L3HARRIS™
FAST. FORWARD.

THE ROLE OF OPEN STANDARDS IN FUTURE FORCE PROTECTION ECM

Operational, Technical and Industrial Drivers

L3HARRIS™

THE ROLE OF OPEN STANDARDS IN FUTURE FORCE PROTECTION ECM

Operational, Technical and Industrial Drivers

CONTENTS

> “The nature of war remains constant: it is visceral and violent... and it is always about politics. What is changing is the character of warfare, which is evolving significantly due to the pervasiveness of information and the pace of technological change.”
>
> - General Sir Nick Carter, Chief of the Defence Staff

FOREWORD

The character of conflict will continue to evolve. Whilst impossible to predict what a future conflict will look like, it is inevitable our adversaries will exploit every opportunity to gain advantage. We plan and prepare to conduct operations across a complex, multi-faceted global arena. This arena encompasses not only the three traditional domains of Land, Air and Sea, but additionally those of Space, the interwoven Electromagnetic Spectrum (EMS) and the emergent, interconnected, data rich environment of Cyberspace.

To remain relevant we must quickly adapt to new and emerging threats, whilst maintaining the ability to conduct operations at scale and pace across the battlespace. Fuelled by information, the battlespace increasingly reaches into the cognitive domain across friendly, neutral and hostile populations. Deterred by our strengths, our adversaries operate in a “grey space” just below the threshold of armed conflict, using information to shape perceptions and will; attacking our cohesion and purpose. The dilemma we face is adapting to this evolving character of conflict whilst balancing the competing demands of our tactical and strategic mission priorities.

The scale, complexity and diverse nature of these operating domains necessitates a change of approach as coherence will not be achieved by strict controls, over specification and detailed requirements documents. Parallels can be drawn between this challenge and the scaling of web technologies and the Internet of Things (IoT) in the commercial sector. The role of Open Standards and architectures has been crucial to achieve coherence, foster innovation and accelerate development of new capabilities at scale and pace.

Freedom of action in the EMS is essential for effectiveness of capabilities across all military domains. This white paper has been produced to discuss the profound change in future warfare; considering the Operational and Technical drivers necessitating change in the Information Age, while providing a route to EMS superiority via open extensible solutions that enable a route to the practical realisation of Information Advantage.

Steve Clover
Director of Science
& Technology

Intelligence & Cyber
International EMEA

L3Harris

EXECUTIVE SUMMARY

The arrival of the fourth Industrial Revolution, the Information Age, has impacted both society and defence. The pervasiveness of technology and the resultant large amounts of data and information has changed how future conflicts will be conducted. While current technologies and capabilities are individually competent within their given operational domain, they are traditionally aligned to specific roles, mission sets and platforms; the underlying philosophy of their use is aging. Existing systems can no longer keep pace with operational needs or the desire to advance in step with exponentially evolving technology as they lack the ability to adapt to these changing circumstances at will.

This range of challenges demands that Armed Forces are both equipped and prepared for current conflicts, but remain poised and prepared to counter emergent threats. Meanwhile, growing demands for cross-domain collaboration between the physical and virtual domains requires a more holistic approach to the employment of sensors and effectors and a more evolved understanding of the Spectrum Operational Picture.

In the face of these challenges, the drive for technical advancement continues to quicken and requires collective agility and innovation in order to maintain our advantage over a diverse range of adversaries. These interlinked operational and technical demands are mirrored in the EMS. As the adversary's capacity to contest the EMS becomes more sophisticated, so maintaining our superiority in the EMS becomes increasingly challenging. EMS superiority is critical to life-saving Force Protection Electromagnetic Countermeasures (FP ECM), and an increasingly broad spectrum of threats demands the ability to quickly understand and distribute threat intelligence to rapidly generate effective counter-measures. In meeting this challenge, the role of Open Standards and architectures will be crucial to achieving coherence across complimentary technologies, fostering innovation and accelerating development of new capabilities at scale and pace.

In order to achieve dominance in the EMS, precision, analysis and rapid innovation are fundamental to success. Future Force Protection systems will require agility and openness by design in order to keep pace with emerging technologies without recourse to additional hardware or lengthy procurement procedures. The pressures on size, weight and power in modern vehicle platforms and the increasing complexity of the Electromagnetic Environment (EME) will require our Force Protection systems of the future to fulfil wider roles as Electronic Warfare & Cyber Sensors and Effectors. This combined with the processing, evaluation and dissemination of threat data, will offer genuine Information Advantage to the end user.

This paper focuses on four elements as an approach to the realisation of solutions that use Open Standards and open architectures to achieve EMS superiority:

Operational Drivers: Defining the need for change with respect to Vehicle-based FP ECM

Technology Drivers: Identification of the key technology influences and advancements that necessitate change for FP ECM

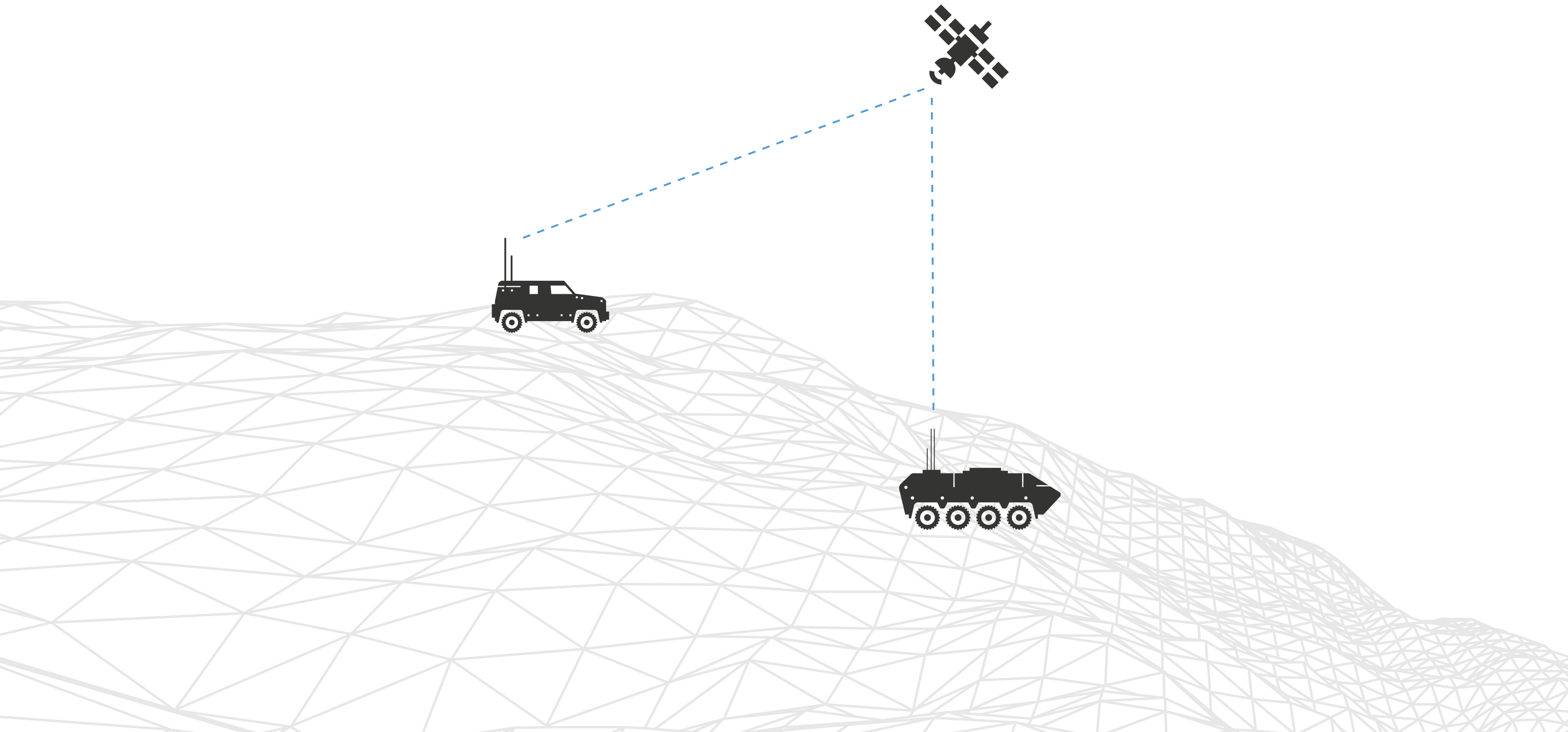
Open Standards and CORVUS Solutions: An example of how Open Standards and architectures can be applied to connectivity and extensibility

Programmatic and Industrial Approach: Exploring the way in which an open standards and iterative capability development and delivery supports supply chain diversity, innovation and provides the procurement authority more choice in how they deliver capability to the end user.

OPERATIONAL DRIVERS

The current information-rich environment in which FP ECM is now expected to operate is complicated by the diverse range of operational and technological concerns that exist. There is no single measure that can be used to reduce the scale of this complexity and the transformation that is required, across all domains, will take time. The role of Open Standards and open architectures will lay the foundation for success.

The operational drivers that influence this change can be observed directly by the need for highly optimised Size, Weight and Power (SWaP) solutions, indirectly from the wide variety of expected operational environments, and the desire to realise force multiplication via coordination, cooperation and collaboration between tactical assets and strategic decision-making.



SIZE, WEIGHT AND POWER (SWaP)

The current fleet of vehicle platforms have undergone many upgrades over time, typically driven by Urgent Operational Requirements. This has had a profound impact on SWaP with respect to adding additional systems, requiring more space and power while adding weight. The continual need to advance in step with technology and threats has adversely influenced current SWaP profiles. The advent of multi-mission, multi-function and multi-role Concepts of Operation requires optimised solutions to meet future operational aspirations.

NEW VEHICLE SYSTEMS

The demand for single domain, platform-centric capabilities has diminished. Current and future requirements are for smaller faster assets with low observability, multi-spectral stealth, integrating active and passive multi-function Electronic Warfare assets distributed across the area of operations. The data generated and the information derived from it should also be timely, assured and resilient in order to deliver Information Advantage. Operators must now manage a vast number of complex sensors and effectors, each providing data and information streams that contribute to a consolidated strategic picture informed by real-time tactical feeds.

SPECTRUM COMMON OPERATIONAL PICTURE

The EMS will be seen as a generic military enterprise resource that must be secured. Freedom of action in the EMS is essential for effectiveness of capabilities across all military domains. The EMS facilitates the exchange of data, information, intelligence and capability on demand. The orchestration of tactical assets from a strategic perspective across multiple deployments is predicated on extensive Situational Awareness of the EMS. Superiority of the EMS should be considered an underpinning objective to all future operations; the integration of a Spectrum Common Operating Picture is a key component to realise this objective.

CONGESTED, CONSTRAINED, CONTESTED EME

The scope of operational environments that FP ECM are now expected to deploy within span a wide variety of scenarios positioned against a multitude of different threat profiles. The continued growth in consumer electronics has resulted in a highly congested EME, typically comprised of civilian communications systems. This presents a significant challenge for FP ECM in relation to collateral RF, so the need for precision countermeasure is key. Congestion is also observed within a military context in relation to the plethora of electronics and sensors and effectors modern forces employ to achieve mission objectives.

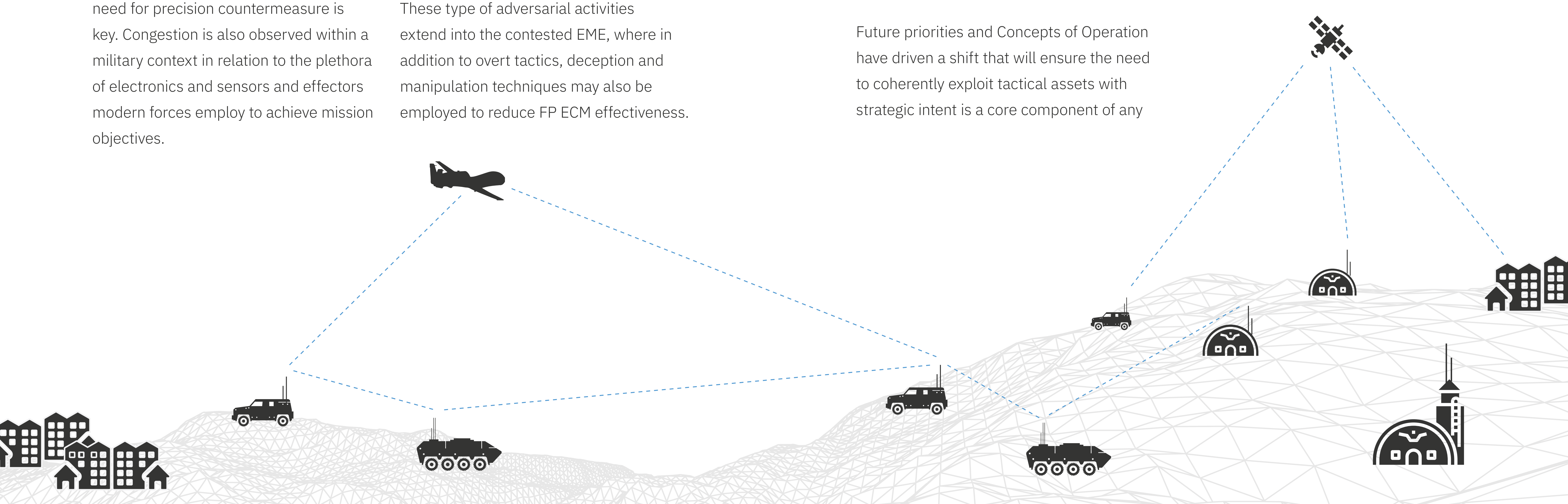
While congested EMEs are assumed to be commonplace, modern day forces are now expected to operate within constrained scenarios, where RF emissions are tightly controlled for more than just minimising collateral and optimising capabilities. Advanced adversaries may exploit FP ECM systems to trigger RF emitters to augment their own target acquisition or spectral intelligence, severely impacting the chance of friendly forces completing a mission successfully.

These type of adversarial activities extend into the contested EME, where in addition to overt tactics, deception and manipulation techniques may also be employed to reduce FP ECM effectiveness.

COLLABORATION, COOPERATION AND COORDINATION WITH MISSION PARTNERS

The aspiration to conduct operations with mission partners in ever more collaborative ways in turn drives the need for cooperation during the development and deployment of new capabilities and the coordination of effort. There is a significant gap when it comes to collaboration and information-sharing across domains and in some cases mission partners.

Future priorities and Concepts of Operation have driven a shift that will ensure the need to coherently exploit tactical assets with strategic intent is a core component of any mission. The ability to exponentially grow our Situational Awareness and increase the speed of decision-making will ensure we are able to outpace our adversaries. This level of enterprise collaboration far exceeds the objective of joint concepts, every platform considered multi-domain, multi-mission, multi-role, either as a generalised or specialised information provider and/or effector.



COMMON CHALLENGES

This operational view provides an illustration of the key issues that comprise the drivers that are influencing the need to consider open, extensible solutions for future FP ECM capabilities.

SIZE, WEIGHT AND POWER

> Equipment space on today's vehicle platforms is almost at capacity
> Delivery of new capability places increasing demands on vehicle infrastructure
> Introduction of new hardware results in capability trade offs
> Current RF system design ensures that resources cannot be rationalised

CURRENT VEHICLE SYSTEMS

> Reaching End-of-Life
> Ill-prepared to combat emergent/future threats
> Designed to be target set-specific with limited broader utility
> Lack of modularity and focus on mission-specific design limits extensibility

SPECTRUM COMMON OPERATIONAL PICTURE (COP)

> Manual de-confliction of spectral activities requires careful planning
> Optimisation of spectral resources is often governed by a fixed rule set with limited automation
> Spectrum COP lacks the detail and timeliness to support operational decision-making
> Limited availability of critical mission information across platforms and partners

CONGESTED, CONSTRAINED, CONTESTED EME

> Inability to reconfigure for specific operational environments efficiently and economically
> Slow to develop and deploy scalable resources
> Limited ability to balance activity load across tactical and strategic assets
> EME complexity limits ability to rapidly identify and exploit vulnerabilities in complex threats

COLLABORATION, COOPERATION, COORDINATION

> Manual optimisation of countermeasure profiles
> Limited sharing of data and/or information
> Limited input back into wider mission planning
> Limited cross-domain collaboration
> Lack of collaborative mission planning

TECHNICAL DRIVERS

The need to consider the bigger picture in relation to architectural design is now recognised by leading NATO nations who are focussed on the adoption of an Open Standards approach. This approach addresses rationalisation at the platform level, outlines an approach to decouple software and hardware, and considers the sharing and proliferation of information across the wider land and partner environments.

OPEN STANDARDS AND ARCHITECTURE

The drive towards Open Standards and architectures is intended to address the following issues currently encountered in defence technologies:

> Capabilities are platform, domain and mission-specific with limited opportunity for re-use or extensibility via software or hardware upgrades

> Proprietary vendor solutions do not keep pace with technical advancements in hardware and preclude innovation through software enhancements

> Capabilities cannot adapt quickly enough to counter evolutionary adversary tactics

> Data and information generated on a platform cannot be shared across domains or with other platforms or allies, limiting the capacity to generate timely intelligence and slowing the Commander's decision-making cycle

> Interoperability with our own force and partner organisations is hampered by incompatible interfaces, security domains and specific spectral requirements

The guiding philosophy that drives an Open Standards approach is that a collective community is better than an isolated perspective. When considering multiple diverse operating domains, coherence cannot be achieved by strict controls, over specification, and detailed requirements documents that are commonplace in the defence enterprise. Open Standards are inherently not fixed, constantly evolving and improving architectures over time.

Building enterprise-level architectures based on standards outside of the Design Authorities' direct control introduces potential risk that is alien to the defence community.

The decomposition of the problem into manageable groups provides a feasible method for identification and mapping of Open Standards and architectures to either resolve an issue or position for future advancement in technology or doctrine. The resultant mapped set of Open Standards and architectures is abstracted over many levels, from electrical pin connectivity to sharing information across multiple domains.

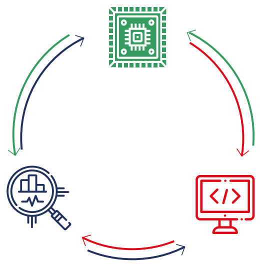
The identification of mission outcomes agnostic to operational domain or environment provides focus prior to architecture definition. Leveraging our experience in the overarching discipline of EW, three high-level mission outcomes in support of EMS Superiority are identified:

> **Sense:** Gather Spectral Intelligence to support ISR activities, developing tactical and strategic situational awareness of the EME to inform operational movement and/or attack/protection options.

> **Shield:** Inhibit adversary System of Interest to protect friendly forces via traditional or precision targeting to enable an Electronic Counter Measure (ECM) or CEMA response.

> **Act:** Interfere with adversary System of Interest via precision or traditional targeting to enable Electronic Attack (EA) or CEMA to degrade hostile use of the EME and shape their behaviour.

The use of Open Standards in this respect will accelerate innovation and provide a route to evergreen capabilities for defence.



EDGE

Provides and develops both a modular and scalable set of hardware options, EC2 and a set of applications focused on the delivery of operational outcomes.

CORE

Provides a set of enabling software tools to support the delivery of a range of operational objectives during preparation, orchestration, analysis and sustainment.

THREAT

Provides a service that maintains a prioritised SOI list, focused analysis to enable targeting and defeat, prototype code, informs optimised deployments

Figure 1: At the highest level abstraction the Sense, Shield and Act approach defines concepts for Edge, Core and Threat as a common anchor that can be specialised into any domain or mission set.

INFORMATION COMPLEXITY

The establishment of the Information Age has driven an exponential increase in our ability to generate information, increased the complexity and variance of information types, and accelerated the velocity at which information can be acquired, generated and accessed. The dominance of hardware-based single purpose systems that were dependent on human interpretation of data has passed. The digitisation of vast quantities of defence related data, including Radio Frequency, Electro-Optical and Radar into a digital format provides the foundation for the Information Age and the driver for exploitation of data analytics at scale.

DECOUPLING CAPABILITY FROM PLATFORMS

This explosion of information has sparked the advancement of edge compute, cloud, and artificial intelligence to augment decision-making. The pace of technical advancement in this area is considered to be driven by Open Standards and architecture, in some part.

Open Standards and open architectures have driven convergence on general-purpose processing, enabling developers and solution providers to innovate in a variety of ways while also ensuring capabilities are portable between platforms and extensible for future needs. There are significant challenges to overcome within military operating domains to agree a feasible concept that decouples capability to the point where it is portable between platforms. The desire to deploy software capabilities at the time of need to platforms of opportunity is a core part of the future vision within defence and is a key benefit of adapting an open approach that realises extensibility at the core.

KEEPING PACE WITH NEW TECHNOLOGIES

Despite the specialised nature of many defence technologies, advancement of new capability does not need to be a protracted process, our adversaries have already shown that it can be achieved at pace. To do this, a paradigm shift is required across all operating domains with the digitisation of data being the first step.

To realise truly modular, scalable, extensible and interoperable solutions that keep pace over time with advancements in technology, an Open Standards approach is required.

THE FUTURE

The Electromagnetic Spectrum acts as the common reference for FP ECM across domains, while the identification of mission outcomes, agnostic to domain, provides direction, e.g. Shield. The definition of future mission scenarios will inform technical roadmaps, ensuring we are ready to meet future requirements. These roadmaps shall guide open architecture development which is focused on delivering adaptive, extensible solutions which expands into non-functional concerns.

This underlying open architecture must enable responses to FP ECM based threats to be developed, scaled and deployed faster than conventional approaches. This approach must reduce the burden on the end user by providing multiple mission capabilities from a common core, thus maximising training efficiency and logistics.

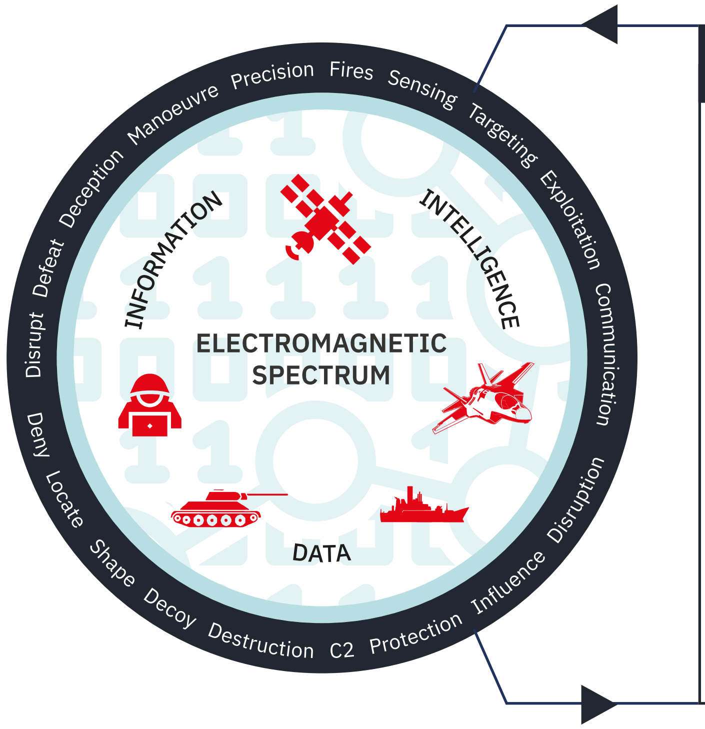


Figure 2: The Electromagnetic Spectrum is the common reference across multiple domains.

Mission activities contribute to the realisation of mission outcomes

SENSE

Gather Spectral Intelligence to support ISR activities, developing tactical and strategic situational awareness of the EME to inform operational movement and/or attack/ protection options.

SHIELD

Inhibit adversary System of Interest to protect friendly forces via traditional or precision targeting to enable an Electronic Counter Measure (ECM) or CEMA response.

ACT

Interfere with adversary System of Interest via precision or traditional targeting to enable Electronic Attack (EA) or CEMA to degrade adversary use of the EME and shape their behaviour.

Non-functional aspects underpin mission activities and outcomes

Workforce
Resources
Acquisition
Development
Training

Education
Execution
Governance
Policy
Strategy

People
Sustainment
Organisation
Planning
Process

Logistics
Political
Legal
Environmental
Social

OPEN STANDARDS AND FP ECM

L3Harris has delivered FP ECM capabilities in a military context for over thirty years, providing innovation, reliable performance and agile support across NATO and other coalition partners. With acknowledgement to both the operational and technical drivers discussed, L3Harris has developed the CORVUS architectural approach as a mechanism to introduce mission partners to next-generation FP ECM and CEMA. CORVUS utilises a number of shared and Open Standards common within NATO, enabling cost-effective research, development and transfer of the emergent capability. CORVUS offers Defence Organisations ownership of their own FP ECM capabilities.

The CORVUS architecture supports a number of configurations, helping mission partners to realise the following benefits:

> Reconfigurable to rapidly address emerging technology and threats
> Evergreen, with rapid development cycles to embrace new technologies
> Lower cost of ownership across development, acquisition and support
> Interoperability at both tactical and strategic levels via Open Standards
> Enables trusted partners to develop their own modules and software

Figure 3: Below and adjacent;CORVUS platform

SOFTWARE EXTENSIBILITY

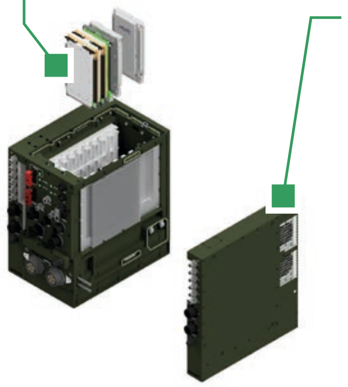
CORVUS has embraced an open approach with respect to mission applications. The development of an Open Component Portability Infrastructure (OCPI) Board Support Package (BSP) that enables third parties to develop and or port their existing applications to a CORVUS platform offers huge benefit via re-use. The ability to develop and deploy applications in this manner is critical to longer term sustainment, the encouragement of innovation, and fostering diversity in the supply chain.

HARDWARE EXTENSIBILITY

All CORVUS solutions incorporate modularity and scalability at their core:

OpenVPX modules

OpenVPX modules in the core processing unit allow extensibility and access to a large ecosystem of Single Board Computers, Network Switches, PCI Switches, Power Supplies, Storage, RF Transceivers, RF Receivers, and Position Navigation and Time Cards

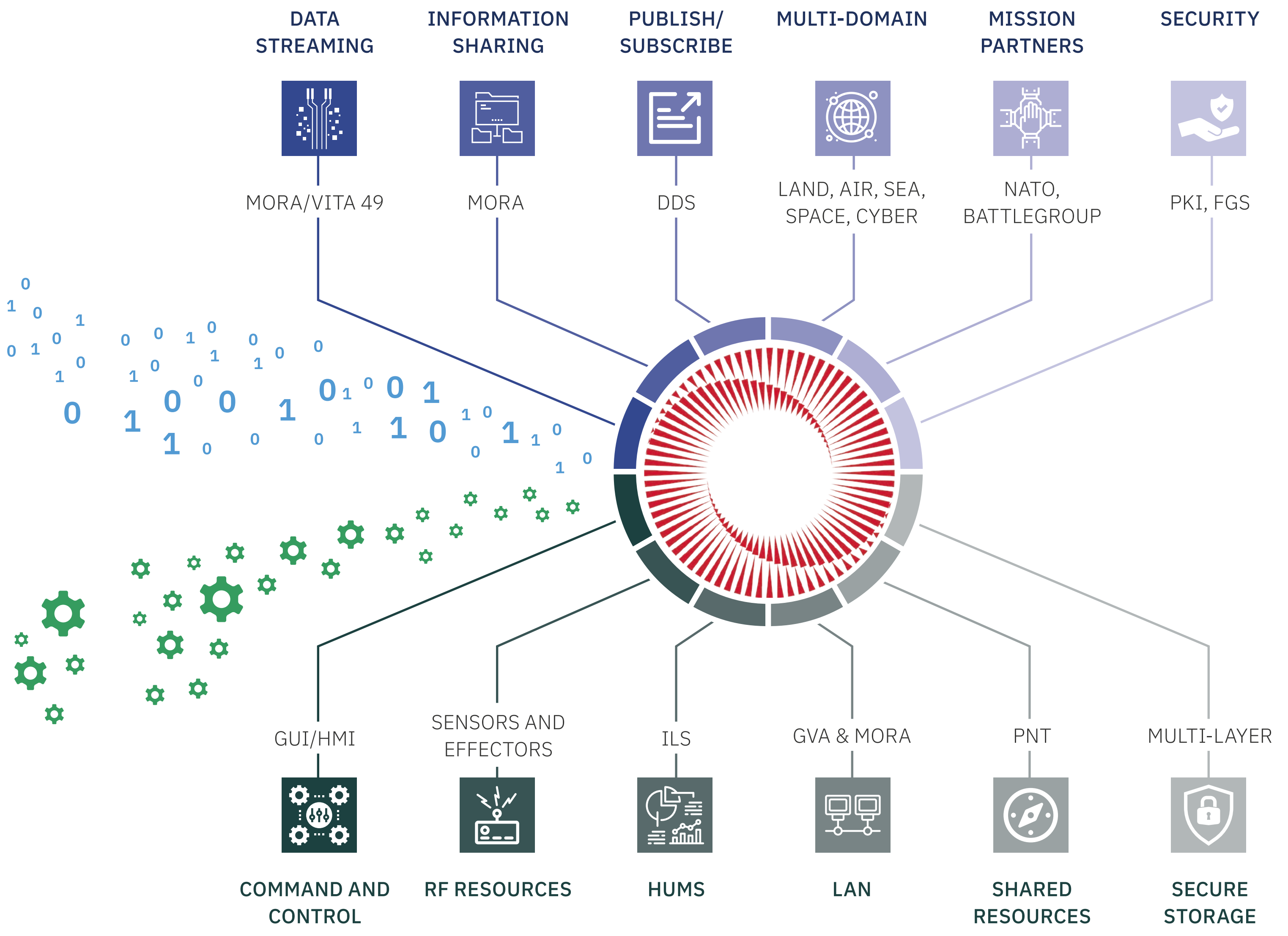


Modular active front end

Designed to employ a modular design for the active front end which enables the amount of RF Power to be tailored for operational needs, whether this is the number of Power Appliers or the absolute power each must emit:
e.g. 4 x 20W, 4 x 100w, 2 x 20w + 2 x 50, 6 x 20w etc

ENTERPRISE CONNECTIVITY

CORVUS-derived solutions consider Enterprise Connectivity as a critical component of overall mission success, especially in support of operational aspirations for collaboration, cooperation and coordination with mission partners. This connectivity shall take advantage of tactical and strategic bearers of opportunity, facilitating data streaming via MORA/Vita 49 and information sharing via Common Services and MORA C4I Network.



DATA STREAMING – MORA/VITA 49
INFORMATION SHARING – MORA
PUBLISH/ SUBSCRIBE – DDS
MULTI-DOMAIN – LAND, AIR, SEA, SPACE, CYBER
MISSION PARTNERS – NATO, BATTLEGROUP
SECURITY – PKI, FGS

GUI/HMI – COMMAND AND CONTROL
SENSORS AND EFFECTORS – RF RESOURCES
ILS – HUMS
GVA & MORA – LAN
PNT – SHARED RESOURCES
MULTI-LAYER – SECURE STORAGE

PLATFORM CONNECTIVITY

CORVUS solutions incorporate Platform Connectivity from inception, covering electrical pin connectivity through power distribution and conditioning to networking and RF resource optimisation via MORA C4I Network and MORA Low Latency Bus (ML2B).

Specific vehicle fleets may already have an underlying architecture such as the Generic Vehicle Architecture (GVA) which extend platform connectivity to include core services such as Heath Usage Metrics and Statistics (HUMS) which provide hooks for efficient support options and a suite of common Graphic User Interfaces (GUI) that reduce cognitive burden for operators.

INDUSTRIAL APPROACH

The use of an open architecture facilitates an innovative industrial approach allowing Defence Organisations access to a wider industrial base and, through open and shared standards, protects from vendor lock-in and the associated through-life expenditure of significant re-design or large-scale technical refresh programmes. It also provides greater access to innovation, increasing potential for research and development outside of the normal industry cohort.

This approach provides the flexibility for defence industry collaboration not only across the region but also heavily supported by localised industry partners including platform providers, systems integrators, equipment manufacturers and small to medium sized enterprises, as well as the generation of local support capability.

The adoption of an Open Standards approach enables the consideration of innovative programmatic approaches that in turn ripple throughout the industry. An example of this is the Scaled Agile Framework (SAFe) which L3Harris has used for both Internal Research and Development (IRAD) and customer programmes. SAFe employs a user-centric philosophy that instils a continuous learning culture throughout the supply chain that facilities innovation and relentless improvement across the entire portfolio. Agile solution delivery that is orientated around user needs allows for continuous exploration, integration and innovation driven by current, emergent and future demand signals.

The delivery of next-generation FP ECM is a challenge at an enterprise scale and the implementation of lean system engineering coordinated across the supply chain will be required. Current solutions have evolved overtime, however future systems need to advance even when live and in operation; this necessitates a continuous delivery pipeline and coordination across the supply chain.

PORTFOLIO MANAGEMENT

The use of Open Standards enables the Defence Organisations to consider lean portfolio management practices for FP ECM and wider CEMA initiatives. This approach will enable the alignment of overarching strategy, funding and execution to the optimisation of efforts across interrelated capabilities. An integrated strategic view of tactical activities should encourage a lightweight governance structure that empowers delegated decision-making, on the principle that the agreed open architecture provides coherency across capabilities. This will enable the evolution of the FP ECM requirements to mature with additional features as required throughout the life of the capability.

AGILITY

In order to respond quickly to operational needs, threats or opportunities, a combination of organisation and technical agility is required. To release the benefits of agility, a lean agile mind-set is required across the organisation. This may manifest as high-performing, cross-functional agile teams or teams of agile teams. For true agility to be realised in a meaningful operational way, quality should comprise the core of these activities. Responsiveness cannot be substituted for quality, especially within the FP ECM domain. L3Harris has incorporated agility by ensuring the delivery of customer-based delivery outcomes, affording prioritisation of evolving requirements and subsequent development, testing and implementation capability enhancements against operational and technical requirements.

DIVERSIFICATION OF SUPPLY CHAIN

The L3Harris approach with CORVUS enables multi-vendor procurement for hardware, software/ countermeasures and other services, underpinned by a commercially and technically open architecture, thus increasing the breadth of the supply chain to include suppliers for adjacent domains and local industry partners and academia. In turn, this increases the competitiveness, avoids vendor lock-in and provides the customer with greater value for money, wider access to technology and different perspectives to solving problems, and increasing innovation.

FLEXIBLE SUPPORT FRAMEWORK

L3Harris is a proven and trusted support partner for NATO customers. With a highly responsive attitude to customer service and a focus on bespoke support arrangements, L3Harris support centres are present across Europe and the United Kingdom. L3Harris is also well versed in the establishment of localised support infrastructure and works with trusted local partners.

The CORVUS approach to Open Standards introduces a genuine change in the way that support arrangements can be facilitated and enables Defence Organisations to benefit from a fully flexible support framework which adheres to the following principles:

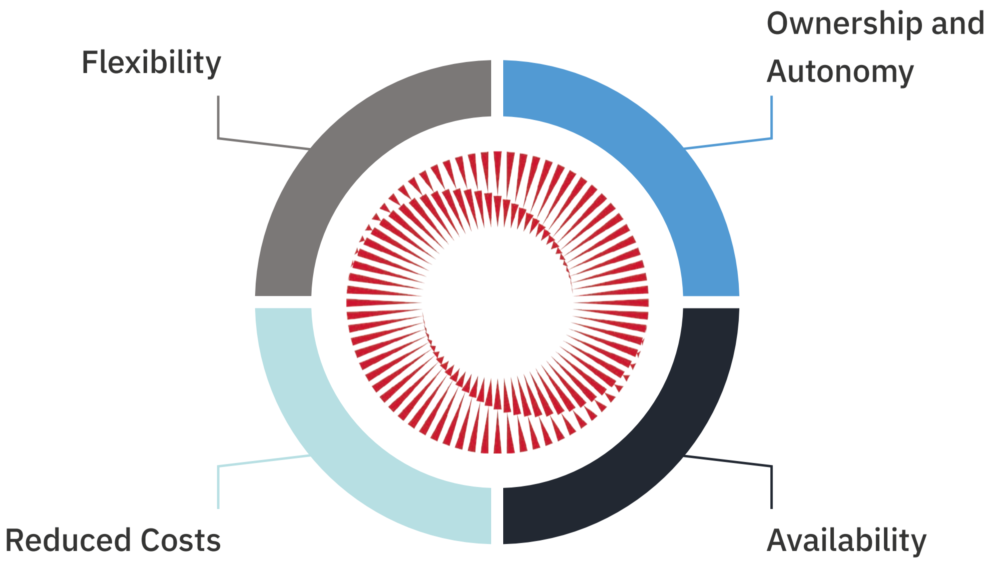


Figure 4: The principles of an Open Standards support framework; flexibility, ownership and autonomy, availability and reduced costs.

FLEXIBILITY

The modularity and scalability of an Open Standards approach enables the end user to develop a highly flexible and bespoke support ecosystem consisting of a range of SMEs with specialist knowledge as well as in-house support capabilities. This flexibility takes advantage of CORVUS' capacity of extensible and iterative development to deliver mission-specific capability throughout the lifecycle of the capability.

OWNERSHIP AND AUTONOMY

The benefits presented by an Open Standards approach also ensures that Defence Organisations can, should they wish to, maintain full ownership of all or part of their support arrangements. This approach also offers Defence Organisations greater autonomy over support operations in the deployed environment by supporting their ability to rapidly field capability enhancements and maintenance arrangements dependent on the threat landscape.

AVAILABILITY

A modular approach based on common standards enables Defence Organisations to engage suitably qualified domestic partners as part of this support ecosystem. This not only supports domestic industry, but also enhances operational availability by significantly reducing Mean Time To Repair (MTTR) in comparison to returning units for repair over international borders.

REDUCED COSTS

A support framework underpinned by CORVUS' extensible and upgradeable Open Standards approach ensures that FP ECM capability remains capable and current throughout its lifecycle without recourse to wholesale reinvestment in new capability.

BENEFITS OF OPEN STANDARDS

This white paper has described the strategic context as well as the operational and technical challenges associated with conducting operations in the modern EME and with particular reference to FP ECM. With these demands in mind, there are significant operational and technical benefits available to the end user in adopting an Open Standards approach to FP ECM such as CORVUS.

OPERATIONAL BENEFITS

Maintain pace with current and future threats:

An Open Standards approach enables the end user to support current operational demands whilst maintaining the capability to rapidly respond to a broad range of emergent threats.

Ensure hardware and software extensibility:

By decoupling capability from stove-piped hardware instantiations, an Open Standards approach enables the end user to configure and integrate mission-specific solutions with agility and whilst avoiding heavy re-investment in hardware or software. This approach also supports iterative extensions of capability.

Enable international and bilateral collaboration:

The adoption of common services ensures that Defence Organisations are able to not only interoperate with international and bilateral partners, but also exploit and contribute to mission-critical information exchange with partner forces where appropriate.

Offers multi-role extensibility whilst maintaining SWaP:

As space and power become ever scarcer in today's vehicle platforms, an Open Standards approach supports multi-role extensibility across FP ECM, EA, ESM and cyber techniques in order to make best use of this space and power and enable the employment of sensors and effectors in mission-specific configurations.

PROCUREMENT OPPORTUNITIES

Supply Chain Diversity:

An Open Standards approach enables a diverse supply chain of both domestic and international contributors of compatible hardware and software with a common understanding of interface requirements.

Promotes defence industry partners working together to offer the best VfM:

The opportunity to further exploit an already strong ecosystem of specialist industry partners provides Defence Organisations technologists and academia with the capacity to collaboratively offer new capability, thereby ensuring that Defence Organisations are offered clear innovation and value for money.

Ensures that Defence Organisations remain in control of their technical needs:

A system approach which supports spiral capability development means that Defence Organisations can maintain greater control of their requirements, ensuring that development satisfies operational and technical requirements whilst ensuring VfM.

Ensures that Defence Organisations are able to exploit new technologies:

The procurement of a system which supports true hardware and software extensibility ensures that Defence Organisations are able to develop applications in response to operational requirements at pace and with agility in order to exploit new technologies and extend the life-span of in-service equipment.

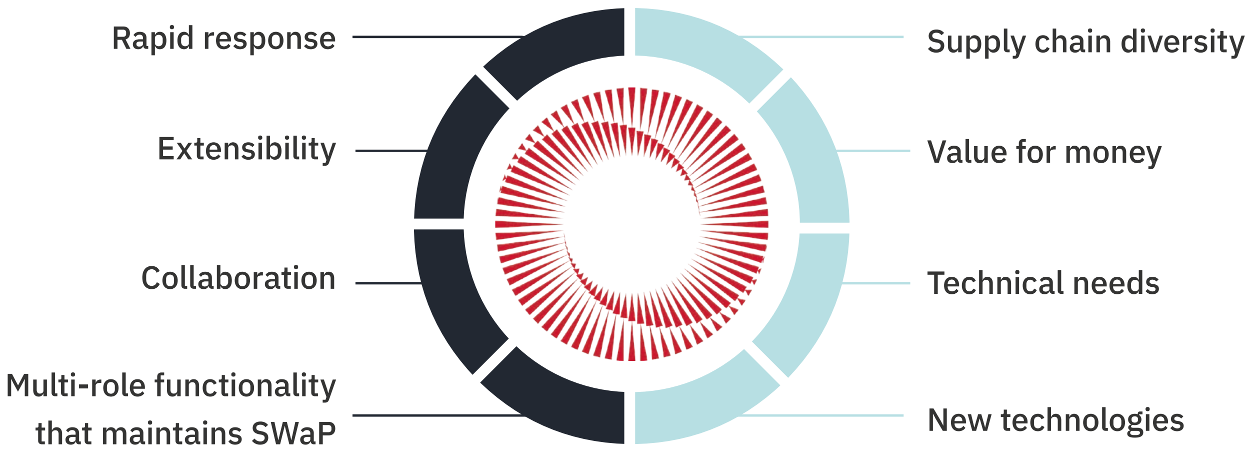


Figure 5: Some of the operational and procurement advantages of an Open Standards approach to FP ECM.

EMBRACING OPEN STANDARDS

It's undeniable that Open Standards and architectures already play a critical role in FP ECM, and will continue to offer transformative advantages well into the future. Adopting this open approach will help to:

Overcome the operational and tactical challenges often faced in the field, such as:

- SWaP
- New vehicle systems
- Spectrum COP
- Congested EME
- Collaboration and coordination

Unlock the following key benefits:

- Adaptability
- Extensibility
- Interoperability
- Lower cost of ownership
- Partner module development

Revolutionise mission success by enabling important integration across all domains through a rich ecosystem of available platforms

Embracing Open Standards, however, does require an open mind, as well as a commitment to evolve from more traditional technologies and processes sooner rather than later.

This combination of speed and a willingness to adapt is essential to remain one step ahead of the adversary – only then can you truly gain, and maintain, the operational advantage.

EMBRACING CORVUS

CORVUS provides multi-platform, next-generation CEMA solutions to meet the evolving threats of today's congested battlespace. Modular and scalable, it enables seamless integration and rapid end user configuration in the field.

Built on Open Standards, CORVUS was designed with agility, connectivity, and extensibility in mind. Thanks to an open, modular approach, interoperability across multiple systems from multiple vendors is made easy, seeing you achieve the end-to-end integration that is so important in the modern EME.

If you would like to learn more about how CORVUS can help you stay ahead of the curve, please get in touch with us to arrange a virtual meeting and live demonstration of the platform.

THE LANGUAGE OF EW

AI	Artificial Intelligence
CEMA	Cyber Electromagnetic Activity. 'The synchronisation and coordination of cyber and electromagnetic activities, delivering operational advantage thereby enabling freedom of movement, and effects, whilst simultaneously, denying and degrading adversaries' use of the electromagnetic environment and cyberspace.'
CMOSS	C4ISR Modular Open Suite of Standards
CONOPS	Concept of Operations
EA	Electronic Attack
ECM	Electronic Countermeasures
Edge Computing	A paradigm of distributed computing that brings processing close to the location where it is needed in the form of 'virtual machines' or local processing.
Electromagnetic Spectrum Superiority	Defined by the US as "The coordinated execution of joint electromagnetic spectrum operations with other lethal and non-lethal operations that enable freedom of action in the electromagnetic operational environment."
EME	Electromagnetic Environment
EMS	Electromagnetic Spectrum
EWSI	Electronic Warfare and Signals Intelligence
FPGA	Field Programmable Gate Array
GPP	General Purpose Pre-processor
GPU	Graphics Processing Unit

Information Advantage	The credible advantage gained through the continuous, adaptive, decisive and resilient employment of information and information systems.
IRAD	Internal Research and Development
JICD	Joint Interface Control Document
LCA	Land CEMA Architecture
MDI	Multi-Domain Integration
Mosaic Warfare	A US term that describes a "systems of systems" approach to military warfare that focuses on re-configuring defence systems and technologies so that they can be fielded rapidly in a variety of different combinations for different tasks.
Open CPI	Open Component Portability Infrastructure
OpenVPX	OpenVPX is an architecture framework for hardware that defines system level VPX interoperability for multi-vendor, multi-module, integrated system environments.
SAFe	Scaled Agile Framework
SOSA	Sensor Open Systems Architecture
Sub Threshold Warfare	Warfare that is designed to exploit national vulnerabilities across the political, military, economic, social, informational and infrastructure spectrum without the use of direct aggression.
SWaP	Size Weight and Power

PARTNER OF CHOICE

L3Harris Technologies is an agile global aerospace and defence technology innovator, delivering end-to-end solutions that meet customers' mission-critical needs. The company provides advanced defence and commercial technologies across Air, Land, Sea, Space and Cyber domains.

L3Harris is the partner of choice for the design, development and delivery of advanced electronic systems for the protection of people, infrastructure and assets when and where it matters. Working in partnership with civil and defence organisations, we defend against evolving and emerging threats worldwide. The long-term customer, industry and in-country partnerships we develop pay huge dividends in terms of trust, responsiveness and our understanding of key issues.

FURTHER INFORMATION:

To learn more about how CORVUS can help you stay ahead of the curve please get in touch:

Hello@L3Harris.com

FAST. FORWARD.

L3HARRIS™

THE ROLE OF OPEN STANDARDS IN FUTURE FORCE PROTECTION ECM

L3Harris Technologies is an agile global aerospace and defence technology innovator, delivering end-to-end solutions that meet customers' mission-critical needs. The company provides advanced defence and commercial technologies across air, land, sea, space and cyber domains.