

Issue 3 – Summer 2026



DEFENCE

FILTRONIC:

Why space is the future of critical connectivity

HEWLAND:

Could UK motorsport be the defence sector's secret weapon?

BENEATH THE SURFACE OF SUBSEA SEMICONDUCTORS

FRONTLINE

Innovation from sky to sea **4**

NEWS BRIEFING **6**

NAVAL & SUBSEA

FILTRONIC: Undersea cable threats: why space is the future of critical connectivity **10**

BOIES SCHILLER FLEXNER: Subsea sabotage: underwater, undermined and under siege **14**

SWINDON SILICON SYSTEMS: High reliability semiconductors beneath the surface **16**

INSIGHTS

APRICORN: AS9100 certification explained **18**

PLEXTEK: GNSS resilience: The security imperative of modern warfare **20**

E2E-ASSURE: AI as the adversary: is defence doing enough to combat military AI? **24**

HEWLAND: Could UK motorsport be the defence sector's secret weapon? **26**

INTELLIGENCE SYSTEMS

FIVECAST: Fusion, not confusion, in revitalised border security **30**



26

IN CONVERSATION

ASL GRP: Jonathon Diffey, Managing Director **32**

Publisher

David Webb

d.webb@2bpublishing.co.uk

Editor

Jon Hughes

jon@industrialnews.co.uk

Design

2b Media

Partnerships

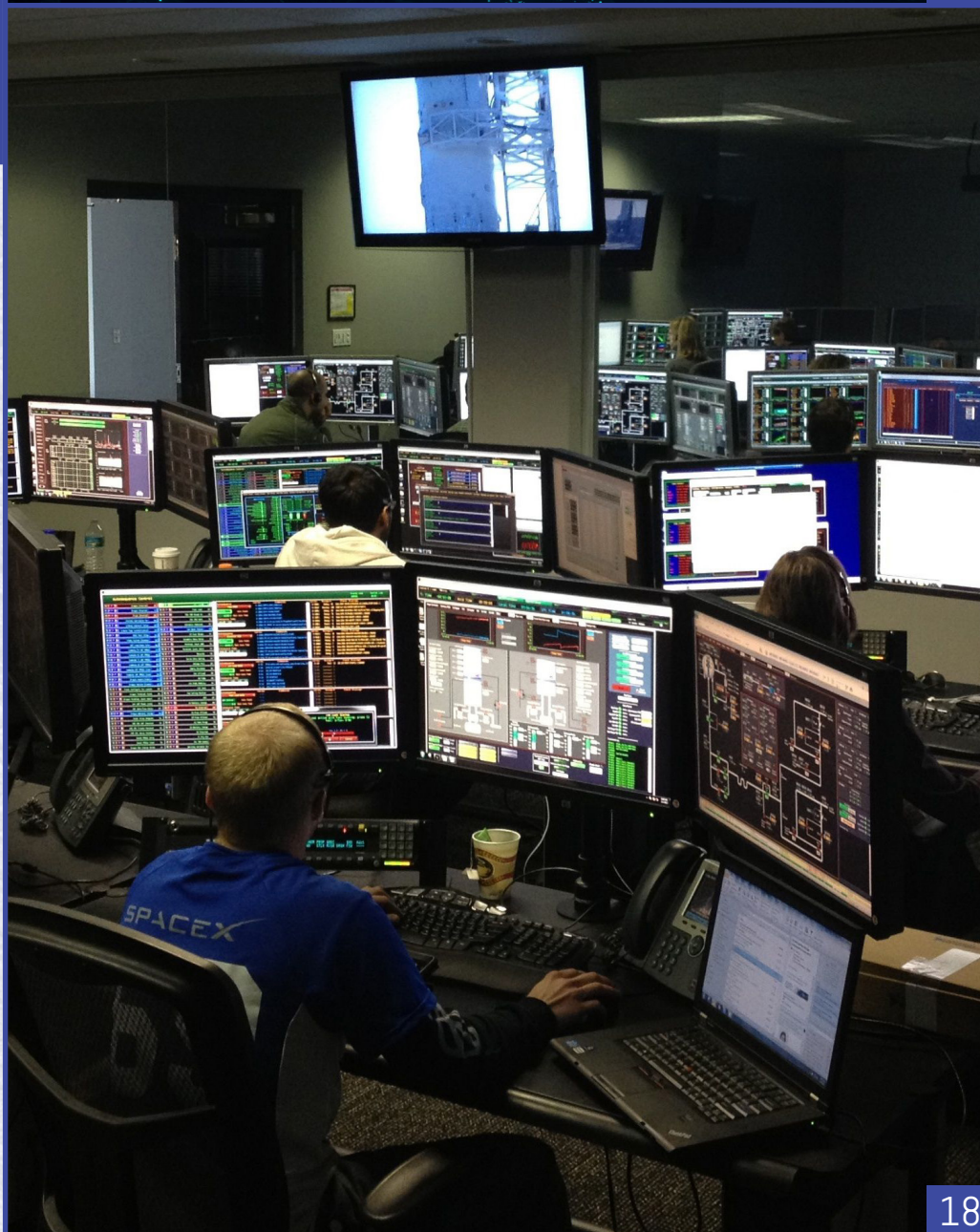
Jenn Blakesley

jenn@industrialnews.co.uk

Copyright is the contents of Industrial News, its sub-brand magazines, Industrial Views special reports, its website and newsletters is the property of the publisher. The publisher and the sponsors of the magazine are not responsible for the results of any actions or omissions taken on the basis of information contained within this publication.

Published in Birmingham, UK.

16



18

INNOVATION FROM SKY TO SEA

— by Jon Hughes, Editor, IN Defence

Farnborough 2026 opened at a point when demand for defence equipment had risen faster than the industrial base built to supply it. The flying programme drew the usual crowds, but inside the exhibition halls the discussion had very evidently moved on from what engineers could design to whether industry could build it in volume and keep it in service.

Autonomous aircraft and lower-cost interceptors featured prominently, although neither could be separated from the question of output. Governments want greater control over the systems they buy, particularly where upgrades and long-term support remain tied to an overseas supplier. Manufacturers are therefore being asked to increase production while dealing with skills shortages and supply chains that were never set up for sustained wartime demand.

The gap between prototype and production ran through much of the show. A design that cannot enter serial manufacture quickly, or cannot be replaced once deployed, offers limited military value. Ukraine has made that weakness difficult to ignore, and procurement teams are now addressing it in contracts rather than leaving it for a future mobilisation plan.

Sovereignty also appeared in practical terms, rather than as a political slogan. Buyers are pressing for domestic work and the freedom to maintain equipment throughout its service life. International programmes will continue, but the terms are changing as governments become less willing to accept dependencies that could restrict them once operations begin.

While Farnborough kept its eyes on the skies, this issue is firmly fixed on another



frontier: the seas, and what lies beneath them.

The undersea domain carries many of the same industrial pressures without the spectacle. Equipment must work for long periods in places where access is difficult, and where failure may remain hidden until a cable, sensor, or platform stops working. Autonomous systems depend on reliable power, secure communications, and materials able to withstand depth, pressure, and corrosion.

Subsea infrastructure has also become a direct defence concern. Pipelines and data cables sit beyond

routine public view, yet damage can have national effects before anyone establishes whether the cause was accidental or hostile. Protecting them requires persistent surveillance and the means to respond before uncertainty becomes an excuse for delay.

The aircraft at Farnborough were built to be seen. Much of the capability examined in this issue is designed for the opposite condition, but industry will judge both by the same standard: whether they can be delivered when required.



AIRBUS AND DIEHL DEEPEN AIR DEFENCE PARTNERSHIP

Airbus Defence and Space and Diehl Defence have agreed to expand their cooperation on integrated air and missile defence, building on their work on the IRIS-T SLM ground-based air defence system.

Signed at ILA Berlin Air Show 2026, the agreement will explore product enhancements intended to improve capability, responsiveness, and interoperability. One proposal is a shared “battle lab” development environment, allowing both companies to test next-generation command-and-control functions alongside Diehl Defence’s launchers and effectors.

Airbus supplies the combat-proven command-and-control architecture used within IRIS-T SLM and SLS, while Diehl Defence leads the wider system, including launchers and interceptors. The partners said closer integration could support a scalable, networked defensive shield aligned with NATO and European Sky Shield Initiative requirements.

The systems have gained operational validation in Ukraine and have been adopted by Germany, Bulgaria, Denmark, Estonia, Latvia, Slovenia, Sweden, and Switzerland. The agreement deepens established cooperation across European air defence programmes.



FAM GROUP CONSOLIDATES AEROSPACE MANUFACTURING

FAM Group has launched in the South West, bringing three specialist engineering businesses under shared strategic leadership to support defence and aerospace programmes.

The investment and oversight group comprises TML Manufacturing, Surface Coating, and Precision Engineering. Rather than operating the businesses directly, FAM Group will support their growth, align quality and compliance standards, and enable collaboration on complex programmes requiring fabrication, machining, and certified finishing.

TML Manufacturing provides coded welding, CNC machining, laser cutting, fabrication, and finishing. Surface Coating operates a NADCAP-accredited facility specialising in wet painting, powder coating, and blasting, while Precision Engineering supports projects from prototype development through to volume production.

The combined offer is intended to reduce supplier management complexity for customers requiring traceable, compliant, UK-based production.

FAM Group plans to add further businesses and invest in new roles and apprenticeships. Managing director Ryan Hanger said the structure would give customers access to end-to-end capability while allowing each company to retain its specialist identity for customers across demanding, highly regulated engineering sectors.

The group will present its combined capabilities at Farnborough Airshow 2026.

600+ INVESTORS SET SIGHTS ON FARNBOROUGH'S NEW AEROSPACE FINANCE SUMMIT



Farnborough International Airshow launched a new Finance Summit at this year's show, bringing more than 600 investors and finance leaders together with aerospace, defence, space, cyber, and enabling-technology businesses.

Held within the Aerospace Global Forum, the summit connects industry with capital and provide investors with direct access to emerging projects, market intelligence, and business development opportunities. Organisers have identified participants from around 350 companies across investment banking, sovereign wealth, private equity, venture capital, fund

management, M&A, stock exchanges, consultancy, and export finance.

Attendees included representatives from Goldman Sachs, J.P. Morgan, Citigroup, Barclays, HSBC, Deutsche Bank, UBS, Blackstone, Carlyle, Mubadala, Qatar Investment Authority, Temasek, the British Business Bank, the London Stock Exchange, and UK Export Finance.

The programme included keynote sessions, panel discussions, roundtables, and dedicated networking, with a focus on linking finance organisations to global primes, established suppliers, and emerging start-ups.

Gareth Rogers, CEO of Farnborough International, said the summit was created in response to growing investor demand for "direct access to high-quality market insight, business development opportunities and emerging innovation across aerospace, defence and space."

The event emphasised investment as a more visible part of Farnborough International Airshow, while giving aerospace and defence companies a structured route to the relationships and funding needed to scale.



17TECH OPENS KYIV DEFENCE TECHNOLOGY R&D CENTRE



Finnish defence technology accelerator 17Tech is opening an R&D centre in Kyiv to help European startups test and refine products with Ukrainian soldiers, military units, and defence specialists.

The facility will give selected companies access to operational feedback, expert assessment, and realistic testing environments. Technologies that reach sufficient maturity may also be evaluated under front-line conditions, giving developers evidence of how systems perform beyond controlled demonstrations.

The centre will support 17Tech's next accelerator programme, which begins on 1 September 2026 and will operate across Finland and Ukraine. Seventeen early-stage companies will be selected from Finland and elsewhere in Europe.

Priority areas include drones and counter-drone systems, electronic warfare, sensors, artificial intelligence, robotics, autonomous systems, field logistics, protection technologies, communications, and software supporting military decision-making.

17Tech said the programme is designed to establish "mission-problem fit" before companies invest heavily in product development. Startups will first test whether the problem they intend to solve is operationally important and whether military users would adopt the proposed solution.

Products will then be assessed for usability, durability, reliability, maintainability, deployment requirements, and compatibility with existing military processes. Feedback from Ukrainian personnel will be used to identify weaknesses, remove unnecessary features, and set priorities for further development.

"In defence technology, an impressive demonstration is not enough," said Antti Kosunen, founder and CEO of 17Tech. "The product must solve a real problem, work in the intended environment and be usable by the people whose lives may depend on it."

The accelerator argues that Ukraine's rapidly changing battlefield has exposed the limits of conventional, multi-year defence development cycles. Drone tactics, electronic interference, countermeasures, and operational requirements can change within months, making continuous access to military users increasingly important.

17Tech currently has 12 defence technology companies in its portfolio. Its new intake is aimed at startups with concepts, prototypes, or existing dual-use products requiring operational validation.

Successful participants are expected to leave with clearer use cases, stronger technical evidence, and greater credibility with defence customers, NATO markets, investors, and international partners.



Successful participants are expected to leave with clearer use cases, stronger technical evidence, and greater credibility with defence customers, NATO markets, investors, and international partners.

Applications are open, with 17Tech seeking scalable, cost-effective technologies that can be manufactured reliably for demanding operational environments.

Across Ukraine's extended frontline, the conflict remains dominated by attrition, dense drone activity, dispersed strikes, and rapid tactical adaptation rather than decisive manoeuvre. Russian forces continue to combine missile attacks, one-way attack drones, electronic warfare, and sustained pressure on

multiple sectors, while Ukrainian units rely heavily on unmanned systems, networked intelligence, and locally adapted technologies to hold ground and disrupt advances.

The effects extend well beyond military positions, with long-range strikes continuing to hit energy infrastructure, transport links, and urban areas, while short-range drones have become an increasingly persistent threat to troops and civilians near the front. Systems that perform reliably in controlled trials can quickly prove ineffective once exposed to jamming, disrupted communications, limited maintenance capacity, difficult terrain, and countermeasures that evolve within weeks.

This operating environment gives 17Tech's

Kyiv centre a clear purpose and urgency. Direct access to Ukrainian users can expose weak assumptions before companies commit to lengthy certification, production, or procurement programmes, while repeated testing allows developers to refine usability, repairability, and resilience against electronic attack.

For European startups, the value lies in shortening the distance between prototype and operational relevance. Products that can be adapted quickly, manufactured economically, and maintained under pressure are more likely to meet real military requirements than technologies developed in isolation from the battlefield.





UNDERSEA CABLE **THREATS** WHY SPACE IS THE FUTURE OF CRITICAL CONNECTIVITY

Tudor Williams, CTO at Filtronic, examines the growing threats facing undersea cable infrastructure — and argues that space-based connectivity, supported by advanced RF technology, must become a central pillar of resilient UK defence and critical communications.



Undersea cables are the backbone of the global digital economy, carrying more than 95% of international data traffic and supporting everything from financial markets and defence communications to cloud services and government operations. Yet as reliance on this infrastructure intensifies, so too do the risks. Incidents of cable damage, whether accidental or deliberate - are rising sharply, exposing a critical vulnerability in the world's connectivity architecture.

For the UK, the stakes are particularly high. As an island nation, over 90% of daily internet traffic travels via subsea cables. This single layer of infrastructure underpins national security, economic stability and essential public services. Any disruption, whether caused by natural events, human error or hostile activity has the potential to create far-reaching consequences across multiple sectors.

Rising risks beneath the surface

Traditionally, most subsea cable faults have been accidental. Fishing activity, shipping anchors and general maritime operations remain common causes of damage. Natural hazards, including seismic activity and underwater landslides, further contribute to cable breaks, often with little warning and

lengthy repair times.

However, the threat landscape is evolving. Growing geopolitical tension and increased undersea activity have heightened concerns around deliberate interference. Reports of foreign adversaries monitoring and potentially targeting subsea infrastructure have elevated these assets to a matter of strategic importance.

Their relative inaccessibility which was once seen as a protective factor now presents a challenge, as monitoring and defending vast stretches of seabed infrastructure is complex and resource-intensive.

The result is a convergence of risks that exposes a fundamental weakness. It is no longer viable to rely on a single, physically vulnerable layer of connectivity.

From vulnerability to resilience

At Filtronic, we believe this challenge demands a fundamental shift in how resilience is baked into communications infrastructure. Space-based connectivity is rapidly moving from a contingency solution to a strategic necessity.

Satellite communications offer an independent and geographically diverse alternative to subsea networks. By bypassing

the ocean floor, they eliminate many of the physical vulnerabilities associated with cable infrastructure. In the event of a disruption whether that be from a cyber-physical attack, natural disaster or geopolitical conflict, satellite networks can maintain critical communications and ensure operational continuity.

Governments and operators are increasingly investing in space-based capabilities to strengthen resilience. Their priorities are clear:

- ▶ Providing redundancy for critical national and defence communications
- ▶ Ensuring continuity during geopolitical crises or coordinated attacks.
- ▶ Enabling rapid failover and recovery when subsea networks are disrupted.

Low Earth Orbit (LEO) satellite constellations are accelerating this transition. Offering lower latency and higher capacity than traditional satellite systems, they are redefining what space-based connectivity can deliver. Increasingly, these networks are not just complementary to terrestrial infrastructure but are becoming integral to future communication architectures.



Enabling the next generation with RF technology

The effectiveness of space-based connectivity depends on the performance of the technologies that power it, particularly radio frequency (RF) systems. As demand for high-capacity, secure and reliable satellite communications grow, advanced RF technology is playing a central role in enabling next-generation networks.

At Filtronic, we specialise in high-performance RF solutions that support the delivery of robust, high-throughput satellite links. These technologies are critical in ensuring that data can be transmitted efficiently, securely and reliably between ground infrastructure and space-based assets.

Advanced RF capabilities enable:

- ▶ **High bandwidth data transmission**, supporting increasingly data-intensive applications.
- ▶ **Secure and resilient communications**, with protection against interference and signal disruption.
- ▶ **Scalable network architectures**, allowing operators to expand capacity as demand evolves.

As satellite systems move into higher frequencies like Ka-band, RF performance becomes more critical. These bands offer higher capacity but are more affected by signal loss and atmospheric conditions, requiring precise engineering to ensure reliable operation.



A strategic imperative

For the UK, the case for space-based resilience is clear. The combination of heavy reliance on subsea cables and an increasingly complex threat environment demands a more diversified approach to connectivity.

Satellite infrastructure provides a vital second layer, enhancing resilience, protecting critical services and reducing exposure to single points of failure. This is not about replacing subsea cables, but complementing them within a multi-layered ecosystem where

redundancy limits risk.

As investment grows, collaboration between governments, operators and technology providers will be essential, along with interoperability between terrestrial and space-based systems to ensure seamless connectivity.

In a world where outages can cost billions, resilience is a strategic necessity. The vulnerabilities of subsea infrastructure highlight the need for a more diversified approach. At Filtronic, we believe space-based connectivity, combined with advanced RF technology, will enable faster, more

secure and resilient networks. As threats evolve, the priority is no longer whether to invest, but how quickly space-based solutions can be scaled.



SUBSEA SABOTAGE

UNDERWATER, UNDERMINED AND UNDER SIEGE

David Hunt, partner at global law firm Boies Schiller Flexner, examines the growing threat of subsea cable sabotage — and asks what international law permits the UK to do when hostile interference falls short of a conventional armed attack.



“We see you. We see your activity over our cables and our pipelines, and you should know that any attempt to damage them will not be tolerated and will have serious consequences.”

Those were the words of UK Defence Secretary John Healey, directed at Russian President Vladimir Putin during a Downing Street press conference earlier this year. The statement followed reports that Russian submarines had conducted surveillance and mapping operations targeting subsea cables and pipelines in the North Atlantic.

Mr Healey’s concerns are unsurprising. Subsea cables are increasingly vulnerable to deliberate damage. The cables are made of thin strands of glass fibres surrounding a metal core that lie across the ocean floor and which run far outside national waters. Sabotaging subsea cables can cause major disruption, the UK relies on subsea cables for its internet system, the cables carry data that power the UK economy, everyday communications and critical services.

However, what “serious consequences” does international law permit the UK to impose?

The legal regime governing subsea cables reflects its nineteenth-century origins. The 1884 Convention for the Protection of Submarine Telegraph Cables, to which a limited number of maritime States are party, requires State parties to criminalise breaking or injuring submarine cables either wilfully or by culpable negligence (Article II). Similarly, the UN Convention on the Law of the Sea 1982 requires State parties to enact criminal legislation prohibiting the wilful or culpably negligent damaging of undersea cables (Article 113).

However, both conventions suffer from the same deficiencies. States do not enjoy universal jurisdiction over the severing of subsea cables. As a general principle on the high seas, jurisdiction to prosecute rests solely with the flag State, that is, the State under which the vessel responsible for the damage is registered. Neither convention imposes an express international law obligation on States not to deliberately damage or interfere



with subsea cables. Further, many states are either not party to the relevant agreements or have failed to implement their requirements.

Ultimately, both Conventions are ill equipped to deal with the present state of increasing hybrid warfare in which States intentionally threaten subsea cables to undermine other states' security or economy. That implicates the international law prohibiting the use of force and interference in a state's sovereign domain.

Article 2(4) of the UN Charter prohibits States from using force against the territorial integrity or political independence of another State. Meanwhile, customary international law prohibits a state from coercively interfering in the sovereign affairs of another state.

The main problem lies in regulating the remedies a state can take in response to such intentional damage. International law allows a state to use force in self-defence but that right is only triggered under Article 51 of the UN Convention if

an "armed attack occurs". Article 51 was written when international law contemplated so-called "Kinetic attacks" – direct physical violence against the state.

In the context of cyber attacks, some states, the UK among them, have said that they will regard actions having effects equivalent to a kinetic attack (i.e. significant physical harm to life or property) as potentially engaging the Article 51 right of self defence. In the same way as a cyber attack can cause serious physical harm, so could cutting cables by disrupting key information and safety systems.

Importantly, the right of self-defence is limited – the defending state must only take steps that are proportionate. For example, if Russia planned to use uncrewed submarines to damage a cable, causing serious physical damage to the UK, the UK would be entitled to use force to prevent it doing so. But the UK would not be entitled, for example, to attack Russian civilian vessels by way of retaliation.

Given the escalatory risk associated with such steps and the difficulty of showing a clear intention to engage in an armed attack, it is far more likely that the UK will rely on its other international law rights, which do not require there to have been an armed attack. For example, in the event of an interference in its sovereignty short of an armed attack, the UK would be entitled to engage in retorsion (i.e. internationally lawful but hostile steps, such as the imposition of sanctions or the expulsion of diplomats) or by taking countermeasures (suspending its treaty obligations to the hostile state).

Such legal niceties can seem footling at a time of ever-increasing hostility. But the risks associated with not having a clear and principled doctrine for the limited use of force are all the greater in such unsettled times. Any steps by Britain to make clear its red lines are to be welcomed.



HIGH RELIABILITY SEMICONDUCTORS BENEATH THE SURFACE



Ross Turnbull, Director of Business Development at custom IC specialist Swindon Silicon Systems, explores what high reliability means in maritime defence electronics.



Modern naval capability depends on electronics that can perform predictably for years, whether installed in shipboard mission systems or sealed into subsea payloads where recovery is slow and expensive.

This timescale matters. When HMS Astute entered a mid-life maintenance period, the Royal Navy noted that the submarine had “completed 15 years’ continuous service”. Reliability is not only about meeting an electrical specification on day one, but also about maintaining stable behaviour over the service life.

Maritime environments create failure mechanisms that are easy to underestimate in early design. During storage, deck handling and shipboard operation, persistent humidity and salt contamination can accelerate corrosion and increase the risk of conductive contamination. The effect is often gradual, leading to leakage drift, rising contact resistance and connectors that become intermittent under vibration.

Temperature cycling and mechanical loading add further stress. Ambient conditions shift, equipment heat loads vary and assemblies expand and contract across interfaces, solder joints and printed circuit board materials. Vibration from propulsion systems and sea state can be continuous, while handling and launch or recovery can introduce discrete shock events. If parts of an enclosure or board are excited near their natural frequencies, strain can be amplified at interconnects and component terminations.

Subsea deployment adds hydrostatic pressure, sealing challenges and long-term ingress risk. Electronics are typically installed in pressure housings or encapsulated assemblies where access is restricted by design. Once deployed, the cost of failure can extend beyond replacement hardware to mission disruption and requalification work.

Reliability extends beyond silicon

Because many problems are driven by interactions, a narrow focus on silicon selection can overlook the main causes of field issues. In practice, reliability is often won or lost at boundaries, such as where a package meets the board or where a connector meets a harness. These interfaces are shaped by materials, thermal behaviour and process control, and they often determine whether performance remains stable when conditions change.

This is why high reliability tends to come from early alignment across design, packaging, board layout, manufacturing and qualification. A device may be electrically suitable yet still become the weak link if its package is moisture sensitive, finishes and cleanliness controls are not matched to long-term exposure, or mounting choices concentrate stress on solder joints. Validating those choices against a realistic operating profile, rather than relying on generic assumptions, is often what separates a robust design from one that slowly loses margin.

Where ASICs add value

Integrated circuits sit at the centre of modern naval and subsea electronics, defining how signals

are conditioned, how power is managed and how data moves through the system. Application-specific integrated circuits (ASICs) can support maritime reliability goals by improving integration and lifecycle control.

Consolidating functions can reduce component count and interfaces, lower the number of potential failure points and simplify board-level interconnects. In sealed subsea housings, power and heat are limiting factors, so tailoring functionality to the operating envelope can simplify thermal management and support long-term stability. For sensor-rich payloads, integrating analogue front ends, data conversion and control in a single characterised device can improve build-to-build consistency.

In defence programmes, lifecycle planning is part of reliability rather than a procurement concern. Naval systems may remain in service for decades, while many commercial components have far shorter lifecycles. When parts change or reach end of life, the impact is not limited to procurement. It can trigger redesign, requalification and documentation updates. A managed ASIC programme can help by enabling controlled revisions and clear equivalence

documentation, reducing disruption as supply chains evolve.

Verification is most effective when it reflects the mission profile rather than a generic checklist. That principle is consistent with established qualification practice. MIL-STD-810H is intended to tailor environmental design and test criteria to the conditions a material item is likely to encounter throughout its service life.

A useful approach is to map the journey the electronics will experience, from storage and transit through to operation and refit, then select tests and limits that mirror those stresses. That includes power cycling and thermal gradients inside sealed enclosures, as well as defining acceptable drift over time.

Naval and subsea defence systems are becoming more sensor-rich and more dependent on edge processing. That trend increases the premium on predictable, long-life electronics. The key question is whether the complete electronics solution, including its IC strategy, can remain dependable and supportable for the life of the platform in the environments it will actually face.



AS9100 CERTIFICATION EXPLAINED:

WHAT IT INVOLVES AND WHY IT MATTERS

Jon Fielding, Managing Director at Apricorn, explains why AS9100 certification has become a commercial and operational prerequisite across aerospace and defence — and how secure data management, traceability, and continuous improvement will shape organisations' readiness for the transition to IA9100.



In sectors such as aerospace and defence, there is no room for risk. Best practices have become non-negotiable, with organisations redlining those partners and suppliers that haven't achieved highly specific criteria.

AS9100 is one certification that is typically required as a prerequisite for aerospace and defense contracts. Developed by the International Aerospace Quality Group (IAQA), it is the international quality management system (QMS) standard for the aerospace sector, building on ISO 9001 by introducing additional sector-relevant requirements. Among these are greater expectations in relation to risk management, supply chain management, configuration controls, product traceability and corrective actions.

From manufacturers to government agencies, AS9100 is broadly applicable to a variety of organisations, with certification depending not only on the quality of aerospace products and solutions, but also a firm's ability to demonstrate robust data management and security protocols.

Here, the standard itself provides a specific QMS framework to help organisations develop stringent security and data controls across everything from document protection to electronic record security, serving as a guideline for the establishment for best practices.

Realising competitive advantages

With many aerospace and defense firms automatically rejecting potential contracts with partners that haven't been AS9100 certified, alignment with the standard can be a critical competitive differentiator, opening the door to customers and opportunities that otherwise wouldn't be available.

The benefits go beyond customer confidence, however. AS9100 certified companies will also stand to reap the rewards of adopting best practices, which can serve as the catalyst for operational optimisation. By establishing effective quality management systems, companies will more easily be able to identify internal

inefficiencies and make incremental improvements that can increase productivity, reduce errors, and lower costs over time.

How to prepare for the AS9100 certification audit

The first step towards AS9100 certification involves ensuring awareness and buy-in to the standards requirements across the organisation. From the motivation for certifying and risks that it helps to mitigate, to the practical realities such as the secure and reliable management of data, everyone within the company needs to understand the reasons for aligning with these best practices, and the precise controls they must adhere to.

From here, organisations can then begin to see how their current policies and processes compare to the standard, identifying areas that are already aligned, as well as areas where changes will be needed. This might involve improvements to data storage and security, for example, which directly meet AS9100's requirements around configuration control and traceability.

Once any gaps have been identified, the next step is to set measurable goals and realistic timelines in addressing them, adapting operations to fit AS9100's requirements. And finally, once the necessary

changes have been made – complete with supporting documentation that can guide processes and verify compliance – firms can look to schedule in their certification audit with a qualified certification body.

The audit itself will be carried out in two phases. The certification body will begin by reviewing documentation, with this then being followed by an on-site assessment.

Continuous improvement and proactivity ahead of IA9100

Becoming AS9100 certified is a key milestone, yet it's important to recognise that maintaining accreditation will require firms to adopt a culture of continuous improvement, assessing and adapting their practices, and aligning with the standards evolving requirements. This is because AS9100 will soon transition to IA9100, which is expected to be released in 2026 as the next-generation international quality management standard for the aviation, space, and defense industries.

The aim of IA9100 is to further ensure compliance aligns with modern operational realities. While the details are yet to be confirmed, the IAQG has already hinted that the new standard could include

changes relating to product safety, quality culture and organisational accountability, stricter controls on counterfeit parts and supplier management, and greater expectations around the integrity, control, and traceability of digital information.

Once IA9100 comes into effect, organisations will have the usual three years to meet the new requirements. However, this does not mean that companies should kick the certification can down the road. In an industry in which contracts demand best practice alignment, being proactive will likely pay dividends.

Trust, traceability, and operational assurance are non-negotiable in the defence and aerospace industries. Therefore, those companies that invest early in quality management system improvements and secure, disciplined information management will gain a competitive advantage, proving themselves to be reliable partners actively embracing best practices.



GNSS RESILIENCE

THE SECURITY IMPERATIVE OF MODERN WARFARE

Plextek's Professor Aled Catherall examines how GNSS disruption has become a weapon of hybrid warfare — and why layered, assured Position, Navigation, and Timing capabilities are now essential to protecting military operations, critical infrastructure, and economic stability.



High-profile global gatherings bring renewed scrutiny to our collective dependence on Global Navigation Satellite Systems (GNSS). This dependence underpins everything from aviation safety and emergency response to communications, finance and energy infrastructure. Yet the degradation of GNSS is far easier to achieve than many assume, with potentially severe consequences.

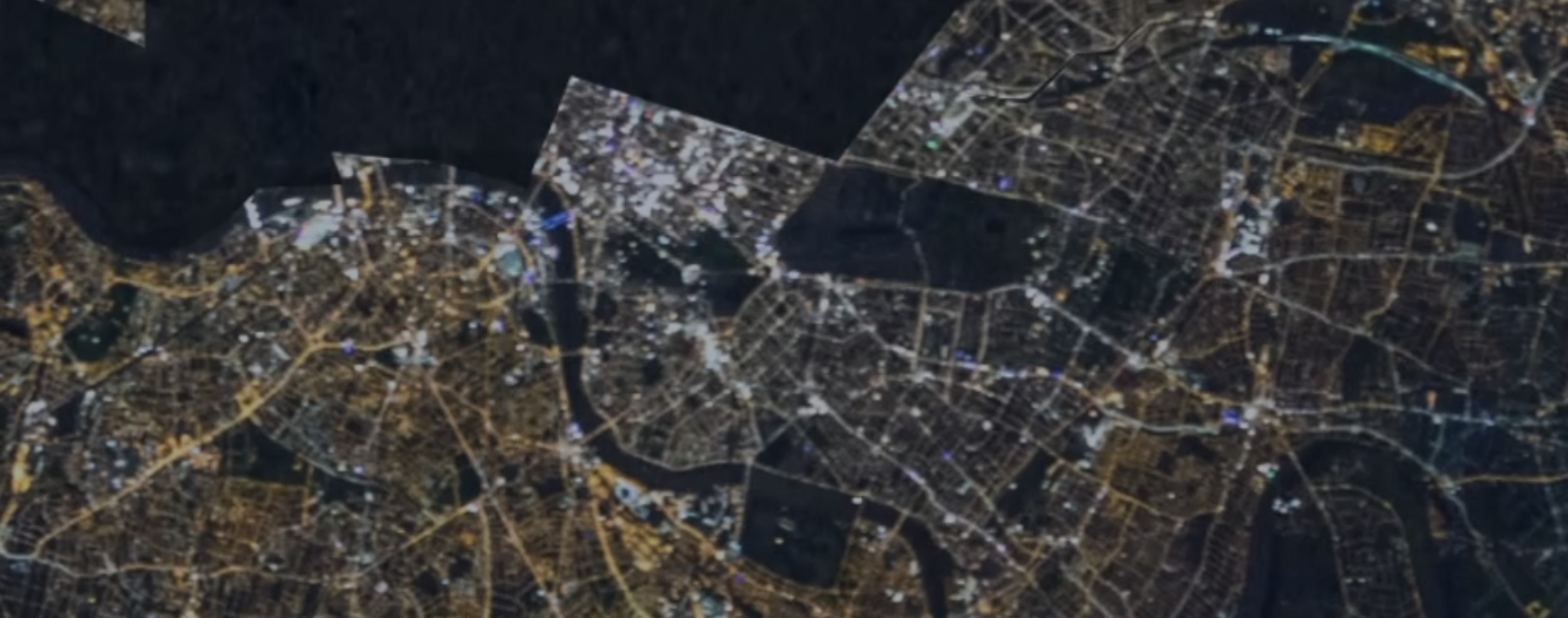
While deliberate GNSS jamming is typically illegal, disruption can arise from a broad range of sources. These include malicious interference, as well as natural phenomena like solar flares or technical anomalies within satellite constellations. However, it seems the problem is on the rise.

According to IATA, GNSS interference is impacting over 5% of commercial flights within Europe, with a 220% increase in signal loss events between 2021 and 2024. Recent incidents, such as the jamming

that affected European Commission President Ursula von der Leyen's aircraft, highlight the very real risks of malicious attacks.

However, although GNSS is widely recognised for its role in positioning and navigation, its equally critical function in delivering precise timing is often overlooked. Sub-microsecond timing accuracy is essential for modern society, enabling synchronised power grids, resilient broadcast and cellular networks, accurate financial trade timestamping and reliable industrial automation. And, systems that rely exclusively on GNSS for timing are increasingly vulnerable to disruption, whether through accidental outages or deliberate interference.

With global leaders gathering in one location throughout the year for major events like the World Economic Forum, G20, NATO Summit and COP31, the potential for targeted disruption may be even greater.



A silent weapon in hybrid conflict

In response, attention is increasingly turning to the need for real-time detection of GNSS disruptions, using layered technologies to assure Position, Navigation and Timing (PNT) data across both autonomous and crewed systems. By continuously assessing GNSS signal integrity, comparing it against multiple, diverse data sources, such approaches provide early warning of jamming, spoofing and other anomalies before they escalate into operational or safety-critical failures. When GNSS disruption occurs, the ability to draw on a range of other data sources, such as inertial sensors, atomic clocks and other complementary technologies provides resilience and the ability to continue operating in the absence of reliable and trustworthy GNSS.

This capability is already strengthening the ability of global armed forces to monitor, secure, and protect national airspace and

critical PNT infrastructure during major international events. By enhancing situational awareness, it enables faster anomaly detection, more accurate threat assessment, and coordinated protective measures across both the physical and cyber domains, a crucial requirement when safeguarding sensitive airspace and high-profile global gatherings.

If GNSS resilience were not robust, the repercussions could be severe. Disruption to timing and navigation signals can affect everything from aircraft routing and air traffic control coordination to military communications, surveillance systems, and emergency response operations. In a worst-case scenario, compromised GNSS could create confusion in crowded airspace, delay critical decision-making, or increase the risk of misidentifying threats during already heightened security conditions.

In such circumstances, established protocols and emergency response

procedures would be activated immediately. Armed Forces and aviation authorities would shift to contingency navigation and timing systems, such as inertial navigation, terrestrial-based backups, or alternative secure PNT sources. Airspace restrictions could be rapidly enforced, with flights rerouted or grounded depending on the severity of the disruption. Simultaneously, cyber and electronic warfare teams would work to identify the source of interference, assess whether it is accidental or hostile, and deploy countermeasures to contain the threat.

This coordinated response, spanning defence, aviation, and cybersecurity stakeholders, is essential to maintaining operational continuity, protecting civilian safety, and ensuring that major international events remain secure even in the face of sophisticated GNSS disruption attempts.





CYBER WARFARE IS NOT THE ONLY DIGITAL BATTLEFRONT

Defence production depends on more than protected platforms. It depends on secure suppliers, trusted software, resilient factories, protected engineering data, cloud assurance, identity control, and the ability to keep operating under pressure.

Cyber Insider follows the cyber issues that threaten organisations of all types and sizes — ransomware, AI security, supply chain exposure, cloud dependency, regulation, incident response, and operational resilience.

Go deeper with reporting and analysis on the issues shaping cyber risk across UK and European organisations.

cyberinsider.co.uk

**CYBER
INSIDER**

The art of (modern) war

Governments are now actively modelling and stress-testing the economic consequences of GNSS outages, recognising the sheer scale of the risk. The UK government, for example, has estimated that a nationwide GNSS disruption lasting just 24 hours would cost the economy more than £1.4 billion, with similar, or even greater, impacts likely across other highly digitised nations. For transport systems in particular, GNSS degradation can be profoundly disruptive, affecting aircraft navigation, maritime operations, logistics supply chains and road networks alike, and exposing critical national infrastructure to cascading failures that extend far beyond the initial outage.

What makes this risk even more urgent is the changing nature of warfare and global security. Defence spending is rising sharply worldwide, not solely because of traditional military threats, but because conflict has evolved into a far more complex arena. Modern warfare is increasingly fought through electronic disruption, cyber interference, and space-based vulnerabilities rather than the trench-style confrontations of the past. GNSS has become a strategic target in this

new landscape: jamming, spoofing and signal denial are now recognised tools of hybrid warfare, capable of undermining both civilian stability and military readiness without a single shot being fired.

This shift is driving significant investment into resilience measures, as nations seek to reduce dependence on any single source of positioning, navigation and timing. The future will likely see a layered approach to PNT security, combining alternative satellite systems, terrestrial backups, inertial navigation, and advanced monitoring technologies that can detect anomalies in real time. Overcoming the threat will depend not only on technical innovation, but on coordinated defence strategies that treat GNSS resilience as a core pillar of national security.

Ultimately, as reliance on GNSS continues to deepen, ensuring its protection will remain a defining challenge of modern security and economic stability.

At major international gatherings such as the recent World Economic Forum, where global leaders convene with differing policies and agendas, the issue of GNSS resilience raises an important question: is this a universal priority, or does each country approach it differently?

In practice, while the vulnerability is shared globally, national responses vary. Some nations invest heavily in sovereign navigation systems or independent backups, while others rely on alliances and shared infrastructure. But with the interconnected nature of global transport, finance and communications means that GNSS disruption is rarely confined by borders. Resilience, therefore, is increasingly becoming a collective imperative, one where cooperation, standards, and shared situational awareness may prove just as important as national capability.

However, despite growing awareness and debate, significant vulnerabilities remain. As reliance on satellite-derived PNT continues to deepen, the question is no longer whether GNSS disruption will occur, but how societies can build resilience against it, and how trusted civilian-military technology partnerships can help safeguard critical events, infrastructure and economies in an increasingly contested navigation environment.



AI AS THE ADVERSARY

IS DEFENCE DOING ENOUGH TO COMBAT MILITARY-ENABLED AI?

Rob Demain, CEO of e2e-assure, examines how military-enabled AI is accelerating the cyber threat landscape — and argues that sovereign, AI-powered defence capabilities will be critical if the UK is to counter adversaries operating at machine speed and scale.



When Anthropic went public with Claude Mythos Preview, an AI with supposedly unprecedented abilities, and Project Glasswing, which restricts its use to a selection of US companies, governments were understandably rattled. That's because the technology could pave the way for nation state actors to train their own specialised models on decades of accumulated offensive cyber tradecraft and apply that knowledge at machine speed and scale, so these frontier AI models pose an unprecedented threat.

The ability of Mythos to discover, combine and exploit vulnerabilities is the tip of the iceberg. What if a nation-state AI trained could target critical national infrastructure (CNI)? Or carry out culturally-specific social engineering and disinformation campaigns against target populations? Or economic warfare through systematic market manipulation? As Richard Horne, CEO of the National Cyber Security Centre (NCSC) recently warned, cyber operations are now integral

to warfare making cybersecurity the home front.

In a bid to ascertain the extent of the threat, the National Cyber Force which supports the armed forces and foreign policy, and its parent agency, GCHQ, are working with the AI Safety Institute (AIS), a state-funded AI research centre, to evaluate Mythos. AISI, which has been tracking AI development since 2023, came to the conclusion that frontier model capabilities are now doubling every four months, compared to every 8 months previously.



Added impetus

But to add fuel to the fire, there's also much debate over whether Mythos does surpass current AI capabilities. Research by AISLE found it was possible to identify the same FreeBSD exploit detected by Mythos using smaller, open-source models for just \$0.11 per million tokens, refuting the assertion that such attacks are limited to frontier models. That suggests nation state actors don't need to wait to get their hands on a frontier model but could instead use these models locally over consumer hardware.

Mythos has, however, added a sense of urgency to the government's initiatives. In quick succession we saw the launch of the £500 million Sovereign AI Fund to support homegrown AI startups followed by calls for AI and UKPLC to bolster national cyber defence capabilities and develop a 'National Cyber Shield' by Security minister Dan Jarvis.

Developing a sovereign AI defence capability is key to the UK becoming not an 'AI taker' but an 'AI maker', according to Science and Technology Minister, Liz Kendall. That's because all major frontier AI organisations are currently US-based. Not only does this present a troubling dynamic given fraying international relations but it also has practical implications. Cyber threats targeting UK financial systems or CNI may have different characteristics,

motivations or techniques than those targeting US assets. Yet the defensive AI being developed by US AI companies is primarily trained on American threat landscapes and optimised for US operational environments rather than being tuned to UK needs.

Prioritising sovereignty

The drive for AI sovereignty is not at odds with previous strategy, however. While the Defence Artificial Intelligence Centre (DAIC), which aims to accelerate the adoption of AI in military defence, has predominantly worked collaboratively with allies in testing new technologies, it has also sought opportunities with sovereign partners. DAIC says it will work with UK industry and academia to capitalise on UK AI leadership, so we could well see greater emphasis or even preference given to UK-based AI in the future.

Sovereign AI-powered cybersecurity solutions are also now being brought to market which can bolster home front defences. These utilise a deep understanding of the regional threat landscape, more agile development cycles that are unconstrained by international bureaucracy, and the ability to customise defensive AI for geopolitical contexts and adversaries. It's also a move that will see the democratisation of AI, so that rather than being

dependent upon decisions made in Silicon Valley boardrooms or Washington policy meetings, we can steer our own ship. And it's a shift that will favour the brave, allowing innovative smaller firms to compete with larger cybersecurity providers constrained by legacy systems and technical debt.

AI will redefine both attack and defence. The question then remains whether the UK can adapt before adversarial AI outpaces human-centric defences. However, the advances made in cybersecurity have currently tipped the scales in our favour. The Security Operations Centre (SOC) has moved from artifact to behaviour-based detection, using AI-powered behavioural analysis to recognise attack patterns, autonomous threat hunting that doesn't rely on indicators of compromise or signature updates, behavioural baselining to detect deviations in real-time, and AI orchestration to reduce the time taken to conduct investigations. In fact, some SOCs now run entirely on sovereign AI infrastructure.

What this reveals is that we do have the talent and the capabilities to deploy our own AI defences, both militarily and domestically. Has enough been done to communicate the urgency of the issue and to boost uptake? That remains to be seen.



COULD UK MOTORSPORT BE THE DEFENCE SECTOR'S SECRET WEAPON?



Mark Ingram, technical director at Hewland Engineering, discusses the pivotal role of motorsport and automotive businesses in the defence sector of the future.



The UK's defence spending commitments have rarely been more visible than they are today. In the wake of the latest Strategic Defence Review, public and political attention has focused sharply on how quickly the nation can strengthen its military capabilities in an increasingly uncertain world.

Yet alongside the headlines, there has also been a clear note of frustration. As George Robertson, former Secretary General of NATO, has pointed out, ambition without timely delivery risks leaving us 'under prepared, under insured, under attack and not safe'.

The challenge is not simply about allocating funds. It is about deploying them effectively and, crucially, at pace. In real terms, this commitment should see annual defence spending increase from £66bn to £100bn. However, with the defence investment plan still awaiting

final sign-off by Kier Starmer, the need for positive action becomes vital.

Once budgets are confirmed, the UK must move swiftly to translate investment into operational capability. This is where an often-overlooked national asset comes into sharp focus: the UK's world-leading motorsport sector.

Harnessing the 'motorsport mantra'

Motorsport is built on three pillars that are directly transferable to defence: pace, precision and execution. In racing, there is no room for delay. Components must be designed, manufactured, tested and deployed within extremely tight timelines, often measured in weeks rather than months or years.



PUT YOUR BRAND IN FRONT OF DEFENCE'S DECISION MAKERS



Advertise in future editions
of IN Defence.

Contact
advertising@indefencemag.com

The industry thrives under pressure, delivering complex engineering solutions at speed without compromising on quality or reliability.

Equally important is precision. Motorsport engineering operates at the highest levels of performance, where marginal gains can determine success or failure. This relentless pursuit of optimisation has driven innovation in materials, manufacturing processes and system integration – capabilities that are directly applicable to modern defence requirements.

Finally, there is execution. Motorsport organisations are experts in coordinating multidisciplinary teams, managing supply chains and delivering against immovable deadlines. These are not theoretical strengths; they are proven capabilities, demonstrated repeatedly on the global stage. It is no coincidence that the Strategic Defence Review itself highlights the potential role of motorsport in supporting the UK's defence ambitions, recognising the sector's ability to accelerate innovation and delivery.

At Hewland Engineering, we have seen firsthand how these strengths can be applied beyond the racetrack. While our heritage lies in high-performance transmission systems for motorsport, in recent years we have successfully pivoted into adjacent sectors, including defence and advanced air mobility.

A key milestone in this transition has been achieving AS9100 certification, the internationally recognised quality standard for aerospace and defence manufacturing. This accreditation reflects not only our technical capabilities but also our commitment to rigorous processes, traceability and continuous improvements – all essential requirements in defence applications.

Our experience now spans a diverse range of projects, from supporting the development of electric vertical take-off and landing (eVTOL) aircraft to contributing to advanced land-based vehicle programmes. These initiatives

demand the same core competencies that underpin motorsport success. Rapid development cycles, high-performance engineering and robust system integration.

Central to this capability is our investment in test and validation. We recognise that in both motorsport and defence, performance on paper is not enough. Systems must be proven under real-world conditions before they are deployed. To support this, we have invested £1.5m in a new test facility in Warwickshire, designed to enhance our ability to validate complex transmission systems.

At the heart of this facility is our 3E test rig, which comprises one input motor and two absorber motors. This facility is incredibly configurable and will support all motorsport transaxle configurations in 2WD mode. This capability only applies to in-line transmissions (north-south / 1 input & 1 output) and would be beneficial to support loaded transmission testing on a gradient, such as hill climb evaluations.



This sophisticated platform has significant application potential in defence, enabling us to simulate operating conditions and assess performance with a high degree of accuracy. This capability allows us to identify and address potential design flaws early in the development process, long before a system reaches full production.

The benefits are significant. By validating designs at an early stage, we can reduce development times, improve overall vehicle performance and minimise the risk of costly redesigns later in the programme. Just as importantly, this approach supports one of the most critical objectives in defence projects: delivering on

schedule.

This emphasis on testing and validation is a direct reflection of motorsport's DNA. In racing, there is no substitute for real-world performance data. The same principle applies in defence, where reliability and readiness are paramount. By bringing this mindset to new sectors, companies like ours can help bridge the gap between concept and capability.

Looking ahead, the opportunity for the UK is clear. The motorsport sector combines a unique blend of engineering excellence, agility and a "can-do" attitude that is ideally suited to the demands of modern defence. It is an industry that is used to solving complex problems

quickly, adapting to changing requirements and delivering results under pressure.

If the UK is serious about building a world-class defence infrastructure, it should look closely at the capabilities already on its doorstep. Motorsport is not just a source of national pride; it is a strategic asset. With the right support and collaboration, it has the potential to play a pivotal role in strengthening the country's defence capabilities—quickly, effectively and at scale.

For more information about Hewland Engineering, or its experience in the defence and aerospace sectors, visit www.hewland.com.



FUSION, NOT CONFUSSION, IN REVITALISED BORDER SECURITY



David Janson, VP EMEA at Fivecast, examines how AI-enabled open-source intelligence and cross-agency data fusion are reshaping border security — and why effective deployment must combine faster threat detection with human judgement, explainability, and robust oversight.

Border security is no longer shaped only by what happens at a checkpoint or stretch of coastline. It is increasingly influenced by digital activity that may begin long before a traveller or vessel reaches a physical border.

This shift creates a challenge that is as much about interpretation as collection. Agencies do not simply need more information; they need the ability to bring relevant intelligence together in a way that supports faster and more defensible decisions under pressure. Open-source intelligence has an important role to play in that process, particularly when it can be fused with other sources

such as human intelligence and classified reporting. Without that fusion, analysts risk being left with disconnected feeds rather than a coherent picture.

The importance of that fusion is clear when looking at how cross-border threats now develop online. In August 2025, Home Office analysis found that approximately 80% of migrants arriving by small boat told officials they had used social media during their illegal journey to the UK, including to locate or communicate with an agent or facilitator linked to an organised crime group. That does not diminish the vulnerability of individuals making dangerous journeys. It does, however,

show how heavily criminal networks rely on online reach.

The National Crime Agency's (NCA's) work reinforces the point. During 2025, NCA activity triggered the removal of almost 10,700 accounts, pages and posts linked to organised immigration crime. The agency also reported that criminal actors often manage large numbers of accounts to maintain reach when others are removed. For analysts, the issue is not only the content itself but the speed with which networks can reappear in new forms.

Smuggling groups and traffickers can shift between mainstream platforms, closed channels

and hidden parts of the web with little warning. Their activity is often deliberately fragmented, with aliases, changing accounts and multilingual content used to obscure the relationships behind an operation. Human analysts remain central to the response because context and judgement cannot be automated. However, the scale and pace of relevant online information now exceed what manual methods can handle.

This is why border security teams need capabilities that do more than monitor online spaces. They need systems that help turn fragmented signals into intelligence that can be assessed, shared and acted on responsibly.

From collection to confidence

For government teams, an effective OSINT capability must support the intelligence cycle in a way that fits operational reality. Border security teams need tools that protect sensitive activity, work with established processes and help analysts move from discovery to assessment without unnecessary delay.

A useful system should help an analyst examine suspicious online activity, compare it with existing intelligence and understand whether it forms part of a wider pattern. It should also make collaboration easier across agencies where appropriate, while

maintaining strict control over access and handling. Secure integration with existing systems and clear data provenance are essential, because activity must be capable of review after the event.

Usability is just as important as technical capability. Advanced analytics lose value if frontline teams find them difficult to apply. Analysts should be able to configure risk indicators, review why material has been flagged and decide what further action is justified. They should not need to become data scientists before they can make effective use of AI-enabled tools.

AI should, therefore, be understood as a form of decision support in border security. It can accelerate discovery and help teams focus their expertise where risk appears greatest, while final assessments remain with experienced officers and analysts who can weigh intelligence against the wider context.

Ethical oversight also needs to be built into deployment. Responsible OSINT should be necessary and proportionate, with

clear limits linked to defined security risks. Strong governance, explainable outputs and auditable workflows help ensure that capability is matched by accountability.

Public trust depends on that discipline. Border agencies operate where security responsibilities and individual rights intersect. Confidence in their work requires assurance that powerful technology is being used lawfully, fairly and with respect for privacy. Security outcomes are stronger when agencies can show that their methods are controlled and proportionate.

As threats become more digitally enabled, intelligence fusion will become a defining capability for border security. Revitalised border security will depend on AI-enabled tools, sound tradecraft and human expertise working together. In high-pressure environments, this combination gives decision-makers the clarity they need without compromising trust.





IN CONVERSATION

JONATHON DIFFEY, ASL GRP

— ▼ —

As unmanned systems, electronic warfare, and sensor-led targeting reshape the maritime threat environment, naval protection is moving beyond armour for crews alone. Jonathon Diffey, Managing Director of ASL GRP, discusses the growing focus on safeguarding propulsion, control systems, and critical infrastructure.

— ▼ —



How are maritime threats changing what naval customers want from protection systems?

“Maritime threat environments are rapidly evolving. They are increasingly part of a wider transformation in modern warfare, where unmanned systems, electronic warfare and sensor-driven targeting are redefining operational risk across land, sea and air.

“All around the globe, drones have transitioned from experimental systems into deployed tools of modern conflict. Unmanned Aerial Vehicles (UAVs) and Unmanned Surface Vessels (USVs) are now routinely used in frontline operations, hybrid warfare environments and contested maritime zones. This has blurred the traditional boundary between maritime and land-based threats, with similar technologies, tactics and targeting logic now being applied across domains.

“As a result, naval customers are no longer asking only

how to withstand impact or blast, they are increasingly focused on how to maintain operational capability under attack and ultimately, protect their teams and assets, whilst keeping them moving. In practice, this means protecting propulsion, communications, control systems and mission-critical equipment.

“This shift is particularly visible in fast response craft, patrol boats and RIB platforms operating in high-risk environments. These vessels are often exposed and reliant on their propulsion systems.

“Traditional armoured vessels often have protection that is optimised against missiles, artillery or blast attacks but are less effective against small, manoeuvrable UAVs or low profile USVs – which can often evade detection, target critical infrastructure and deliver explosives remotely. Many UAVs can also now incorporate advanced electro-optical and infrared sensors, meaning heat signatures from engines, exhausts or crew areas can be rapidly detected and targeted.

“Thanks to advanced developments of protective materials and bespoke fabric make-ups, there are solutions at hand from specialist companies, which are designed on a bespoke basis to ensure maximum fit and protection. This includes solutions including Infra-Red Reflective (IRR) technology, and specialist

composite materials and conductive shielding layers which can protect against electromagnetic pulses (EMP), particularly for navigation systems, communications equipment and engine management systems.

Where do lightweight composite armour systems outperform traditional metal protection at sea?

“The fundamental advantage of lightweight composite armour systems lies in their ability to reconcile two competing demands: protection and performance.

“At sea, weight is not a secondary factor, it directly determines speed, fuel efficiency, range and manoeuvrability. Traditional metallic armour systems introduce significant challenges that often make them unsuitable for high-speed maritime platforms or small tactical craft.

“Composite systems by contrast, enable protection to be engineered as a performance-compatible material layer rather than an external structural burden. At ASL GRP, advanced multi-layer aramid and composite architectures are designed to meet NIJ IIIA and III+ ballistic standards, alongside V50 fragmentation resistance up to 600–700 m/s depending on configuration, while maintaining significantly reduced weight compared to metal alternatives.

“Where composites outperform metals most clearly, is in the flexibility of its integration. Instead of reinforcing entire vessel structures, protection can be retrofitted precisely where it is needed most – such as propulsion units, internal bulkheads or electronic compartments.

“Recently, we launched our ballistic outboard engine covers to directly respond to this emerging operational gap. Designed as removable, non-invasive composite armour systems, these removable engine covers protect exposed engine powerheads from ballistic and fragmentation threats while preserving full mobility and OEM functionality. Rather than attempting to armour an entire stern structure, protection is applied directly to the engine system itself in a modular, lightweight custom design. This allows operators to retain OEM integrity, maintain serviceability and adapt protection levels depending on threat exposure without permanently modifying the vessel, allowing mission flexibility and rapid deployment without additional significant weight onboard.

“Thanks to the modular approach, this is central to modern naval procurement planning, because it enables scalable protection without locking platforms into permanent weight penalties.”



Are operators putting more focus on protecting engines, controls, and mission-critical equipment, not just crews?

“Yes, and this is one of the most significant shifts in maritime survivability thinking.

“There is now widespread recognition that protecting personnel alone is insufficient if the vessel loses mobility or control capability particularly in high-risk environments. In modern asymmetric engagements, a vessel that cannot move is effectively mission-killed, regardless of crew survivability.

“As a result, propulsion systems, steering controls and onboard electronics are now considered critical protection priorities. This is particularly relevant for fast patrol craft and interception vessels, where outboard engines are both the primary propulsion source and one of the most exposed components in the entire platform.

“Similarly, pilot vessels are rarely equipped with hard armour or blast mitigation features and therefore in hostile environments, loss of propulsion, command systems or crew protection can quickly cascade into mission failure, vessel loss or worse. Therefore, protection in these instances must be lightweight, adaptable and effective without compromising speed, performance or operational flexibility.

“In recent months, our order books have seen an upturn in ballistic outboard engine cover sales – ASL GRP’s solution developed specifically to address engine and control vulnerability. By shielding the engine powerhead from ballistic and fragmentation threats, it helps preserve manoeuvrability even under partial damage scenarios and ongoing fire situations. In operational terms, this can provide the critical seconds needed to disengage, reposition, or complete a mission.”

What are the biggest challenges when integrating protection into fast boats and other complex platforms?

“Fast boats present one of the most challenging integration environments for any armour system. These platforms are designed for speed, agility and minimal displacement, meaning every additional kilogram has a direct impact on performance. The challenge is therefore not just about adding protection, but doing so without compromising hydrodynamics, weight distribution or operational access. This is where the removability of the engine covers offers another benefit – particularly in testing and situation analysis.

“Another constraint is the complexity of the platform in question. Fast patrol vessels and RIBs often have limited structural space, exposed systems and high-maintenance operational cycles. Any protection system must therefore be easy to install, easy to remove and fully compatible with existing OEM configurations.

“This is where modularity becomes essential. In practical terms, this flexibility is increasingly important for multi-role fleets that must transition between low-risk and high-risk operational environments rapidly. And, unlike traditional approaches that simply add layers which leads to heavy and inflexible systems, ASL GRP leverages innovative material science and years of expertise to ensure optimal protection without compromising crucial factors like weight and flexibility.”



From a materials and survivability perspective, where do you see the biggest vulnerabilities in subsea infrastructure protection today?

“Subsea and maritime infrastructure vulnerabilities are more focused on exposed interface points.

“The most at-risk areas are typically transition zones – where power, communications and/or control systems move between submerged, surface and shore-based environments. These include cable landing points, buoyed interfaces and surface-adjacent control infrastructure.

“These areas are difficult to fully armour due to the access requirements and environmental exposure, which creates inherent vulnerabilities in otherwise resilient systems. The broader challenge is that modern unmanned systems and hybrid threat platforms are increasingly capable of targeting infrastructure indirectly – through disruption, fragmentation or electronic interference – rather than relying on direct structural attack.

“This is where composite

engineering and modular protection approaches can offer value, particularly in providing lightweight, adaptable shielding that can be integrated without compromising maintainability or system access.”

UK defence policy is putting more emphasis on resilient supply chains, sovereign capability, and advanced manufacturing. What are the real bottlenecks today - and what more could be done to support specialist manufacturers like ASL GRP?

“There is strong alignment between UK defence priorities and the capabilities offered by specialist manufacturers. However, several practical bottlenecks remain.

“One of the most significant is the balance between innovation, speed and qualification timelines. Advanced composite systems can be developed and iterated rapidly, but defence certification and procurement processes often move at a slower pace. This creates a lag between operational need and deployment, even when the materials are ready to enter the factory.

“The second challenge is scalability. Many solutions, particularly in maritime protection, are highly bespoke, with engine-specific, platform-specific and mission-specific needs. Many ballistic protection systems must be tailored to

exact configurations, which is essential for performance and fit, but can introduce friction in the standardised procurement pathways.

“Material supply chain consistency is also a factor, particularly for specialist fibres and advanced resins used in high-performance ballistic systems, and especially with recent trade routes being heavily taxed and restricted – which has a knock-on effect with costs and timelines.

“From an SME perspective, there is also a broader structural challenge around early-stage engagement. Greater collaboration at concept and pre-procurement stages would significantly improve the ability to align innovation with operational requirements earlier in the cycle, reducing delays and improving integration outcomes.

“More flexible procurement frameworks and faster routes for trial and evaluation would also help organisations such as ours bring mission-relevant technologies into service more efficiently, particularly in rapidly evolving threat environments such as maritime drone and unmanned systems warfare.

At present, the pace of threat evolution, particularly in UAV and USV deployment at sea, is outpacing traditional acquisition cycles. Closing that gap is essential to maintaining operational advantage.”



