on the Type 26 frigate has a reported range of 100km, with standard guided projectiles (BAE Systems, 2014, 2013). This ammunition is relatively cheap, compared to missiles, and can be resupplied at sea, limiting the ability of hostile forces to remove a threat by forcing them to waste ammunition. These measures restore the cost parity between the two sides and reduce the number of personnel in harm's way, providing a financially sound strategy. Additionally, due to the nature of plunging fire and a ballistic trajectory, a ship can engage these targets with this type of ammunition more effectively than with a simple unguided rocket, as is likely to be available to the FIAC.

Another example is offering support to land forces in the littoral environment, as shown in Figure 1. Aerial drones offer advantages over traditional aerial artillery spotters since their size makes them much more challenging to spot through radar and visually. Their low cost justifies a higher risk appetite. Therefore, they will likely be closer to the threat than the conventional, crewed alternatives. These drones can then direct gunfire similarly to the counter-FIAC example above.

This data network of cheap drones creates a unified target map. Like GPS, using more data mitigates sensor inaccuracies, minimising errors by comparing enough positional data with known error margins. A pictorial representation of this effect is in Figure 2 and is similar to how the search and rescue methodology works as explored by Lyu et al. (2023). Additionally, using multiple drones reduces the risk of the enemy achieving a mission kill on the spotter since multiple spotters must be removed.

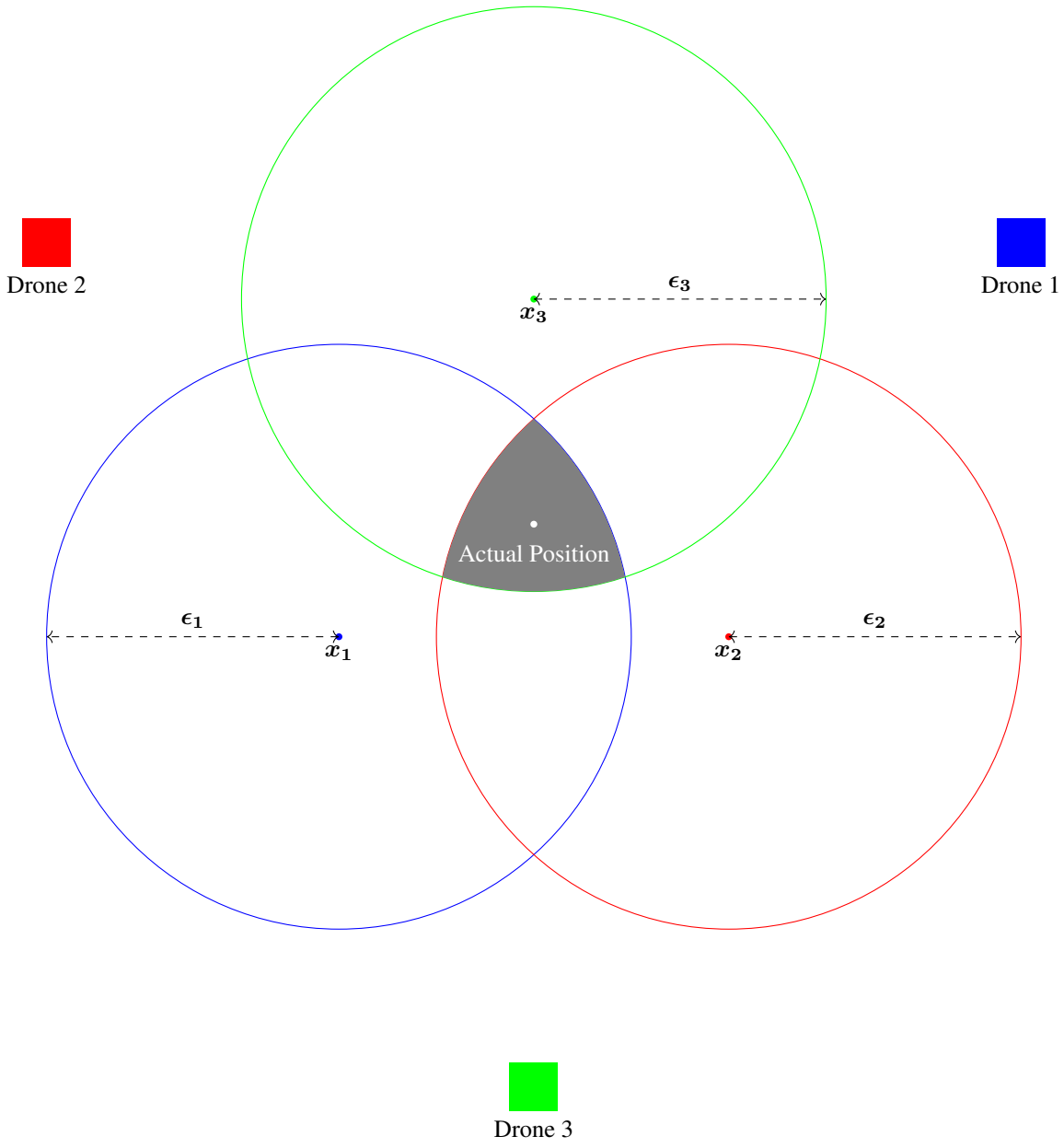

Figure 2: Diagram showing the reduced cumulative error by using multiple drones. The grey-shaded region denotes the cumulative error. The position observed by the i^{th} drone is denoted by $\boldsymbol{x_i}$ and the corresponding error margin by $\boldsymbol{\epsilon_i}$.

While drone swarms offer a promising way to restore tactical advantage and cost parity at sea, their effectiveness depends not only on integration with combat systems but also on their ability to operate in a contested electromagnetic environment. As adversaries deploy increasingly sophisticated jamming tools and fieldable radio frequency directed-energy weapons (RF DEWs), the resilience of commercial off-the-shelf (COTS) platforms becomes critical. To maximise operational benefit and avoid squandering mass through attrition, it is necessary to evaluate how much protection COTS drones require to stay in the fight, and how that affects their affordability, availability, and network value.

5 Resilience of COTS Systems in Contested Spectrum

Commercial off-the-shelf (COTS) drones have become indispensable on the modern battlefield, offering mass, flexibility, and fast adaptation cycles at relatively low cost. However, the emergence of high-end countermeasures, particularly radio frequency (RF) directed-energy weapons, has raised the stakes for survivability. The recent UK government announcement showcasing the Army's successful downing of a drone swarm using an RF DEW underscores the rapidly shifting threat environment Ministry of Defence (2025). This poses a similar problem to optimising the CIA triad: What are reasonable measures to use to harden drones to electronic attack without overly increasing the unit cost?

COTS drones succeed because they are cheap and scalable, but this simplicity leaves them vulnerable. A £200 FPV drone, as advertised by iFlight (2025), is likely to be highly susceptible to electronic attack. RF DEWs, like those demonstrated by the UK, use bursts of high-powered energy to disrupt electronics and communications at line-of-sight ranges. Unlike kinetic defences, they impose no reload penalty and can be used continuously, raising the bar for drone survivability.

There are commercial solutions available to harden against these effects. Snap-on EMI shields, RF-absorbent board coatings, and compact Faraday enclosures initially designed for consumer and industrial electronics can be adapted for drone platforms (Taranovich, 2021). Similarly, COTS navigation modules now routinely integrate inertial measurement units (IMUs), barometric sensors, and visual odometry to maintain position when GPS is denied or spoofed (Luo et al., 2023; Zhang et al., 2024). These upgrades may help a drone survive a DEW pulse and resume its mission vector, but they significantly increase per-unit cost.

This leads to a trade-off: if a hardened drone survives five missions versus one, is that worth the 2x price increase? The answer is often contextual, and the topology described in this paper allows and encourages the use of heterogeneous devices so commanders can select the most appropriate device to use in each situation. In permissive environments or when mass is the objective, such as saturation attacks or short-range reconnaissance, unprotected drones could remain a viable option. However, as RF DEWs and GPS jamming proliferate, a tiered fleet becomes more sensible: some drones are built for mass, others for persistence (The Economist, 2024b).

Mesh networking and adaptive routing are also entering the COTS space. Off-the-shelf radios capable of frequency hopping, beamforming, and encrypted communication can maintain control links even when spectrum is contested (L3Harris Technologies, 2024). Meanwhile, distributed swarming logic, commercially available through software overlays, allows drones to react autonomously if links are lost or a node is destroyed by RF energy (Chakraborty and Kar, 2017). Advances in swarm logic will further facilitate drone swarm flexibility (Abbass and Mostaghim, 2025).

This approach is not designed to turn COTS devices into bespoke defence projects but to apply selective hardening intelligently. A fully ruggedised COTS drone will not equal a bespoke military-spec solution. However, for a fraction of the cost, it can survive long enough to deliver effects in an increasingly hostile electromagnetic spectrum. As RF DEWs become more common, not only in state arsenals but potentially adapted for field use by non-state actors, resilience will define the real value of mass. The ability to stay in the fight, even when irradiated, jammed, or spoofed, quickly becomes the measure of effectiveness, not just cost.

Ensuring that drones survive long enough to contribute meaningful ISTAR or targeting data fundamentally shifts the burden onto the network itself. Secure integration is no longer just about protecting sensitive naval infrastructure from infiltration; it must also account for the variable survivability and trustworthiness of heterogeneous, often disposable, airborne nodes. This places renewed importance on architectures that enforce separation, validation, and layered trust before data is admitted into tactical networks, particularly when dealing with autonomous or semi-autonomous systems in hostile airspace.

6 Proposed Network Topology

The secure integration of COTS devices is essential for implementing this approach in a military environment. The network design adopts zero-trust principles (Rose et al., 2020), including explicit authentication, authorisation, and continuous verification, but applies those principles pragmatically within a "vouched" trust model (operationally-accepted, scope-limited and auditable). The topology must prevent data extraction from, and preserve the integrity of, the existing TDLs. To achieve this, a hardware unidirectional data diode is introduced,

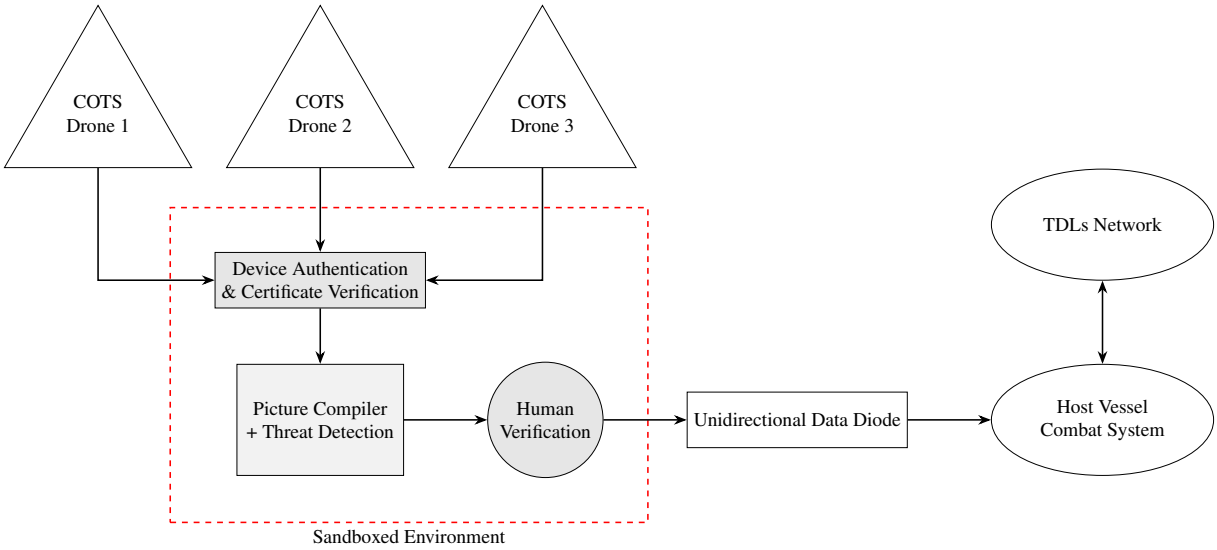

Figure 3: Network topology for securely integrating COTS drones into a naval combat system. The architecture incorporates layered authentication, sandboxed processing, and human verification before unidirectional transfer via a data diode into the host vessel's combat system before being sent into the TDLs, ensuring data integrity and operational security.

described in (Stevens and Pope, 1999), that allows only traffic from COTS devices into the tactical network, an approach used in industrial control systems (Jeon and Na, 2016). This integration is facilitated by developments such as Shared Infrastructure (BAE Systems, 2021) which allows sandboxing and Tacticos (Thales, 2025) which integrates autonomous platforms.

The second requirement requires additional safeguards. Firstly, since the network requires multiple distinct data sources to operate optimally, the host vessel's combat system or TDLs may be overloaded with data from the COTS devices. To mitigate this, a separate COTS picture compiler aggregates, filters and rate-limits inputs from those devices. The compiled, curated picture is then passed through a hardware unidirectional data diode into the combat system ingress; the combat system ingests the curated picture and forwards relevant tactical data onward into the TDLs backbone. Placing the picture compiler, threat-detection and human-in-the-loop verification in a sandboxed, untrusted domain outside the trusted TDLs environment protects the TDLs from data extraction and flooding, while the sandboxed processing defends the combat system's integrity and availability by detecting and rejecting malformed or malicious inputs.. Figure 3 shows the topology of this network.

The data must be secured in transit. This ensures that the data arrives intact and that unauthorised devices cannot access the data in the network. Symmetric encryption would require all drones to share a common password, providing a single point of failure or a unique password for each drone, requiring careful password management. A similar problem is experienced in commercial internet browsing, solved through Public Key Infrastructure (PKI).

PKI is highly used in the civilian world to ensure secure communication and data exchange. Through its use in the Transport Layer Security (TLS) protocol, PKI manages millions of online financial transactions daily. Its asymmetric cryptography enables a high level of confidentiality, with a unique shared key encrypting all messaging and availability since it is easy to create this shared key. Through the Secure Shell (SSH) protocol, PKI has also been used to encrypt communication to a robot (Megalingam et al., 2019), showing the current capability to control complex devices. Figure 4 shows a proposed implementation.

PKI, being asymmetric, significantly supports data integrity. By units exchanging digital credentials before exchanging data packets, the data network can ensure that the data genuinely comes from where it claims to come (Kuhn et al., 2001). This robust system mitigates against an avenue of attack available to an adversary seeking to subvert this network by feeding it erroneous data. Without a valid digital signature, this data stream will be rejected, and the integrity of the data will be preserved, ensuring the reliability of the data network.

Though this method prevents an attacker who does not have a certificate from being able to authenticate the certificate, there is no means to spot a certificate created by the enemy and used to feed erroneous data into the network. Authenticating certificates can be done through certificate authorities (Akram et al., 2020). Centralised allied naval commands could establish central certificate issuing authorities and provide authenticated certificates to units. This would allow allied units to check that a digital signature is signed by a recognised central authority and trust devices vouched for by these recognised signatures. This trust framework is shown in Figure 5.

By contrast, an alternative method is supplied via a Web of Trust. The decentralised approach enables coalition

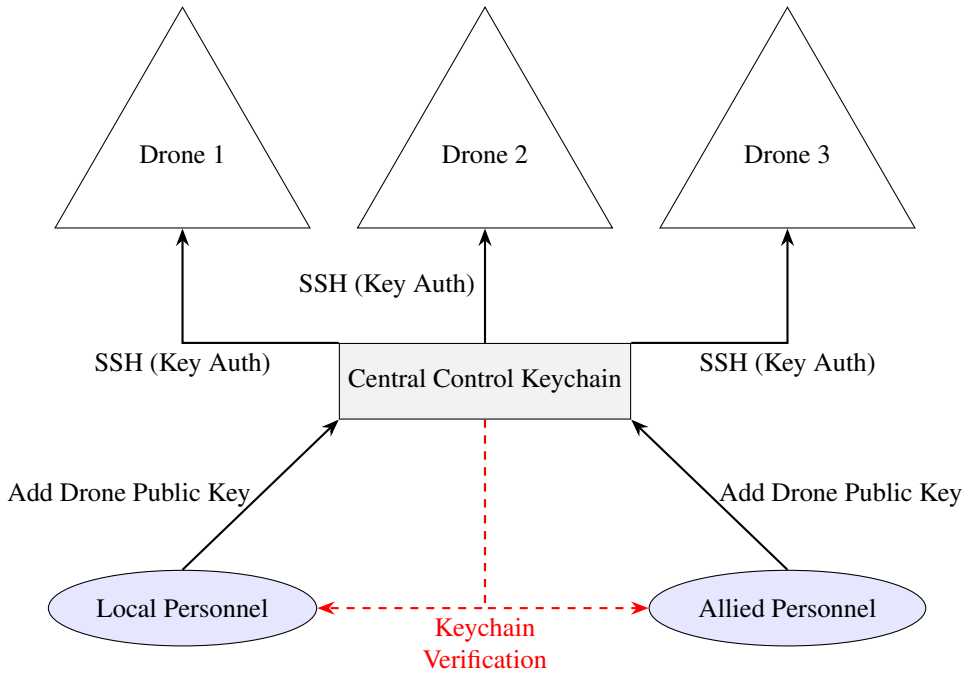

Figure 4: Web-of-Trust-vetted asymmetric key workflow: ship crews add public keys to the Central Control Keychain to authenticate SSH (or other asymmetric encryption such as TLS) sessions to COTS drones.

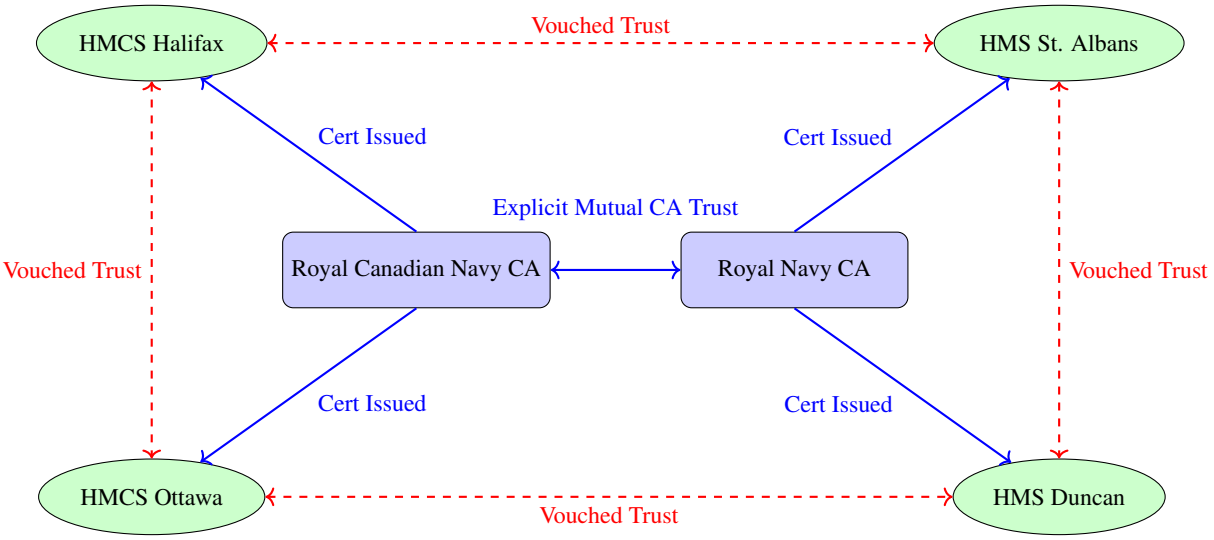

Figure 5: Star network depicting mutual trust between the Royal Canadian Navy CA and the Royal Navy CA, certificate issuance to their respective units, and vouched trust among the units.

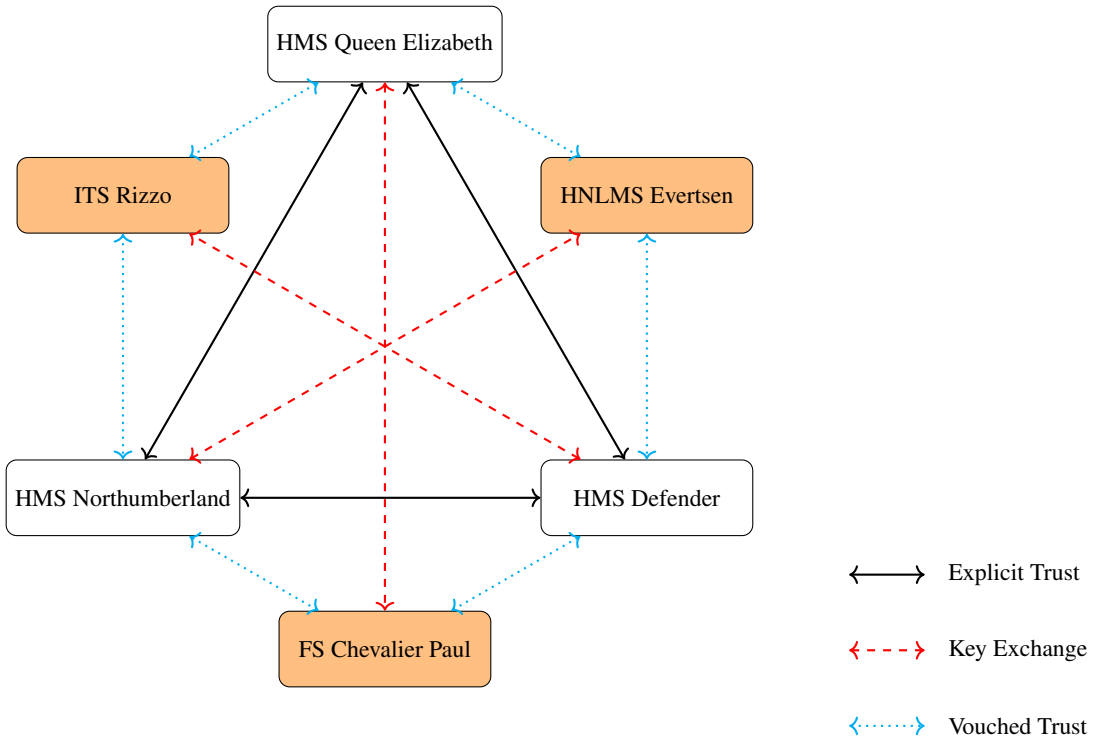

Figure 6: Decentralised Trust Network among UK and European Naval Units with Explicit and Vouched Trust Relations.

partners to have weighting within the network proportional only to their level of interfacing with it. Additionally, the dynamic scaling afforded by this method allows for ad hoc partners to be established while limiting the level of impact these potential bad actors can have. The web of trust reduces dependency on third-party authorities and proves resilient to centralised failures (Zimmermann, 1995). Since nations working together will have representatives meeting outside the operational context at some point, tracing the route of verified identities using the digital signatures from multiple trusted sources. Alternatively, short-term partners can establish a local trust framework without requiring approval or input from higher command. This allows trust to be established between local partners. Note that this method does not determine whether that person is trusted; it is merely that their certificate originates from that person.

This decentralised model ensures that the web maintains cohesion even if a single key is compromised. Before allowing devices from a coalition partner, the level of trust in the provider's identity is gauged through the web of trust, and a decision is made about whether to allow the device to transmit into the data network. Figure 6 depicts a proposed web of trust within a Carrier Strike Group. However, a hybrid trust framework is likely most appropriate in a military context. This establishes centralised trusted authorities, providing a framework through which trust can flow from the central authorities. Additionally, this provides flexibility when the need arises for local trust frameworks to be established.

7 Quantum Resilience

The threat posed by currently used asymmetric cryptography by quantum computing has been thoroughly researched and is well understood. Due to the potential yield from breaking into an enemy's decision-making progress, an adversary with quantum computing capabilities will likely use it to attack. Since it is likely that a "quantum computer capable of breaking 2000-bit RSA [Rivest–Shamir–Adleman] in a matter of hours could be built by 2030" (Chen et al., 2016), it must be considered a certainty in this context and at the timescales being considered.

Since this threat is well understood, substantial research has been conducted to find post-quantum algorithms. NIST has selected the Crystals family of algorithms with encryption provided by the Kyber algorithm and authentication provided by the Dilithium algorithm (National Institute of Standards and Technology, 2024). Together, these protocols fulfil both requirements for a PKI network as described. It is noteworthy that cloud computing

providers have adopted a hybrid encryption approach using both an RSA and a lattice-based encryption method, as recommended by Avanzi et al. (2020). This allows a hedge against quantum computing development and potential vulnerabilities in the lattice protocol.

This method should be avoided for direct interaction with the COTS devices since RSA and lattice encryption require significant processing power, which could slow down tactical decision-making on processing-constrained devices. The additional strain compromises the performance of a highly time-sensitive system. Therefore, the protocol should preserve the most important aspect: the time-sensitive data. However, two parallel webs of trust should be established with RSA and lattice-based keys. Since a breach in this encryption protocol would be limited to a small scale due to the time criticality of tactical networks, once the breach has been identified, use of the compromised protocol can cease, leaving the protocol that has not been compromised.

8 Conclusion

The rapid advancement of commercial technology has transformed asymmetric warfare, particularly in maritime security. Fast In-Shore Attack Crafts (FIACs), such as those used by Iran, pose a significant threat to conventional surface combatants due to their small radar signature and low cost. Countering this threat requires leveraging low-cost solutions like drones for reconnaissance and targeting, as demonstrated in the Ukraine conflict. As these drones are commercially sourced, ensuring secure and interoperable communications is essential, particularly in coalition operations.

A robust data network must balance Confidentiality, Integrity, and Availability (CIA) to maintain secure military operations, as overly secure encryption may hinder real-time decision-making. Maritime drone swarms offer a cost-effective method to enhance situational awareness and neutralise asymmetric threats. By using a network of drones for observation and targeting, naval forces can improve accuracy while minimising risks to personnel. Successful integration of COTS equipment depends on adopting a commercial standard, while a decentralised Web of Trust reduces reliance on central authorities and enhances coalition security. This approach ensures secure collaboration without compromising national security.

The growing quantum threat to asymmetric cryptography must be addressed. While post-quantum algorithms, such as the Crystals family, show promise, hybrid encryption methods that combine traditional RSA with lattice-based encryption may be too resource-intensive for real-time military networks. Instead, using RSA and lattice-based keys, a dual Web of Trust could provide resilience against future cryptographic threats.

This integrated modern network, leveraging drones, secure communications, and post-quantum cryptography, ensures the Royal Navy remains prepared for emerging asymmetric threats while maintaining operational effectiveness and coalition interoperability. Incorporating these capabilities into Royal Navy task groups enhances resilience against asymmetric threats. It lays the groundwork for future doctrine that embraces zero trust principles to provide flexible and data-centric operations in the contested maritime battlespace.

References

Abbass, H. and Mostaghim, S. (2025). The road forward with swarm systems. *Philosophical Transactions A*, 383(2289).

Akram, M., Barker, W., Clatterbuck, R., Dodson, D., Everhart, B., Gilbert, J., Haag, W., Johnson, B., Kapasouris, A., Lam, D., et al. (2020). Securing web transactions: Tls server certificate management. Technical report, National Institute of Standards and Technology.

Alberts, D., Garstka, J., and Stein, F. (1999). *Network Centric Warfare: Developing and Leveraging Information Superiority*. CCRP publication series. National Defense University Press.

Avanzi, R., Bai, S., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J. M., Schwabe, P., Seiler, G., Stehlé, D., Bos, J., and Ding, J. (2020). Crystals-kyber: Algorithm specifications and supporting documentation. https://pq-crystals.org/kyber/.

BAE Systems (2013). 5-inch multi-service standard guided projectile (ms-sgp). https://www.baesystems.com/en/product/5--multi-service-standard-guided-projectile.

BAE Systems (2014). Mk45 mod 4 naval gun system. https://www.baesystems.com/en/product/mk-45-mod-4-naval-gun-system.

BAE Systems (2016). Data link 16. https://www.baesystems.com/en/product/link-16-terminals.

BAE Systems (2021). Shared infrastructure (SI). https://www.baesystems.com/en/product/shared-infrastructure--si-.

Carson, A. and Yarhi-Milo, K. (2017). Covert communication: The intelligibility and credibility of signaling in secret. *Security Studies*, 26(1):124–156.

Chakraborty, A. and Kar, A. K. (2017). Swarm intelligence: A review of algorithms. *Nature-inspired computing and optimization: Theory and applications*, page 475–494.

Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., and Smith-Tone, D. (2016). Report on post-quantum cryptography. https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.8105.pdf.

Finnegan, T. (2006). *Shooting the Front: Allied Aerial Reconnaissance and Photographic Interpretation on the Western Front–World War I*. Center for Strategic Intelligence Research, National Defense Intelligence College.

Gates, B. and Hemingway, C. (2000). *Business at the Speed of Thought: Succeeding in the Digital Economy*. Penguin Books Limited.

Gil, E., Llorens, J., Llop, J., Fàbregas, X., and Gallart, M. (2013). Use of a terrestrial lidar sensor for drift detection in vineyard spraying. *Sensors*, 13(1):516–534.

Hoehling, M. (1958). *Thaddeus Lowe: America's One-man Air Corps, Born August 20, 1832, Died January 16, 1913*. Kingston House.

iFlight (2025). iflight titan dc2 hd bnf with dji digital air unit. https://www.quadcopters.co.uk/dji-digital-fpv-whoops/iflight-titan-dc2-hd-bnf-with-dji-digital-air-unit.

Jennings, G. (2024). Ukraine conflict: UAV takes down helicopter in air-to-air first. https://www.janes.com/osint-insights/defence-news/air/ukraine-conflict-uav-takes-down-helicopter-in-air-to-air-first.

Jeon, B.-S. and Na, J.-C. (2016). A study of cyber security policy in industrial control system using data diodes. In *2016 18th International Conference on Advanced Communication Technology (ICACT)*, page 314–317. IEEE.

Koch, R. and Golling, M. (2015). Blackout and now? network centric warfare in an anti-access area-denial theatre. In *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, page 169–184. IEEE.

Kuhn, D. R., Hu, V. C., Polk, W. T., and Chang, S.-J. (2001). Introduction to public key technology and the federal PKI infrastructure. Technical Report NIST SP 800-32, National Institute of Standards and Technology.

L3Harris Technologies (2024). Anti-jam resilient radio objective waveform for secure coalition interoperability. https://www.l3harris.com/newsroom/editorial/2024/02/anti-jam-resilient-radio-objective-waveform-secure-coalition.

Lu, Z., Sun, H., and Xu, Y. (2023). Adversarial robustness enhancement of uav-oriented automatic image recognition based on deep ensemble models. *Remote Sensing*, 15(12):3007.

Luo, H., Li, G., Zou, D., Li, K., Li, X., and Yang, Z. (2023). Uav navigation with monocular visual inertial odometry under gnss-denied environment. *IEEE Transactions on Geoscience and Remote Sensing*, 61:1–15.

Lyu, M., Zhao, Y., Huang, C., and Huang, H. (2023). Unmanned aerial vehicles for search and rescue: A survey. *Remote Sensing*, 15(13):3266.

Megalingam, R. K., Tantravahi, S., Tammana, H. S. S. K., Thokala, N., Puram, H. S. R., and Samudrala, N. (2019). Robot operating system integrated robot control through secure shell (ssh). In *2019 3rd International Conference on Recent Developments in Control, Automation & Power Engineering (RDCAPE)*, page 569–573. IEEE.

Ministry of Defence (2025). British soldiers take down drone swarm in groundbreaking use of radio wave weapon. https://www.gov.uk/government/news/british-soldiers-take-down-drone-swarm-in-groundbreaking-use-of-radio-wave-weapon.

Mitre Engenuity (2023). Securing command and control links in unmanned aerial systems. Technical Report TR-1234, MITRE Engenuity, McLean, VA.

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.

Nieles, M., Dempsey, K., Pillitteri, V. Y., et al. (2017). An introduction to information security. *NIST special publication*, 800(12):101.

Pemberton, B. (2022). *The Development of Artillery Tactics and Equipment: Official History Of The Second World War Army*. Naval & Military Press.

Pollen, A. (2016). *The British Navy In Battle*. Creative Media Partners, LLC.

Rose, S., Borchert, O., Mitchell, S., and Connelly, S. (2020). Zero trust architecture.

Stevens, M. W. and Pope, M. (1999). *An implementation of an optical data diode*. Citeseer.

Taranovich, S. (2021). Emi shielding for drones and uavs. https://www.electronicdesign.com/technologies/power/whitepaper/21179428/electronic-design-emi-shielding-for-drones-and-uavs.

Thales (2025). Tacticos - combat management system. https://www.thalesgroup.com/en/markets/defence-and-security/naval-forces/above-water-warfare/tacticos-combat-management-system.

The Boeing Company (2024). Mq-25 stingray. https://www.boeing.com/defense/mq25.

The Economist (2024a). The battle between drones and helicopters in Ukraine: Small cheap drones could pose a new threat to expensive russian craft. https://www.economist.com/the-economist-explains/2024/09/04/the-battle-between-drones-and-helicopters-in-ukraine.

The Economist (2024b). How ukraine uses cheap ai-guided drones to deadly effect against Russia: Ukraine is making tens of thousands of them. https://www.economist.com/europe/2024/12/02/how-ukraine-uses-cheap-ai-guided-drones-to-deadly-effect-against-russia.

The Economist (2025). The US army needs less-good, cheaper drones to compete:

Quantity has a quality all its own. https://www.economist.com/united-states/2025/01/05/the-us-army-needs-less-good-cheaper-drones-to-compete.

Thornton, R. (2007). *Asymmetric Warfare: Threat and Response in the 21st Century*. Asymmetric Warfare: Threat and Response in the Twenty-first Century. Polity Press.

UK Ministry of Defence (2022). JDP 0–01: UK defence doctrine, 6th edition. (JDP 0-01). Crown copyright.

Zafra, M., Rao, A., Hunder, M., and Kiyada, S. (2024). How drone combat in Ukraine is changing warfare. https://www.reuters.com/graphics/UKRAINE-CRISIS/DRONES/dwpkeyjwkpm/.

Zhang, B., Shao, X., Wang, Y., Sun, G., and Yao, W. (2024). R-lvio: Resilient lidar-visual-inertial odometry for uavs in gnss-denied environment. *Drones*, 8(9):487.

Zimmermann, P. (1995). *The Official PGP User's Guide*. MIT Press.