TEAM DEFENCE INFORMATION
www.teamdefence.info

DEFENCE INFORMATION 2026

NEWSLETTER

National Armaments Director Group

Opening Address

From Strategic Vision to Digital Advantage

Claire Fry, Interim Chief Digital Information Officer, welcomed delegates to DI26, highlighting collaboration across Defence, industry and academia as essential to delivering digital advantage. Claire emphasised that the Defence Investment Plan's investment in digital, AI, cyber and data presents a once-in-a-generation opportunity, but delivery must now be the priority. Claire reinforced the need for reform, integration and strong partnerships to create operational advantage for the warfighter and strengthen Defence.

The Role of Digital & Data in Building NAD Group

Nigel Shaw, Corporate Chief Information Officer, presented the challenge of digitally integrating the newly formed National Armaments Group to support a more agile, modern Defence. Nigel highlighted the need to modernise enterprise systems, accelerate AI adoption and reduce duplication across legacy organisations. He welcomed investment through the Defence Investment Plan to drive business transformation, ERP modernisation and automation, while stressing that cyber security, common standards and full organisational integration are essential to delivering capability faster for the warfighter.

Panel One - The Digital Function

The Digital Function - Singular, Integrated and Unified

Brigadier Jamie Balfour, Interim Director Functional Integration, outlined how Defence's digital and data operating model will deliver the Strategic Defence Review and Defence Investment Plan. Jamie emphasised that digital is now a core warfighting enabler, supported by investment in data, cyber, AI and the digital backbone. Jamie highlighted progress in digital skills, cloud, cyber resilience and shared platforms, while stressing that integrating digital, data and governance through a unified function is essential to delivering operational advantage at pace and scale.

From Abstract Strategy to Deployed Reality

Silvia Grant, representing the Defence Chief Technology Officer, discussed how Defence's new digital functional leadership provides stronger authority to drive enterprise governance, integration and standardisation. Silvia highlighted major investment in the digital backbone and Digital Targeting Web, emphasising common architectures, sovereign cloud, reusable services and secure-by-design principles. She stressed that Defence must adopt open, standardised and cloud-native technologies while working transparently with industry, ensuring digital innovation delivers greater operational advantage for the warfighter.

Digital Enablement through a Common Digital Foundation of Data

Stuart McKillop, Interim Director Defence Data Officer, explained that data is now a strategic asset at the heart of Defence's digital transformation. Stuart argued that operational advantage depends on trusted, interoperable data enabling AI, faster decision-making and integrated operations. He highlighted initiatives including Project Frontier, common data standards and AI foundations, stressing that success relies on strong partnerships, skilled people and shared platforms. Ultimately, he said Defence's advantage will come from learning, deciding and acting faster than its adversaries.

Transforming Cyber Resilience

William Rimington, representing the Director Cyber Defence and Risk, emphasised that cyber resilience is fundamental to Defence's digital transformation. William highlighted the importance of Secure by Design, robust standards, continuous assurance and close collaboration with industry to protect Defence from evolving cyber threats. Using a pomegranate analogy, he illustrated the need for layered security, detection and resilient architectures. He concluded that regular testing, exercising and preparedness are essential to ensure Defence can operate effectively during cyber incidents.

TEAM DEFENCE INFORMATION
www.teamdefence.info

National Armaments Director Group

Panel Two - Driving Growth Through MOD & Industry Innovating as One Defence

Partnering for Digital Advantage: The Industry View

Gareth Hetheridge, CIO, Leonardo UK, explained that collaboration is essential to delivering the Strategic Defence Review within the Defence Investment Plan's financial constraints. Gareth highlighted the need for greater clarity on digital sovereignty, stronger industry collaboration, cyber resilience and modern contracting models. He argued that successful digital transformation must focus on business outcomes rather than technology alone, while responsible AI adoption, resilient infrastructure and shared standards are critical to delivering capability faster and more effectively for the warfighter.

How the Eleven Commercial Digital Levers Change the Game

Victoria Cope, Commercial Director Enterprise, highlighted how the Defence Investment Plan will transform Defence's commercial approach by accelerating procurement, strengthening collaboration and improving engagement with industry. Victoria highlighted outcome-based procurement, agile delivery, category management and reduced time to contract as key priorities. She stressed the importance of cyber security, preparedness, resilient contracts and continuous dialogue with suppliers, encouraging industry to work closely with Defence to deliver innovation, value for money and operational capability at pace.

Strengthening Partnership through the Defence Industry Joint Council

Harrison Talbot-Brown, Deputy Director Industry Engagement and Collaboration presented how the Defence Industrial Joint Council (DIJC) is driving delivery of the Defence Industrial Strategy and Defence Investment Plan through stronger government–industry collaboration. He highlighted investment in emerging capabilities, readiness and resilience, faster capability development, industrial resilience, and international partnerships. The DIJC has established governance, a delivery programme, and a communications forum while developing a long-term roadmap to 2035. He emphasised co-creation, wider industry representation, digital integration, and turning strategy into measurable delivery and operational outcomes.

UK Defence Innovation (UKDI) and its Demand Signals

James Gavin, Deputy Director, UK Defence Innovation (UKDI), shared how UKDI is refocusing defence innovation funding on delivering operational capability and growing the UK technology sector. He emphasised ending "innovation tourism" by only investing where there is a clear path to exploitation at scale, aligned with the Integrated Procurement Model. UKDI's £400 million innovation budget prioritises autonomy, digital targeting, logistics, space and resilience, while encouraging stronger demand signals for cyber and digital innovation to accelerate capability into service.

Lessons from Operations: Experience into Action

Lt Col Mark Dowds, Integrated Warfare Centre, examined key operational lessons from Ukraine and other recent conflicts, highlighting the need for much faster capability development, with adaptation measured in days and weeks rather than years. He emphasised the importance of rapid data exploitation, close integration between frontline operators, scientists and industry, and continuous learning through effective feedback loops. While recognising the transformative role of drones, he cautioned against overlooking the enduring value of artillery, electronic warfare and integrated air defence. He concluded that future success depends on resilience, deception, electromagnetic spectrum dominance, and stronger collaboration between defence and industry.

Panel Three: Decision Making at the Speed of Relevance

Foundations, Foresight and Frontiers: the Defence AI Centre's Strategic Direction

Brig Caroline Woodbridge-Lewin, Head of the Defence AI Centre (DAIC), discussed DAIC's strategic direction as Defence's enduring AI capability, supported by dedicated funding. She highlighted three priorities: delivering AI through Programme Frontier, coordinating AI activity across Defence, and strengthening AI foundations including governance, data, skills and standards. Emphasising speed, responsible adoption and collaboration, she called for greater investment in talent, AI infrastructure and partnerships. She also proposed a Defence AI Lab to accelerate experimentation, capability delivery and long-term AI integration across Defence.

Bringing AI to Life in Mission Critical Scenarios

Ajay Chakravarthy, UK Chief AI Officer, Thales, emphasised that Defence's biggest challenge is not developing AI but deploying it into mission-critical environments. He emphasised that success depends on building an "AI harness" around models, incorporating governance, assurance, security, monitoring, explainability and human oversight to create trusted operational capability. Rather than pursuing ever-larger models, organisations should focus on scalable, mission-ready AI integrated across systems. He concluded that trusted deployment, not model sophistication, will determine AI's operational advantage in Defence.

From Mechanisation to ASGARD DECIDE: Human Judgement in the Digital Age

Col David Haslam, Assistant Head ASGARD, outlined that modern warfare demands decisions that are timely, trusted and connected across all domains. He emphasised that secure data, AI and federated architectures are essential to turning information into operational advantage, enabling commanders to act before opportunities are lost. Using the ASGARD Decide programme as an example, he highlighted the need for trusted data, machine-assisted planning and coalition interoperability, stressing that success depends on adapting organisations, doctrine and technology together rather than relying on technology alone.

Digital Defence as a System: From AI Foundations to Operational Effect

George Carter, CEO of Darter and RAF Digital Strategic Advisor, shared that AI is only one part of delivering operational advantage, with success depending on data, digital infrastructure, operating models and organisational design. He emphasised that mission success comes from integrating capabilities, not delivering standalone technologies. George called for Defence to build and measure mission-focused digital outcomes, sustain adaptable capabilities, and increase operational testing to ensure AI and digital systems deliver real-world effects rather than simply meeting technical performance metrics.

Panel Four - Innovation and Industrial Power for Competitive Advantage

Exploiting Latent Technologies

David Flanagan, Everfox, encouraged Defence to maximise existing capabilities by exploiting latent technologies rather than relying solely on new innovation. He highlighted how adapting and repurposing technologies already in service can deliver rapid operational benefits, provided users understand what is already available. David stressed that better communication between end users, suppliers and SMEs is essential to uncover hidden potential, shorten innovation cycles and solve operational challenges through collaboration, awareness and creative application of existing technology.

Pacific and Beyond

Fiona Whyte, Strategic Account Director at SiXworks, presented the development of Pacific, a data-centric interoperability platform delivered with Defence Digital for Carrier Strike Group 2025. She demonstrated how close collaboration between industry and the MOD enabled rapid deployment of secure coalition information sharing across multinational platforms. Building on lessons from Carrier Strike Group 2021, Pacific successfully transitioned from experimentation to an operational demonstrator, improving interoperability, enhancing cyber security through zero-trust principles, and establishing a foundation for the future Integrated Mission Partner Environment (IMPE).

Panel Four - Innovation and Industrial Power for Competitive Advantage Cont'd....

How democratic digital states can defend themselves in the age of AI

Priit Liivak, Chief Government Technology Officer, Nortal, outlined Estonia's approach to cyber resilience in the age of AI, highlighting how AI has dramatically reduced the time between vulnerability discovery and exploitation. Drawing on Estonia's experience since the 2007 cyberattacks, he proposed a resilience framework focused on lowering defence costs, raising attack costs and maintaining public trust. He stressed prioritising critical national functions, strengthening digital trust infrastructure, defending at machine speed and improving transparency to ensure nations can withstand sustained cyber attacks.

Special Thanks to Our Day One Panel Chairs

Graham Curtis
Accenture

Kash Addepally
tlmNexus

Luca Leone
Kahootz

Ollie Cowdry
Civica
(TDI Vanguard)

Day One Summary

Day One focused on how Defence must transform its approach to capability delivery, innovation and digital integration to remain operationally relevant in an increasingly contested environment. A recurring theme throughout the conference was the need to accelerate decision-making and capability deployment, moving from traditional procurement timescales measured in years to delivery cycles measured in months, weeks and, where possible, days.

Speakers highlighted the Defence Industrial Strategy, Defence Investment Plan and Defence Industrial Joint Council as the foundations for stronger collaboration between government, industry, academia and international partners. Innovation was consistently framed as delivering operational outcomes rather than technology demonstrations, with increased emphasis on exploiting existing capabilities, scaling proven solutions and ensuring there is a clear route from experimentation to service.

Artificial intelligence, data and digital integration featured prominently. Presentations stressed that success depends not simply on adopting advanced technologies, but on establishing trusted governance, secure data foundations, interoperability and effective deployment at scale. AI was presented as an enabler of faster, better-informed decision-making, supported by robust assurance and human oversight.

Operational lessons from Ukraine reinforced the importance of rapid adaptation, resilient industrial capacity, electronic warfare, counter-uncrewed systems and continuous learning between frontline operators and industry. The conference also showcased practical examples of collaboration, including multinational data-sharing capabilities and Defence AI initiatives, demonstrating how close partnerships between the MOD and industry can accelerate capability delivery. Across every session, the overriding message was clear: Defence must embrace agility, collaboration and continuous innovation to deliver capability at the speed of relevance.

Day Two - Transforming UK Warfighting

Innovation at War Speed: Lessons in Innovation from Ukraine

Quinci Martin, Former US Portfolio Manager for Maritime Assistance to Ukraine, reflected on how Ukraine has transformed wartime innovation through rapid adaptation, close collaboration between frontline forces, industry and government, and accelerated procurement. Drawing on her experience supporting Ukraine's naval forces, she highlighted how autonomous maritime systems and continuous battlefield learning have enabled Ukraine to offset Russian advantages. However, she stressed that innovation alone is insufficient without industrial scale, resilient supply chains and production capacity. Quinci concluded that Ukraine's greatest achievement is building an innovation ecosystem capable of continuously adapting, scaling capability and strengthening the future security of Europe.

Alternative Funding Options for Defence Capability

Air Marshal Andrew Turner CB CBE, Chief Executive of Sabre Capital, reflected on the changes shaping the international security and technology environment. He suggested that the UK must remain alert to a wide range of developing challenges and consider how national resilience may need to evolve. His remarks explored the growing importance of technology, information and infrastructure in future security, alongside the continuing need to adapt traditional approaches. He highlighted areas in which the UK has existing expertise, including advanced technologies, data and space, and encouraged closer cooperation across government, industry and the wider innovation community. He also considered how leadership, investment and procurement could support the development and delivery of new capabilities. Overall, the presentation emphasised the value of long-term planning, strategic collaboration and flexible commercial approaches in helping the UK respond to uncertainty, strengthen its national capabilities and make effective use of emerging opportunities across Defence and security.

The Unseen Warfighter

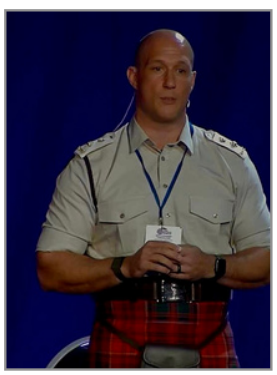
Fiona Scott, Defence Nuclear Enterprise Chief Information Officer, highlighted the critical role industry plays as the "unseen warfighter", arguing that military resilience depends on resilient industrial capability. She identified resilience, data and cybersecurity as three invisible weapons that underpin operational readiness long before equipment reaches the frontline. Fiona challenged organisations to strengthen business continuity planning, supply chain resilience and risk management, warning that cyber attacks, data loss and infrastructure failures directly impact military capability. She emphasised that high-quality data enables predictive maintenance, faster decision-making and greater platform availability, while cybersecurity must be treated as an operational requirement rather than an IT issue. Concluding that capability is built well before deployment, she urged industry to test resilience plans, adopt secure-by-design principles, and ensure people, processes and technology can rapidly recover from disruption to sustain Defence operations in an increasingly contested environment.

Investing in Talent: Building Defence's Digital Future

Molly Cockin and Ciara Cassidy, MOD, (TDI Vanguard) highlighted the importance of diversity as a strategic advantage for Defence, showing how diverse teams make better, faster and more effective decisions. Molly drew on her personal journey to demonstrate how varied experiences, backgrounds and ways of thinking strengthen innovation and problem-solving. Ciara explored how these same principles apply to artificial intelligence, explaining that AI reflects the assumptions and biases of its users rather than thinking independently. She encouraged delegates to use AI as a critical thinking partner rather than simply seeking confirmation of existing views. Together, they demonstrated that diversity must extend beyond representation to include diversity of thought, ensuring Defence develops better technology, makes stronger decisions and remains adaptable to future challenges.

Panel 5 - Delivering the Integrated Force

The Integrated Approach to Defence & The Contribution from Industry



Chris Parker, Director of Government Strategy at Fortinet and Co-Chair of the Team Defence Integration Working Group, reflected on the progress of collaboration between MOD and industry, acknowledging recent challenges while highlighting growing momentum. He stressed the need to share lessons across defence and other critical national infrastructure sectors, improve cyber education, counter misinformation, and create clearer distinctions between commercial and capability discussions to encourage more open engagement. **Lt Col Andy McGrane, C4ISTAR Capability, Strategic Branch,** outlined the Digital Warfighter Group's vision to strengthen Defence's digital workforce, improve retention and develop the specialist skills needed to deliver capabilities such as the Digital Targeting Web. He described plans for a coordinated digital ecosystem bringing together regulars, reserves, civil servants, academia and industry through technical hubs and specialist expertise. Together, they highlighted collaboration, workforce development and shared responsibility as critical to delivering resilient digital capability and maintaining Defence's decision advantage.

Panel 5 - Delivering the Integrated Force Cont'd...

Making it real - A Focused look into the Digital Targeting Web (DTW)

Brig Rich Alston, Deputy Director Integrated Cyber and Electromagnetic Effects, gave a broad update on the Digital Targeting Web and the wider transformation needed to make it work. He described it less as a single system and more as a joined-up way of connecting data, people, platforms and decision-making across Defence, allies and industry. A key theme was that delivery depends as much on culture, governance and collaboration as it does on technology. Rich highlighted the need to combine central direction with faster development at the edge, using common standards while allowing individual commands to build what they need. He also noted that existing capabilities can be brought together more effectively before new investment is added. The overall message was that Defence must change how it works with industry, improve coordination, and focus on practical outcomes if it is to deliver capability at pace and maintain operational advantage over time.

The All-Domain Data Interoperability Capability - Regearing Defence Data

Guy Bewsher, Nexor, presented the All-Domain Data Interoperability capability, a MOD-owned architecture and standard designed to enable secure data sharing across military domains, security classifications, government partners, industry and international allies. Developed over five years, it will provide the reference architecture for the Digital Targeting Web and Maritime Fighting Web. Guy stressed that interoperability, rather than tightly integrated and inflexible systems, is essential for rapidly changing operational environments. He highlighted the need to make data discoverable across potentially hundreds of thousands of battlefield nodes, while allowing information and AI processing to remain at the tactical edge. This would reduce bandwidth requirements and maintain capability when communications are disrupted or denied. The approach aims to connect existing network-centric systems with future data-centric technologies without replacing effective capabilities. Ultimately, it seeks rapid, affordable and near-zero-day interoperability for sensors, decision-support tools, autonomous platforms and effectors, allowing Defence to adopt, replace and scale new technologies more quickly.

Panel 6 - Seizing New Technology Opportunities

Dicky Gray, Senior Director Analyst at Gartner, explored the technologies and operating models likely to shape Defence over the next few years. He highlighted four major trends: faster capability delivery, AI-enabled autonomous systems, sovereign cloud and tactical-edge computing, and post-quantum cybersecurity. Drawing on lessons from Ukraine and commercial responses during COVID-19, Dicky stressed that innovation cycles must shrink from years to around 90 days or less. He noted that future operations will require greater autonomy, interoperable standards and computing power deployed at the edge, particularly when central networks are disrupted. He also warned that Defence and its supply chain must begin preparing now for quantum threats and "harvest now, decrypt later" attacks. His central message was that MOD and industry must work more closely, reduce procurement barriers, strengthen security, and practise rapid delivery before a crisis forces them to do so.

Special Thanks to Our Day Two Panel Chairs

Jim Scott
DefTech Consulting

Colin Johnson
EQ Technologic

Dan Edmunds
Espanaro

Digital Targeting Web Workshop

Record Interest in Digital Targeting Web Workshop at DI26

The Digital Targeting Web (DTW) workshop proved to be one of the highlights of DI26, attracting the highest level of interest ever seen for a DI26 workshop. Building on Brig Rich Alston's DTW presentation, the session was facilitated by John Wharton who was supported by eight members of the joint CSOC and NADG DTW team. It brought together MOD and industry representatives to explore the future of the capability.

Attendees worked through three key DTW themes: Principles, Standards, and Technical Services, generating valuable insights and discussion. The information captured during the workshop is now being reviewed to help shape future development.

As the final session of the two-day event, the workshop provided a fitting conclusion to DI26, showcasing the strength of MOD–Industry collaboration and a shared commitment to delivering outcomes through a One Defence mindset.

Day Two Summary

Day two focused on how Defence can turn strategic ambition into practical capability by accelerating delivery, strengthening digital resilience and deepening collaboration between government and industry. Speakers highlighted the importance of agile institutions, interoperable data architectures and modern digital skills to achieve decision advantage at operational pace. Discussions explored the Digital Targeting Web, digital workforce development and the need for flexible governance that enables rapid innovation while maintaining coherence across Defence.

Several presentations reinforced the critical role of industry as a partner rather than simply a supplier. Sessions demonstrated how existing technologies can be adapted and connected more effectively, while emphasising faster procurement, continuous experimentation and closer collaboration with SMEs. Cyber resilience, data protection and business continuity were presented as operational necessities, with organisations encouraged to strengthen supply chains and prepare for increasingly sophisticated cyber threats.

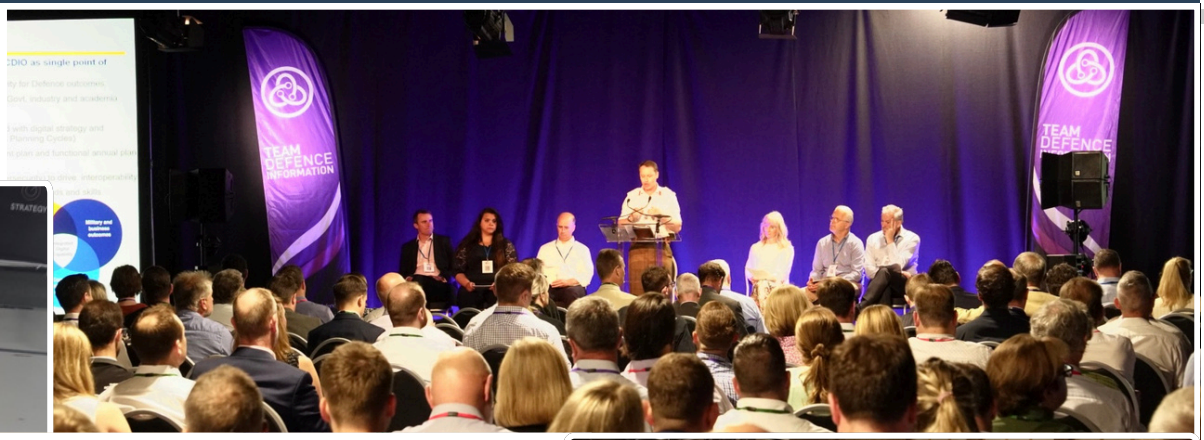
Artificial intelligence remained a central theme, with speakers stressing that success depends not only on advanced models but on trusted deployment, robust governance and diverse perspectives. Presentations also highlighted the importance of inclusive teams, critical thinking and human judgement when adopting AI. Looking ahead, emerging trends such as tactical edge computing, autonomous systems, sovereign digital capability and post-quantum security were identified as priorities. The consistent message throughout the day was that Defence must combine technology, people, culture and partnerships to deliver capability at the speed required by an increasingly contested security environment.

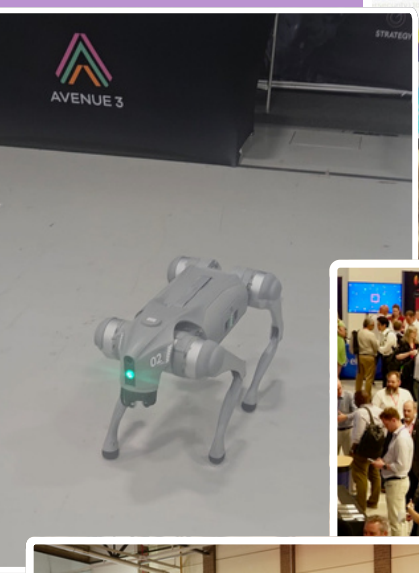
TEAM DEFENCE INFORMATION

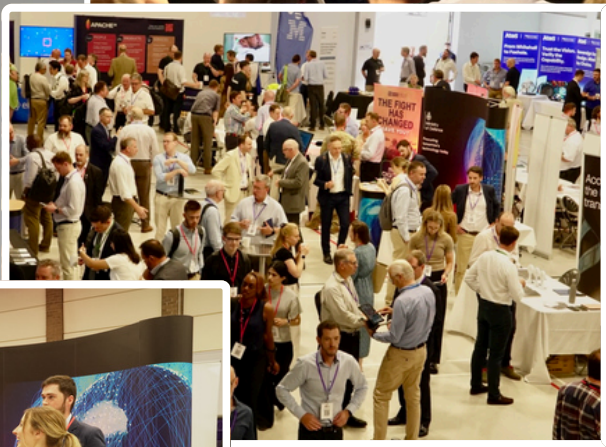
www.teamdefence.info

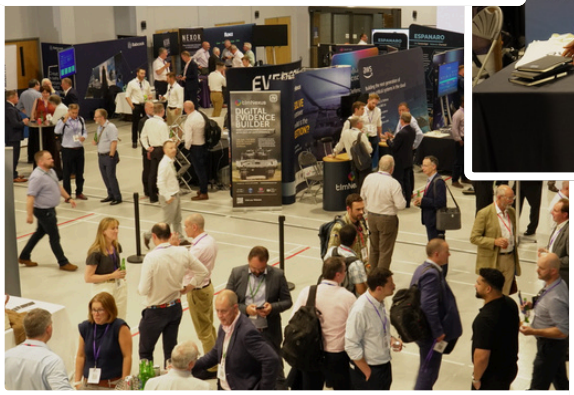
National Armaments Director Group

DEFENCE INFORMATION 2026









www.teamdefence.info

THANK YOU TO OUR SPONSORS

Your support makes this event possible.

PRIME SPONSORS

ESPANARO
eQ Technologic
THALES
kahootz

EVENT SPONSORS

CISCO
EVERFOX
VAST
tlmNexus
DARTER

KEEPING US COOL – A/C SPONSORS

aws
Qlik
fusion
MOODY'S
Atos

THANK YOU TO OUR EXHIBITORS & SUPPORTING SERVICES

Your contribution makes this event possible.

EXHIBITORS

PHOENIX · Bizzdesign · Pennant · CACI · RED SCIENTIFIC · Spectro Cloud

evodia · APACHE IX · TDI VANGUARD · elastic · sas · equinox

Babcock · DEFENCE EYE · IBM · WOMEN IN DEFENCE CHARTER · adarga · DS4D Digital Skills for Defence

LOCKHEED MARTIN · Ministry of Defence · NEXOR · ROKE · DAIC DEFENCE AI CENTRE · THE ACTION BRIDGE

CYBER RANGES CYBER SPACE. ENABLED. · Netcompany · TEAM DEFENCE INFORMATION

SUPPORTING SERVICES

AVON VALLEY SECURITY · EVENTS · MDB Catering · Active Lifestyle Centres