

NEWSLETTER



A New Era for Team Defence Panel One

Charles Forte opened DI25 by highlighting the importance of collective defence and warned that failing to embrace innovation risks irrelevance. Charlie emphasised that modern warfare is now defined by software and data, and the Strategic Defence Review reflects this shift. He called for wholesale changes in how defence operates, warning that small adjustments are insufficient. Key challenges identified include understanding global competition, adopting new ways of working, and building a supplier ecosystem that supports SMEs.



The Military Strategic Headquarters

Lt Gen Tom Copinger-Symes announced the transformation of UK Strategic Command into the Cyber and Specialist Operations Command, focused on integrating cyber and electromagnetic capabilities. He called for a whole-of-society approach, involving industry, academia, and citizens in national defence. As lead command, it will ensure coherent cyber operations.

He also outlined a digital targeting web to link sensors and effectors for faster decision-making, stressing the need for collaboration with Defence Digital, system integration, and effective use of data, people, and tradecraft.



Treating Data as a strategic asset and the lifeblood of the Integrated Force

Caroline Bellamy stressed that data is a strategic asset and must be exploitable by design. She called for collaboration, diversity of thought, and a unified digital approach across defence. Tools like the digital targeting web need to be built through partnership, not bought. Her message: seize the moment for digital, data, and AI transformation—with people at the centre.



Emerging technologies and their effect on global security

Rear Admiral Massimo Esposito emphasised NATO's focus on emerging technologies to strengthen defence capabilities and maintain a competitive edge. He highlighted the critical need for international cooperation, including sharing intelligence and aligning on security goals. He also stressed the importance of ethical, legal, and responsible use of new technologies to ensure trust and compliance across nations.





Ministry
of Defence

Panel Two

War at the Speed of Light



Nigel Shaw stressed the urgent need to speed up defence delivery, integration, and decision-making. He highlighted how capability centres and digital tools like model-based engineering and AI can cut timelines and improve outcomes. Embracing AI and tighter collaboration are key to staying ahead of evolving threats.

An Air perspective of the New Era



Arif Mustafa highlighted that digital is mission-critical for the RAF. RAF Digital is boosting combat readiness through AI, data, and innovation, with tools like Ballistic and Raven. The focus is on speed, impact,

strong governance, and collaboration to stay ahead in modern warfare.

Speed to scale: Transforming the UK Defence Industrial Base



Aditi Charanji explained how cloud and AI technologies can help transform defence by enabling faster scaling, automation, and better decision-making. Using Amazon's own examples, she showed how these tools free teams to focus on high-value work. She encouraged defence organisations to explore these solutions to innovate, cut costs, and improve efficiency.

Powering the Fight: How the Digital Backbone Enables Faster Targeting



Mivy James emphasised the digital backbone as critical to Defence—an integrated, secure tech ecosystem enabling faster, smarter operations. It connects people, data, and systems, supports real-time targeting, and requires industry to build open, reusable, scalable solutions. Bottom line: To stay ahead, Defence must build fast, integrate widely, and adapt continuously—with the backbone at the core.

15 years in - a view from the SME “front line”



Robin King discussed how SMEs can better engage in defence innovation by focusing on ecosystem collaboration rather than rigid strategies. He highlighted challenges like complex procurement, high risk, and funding barriers, stressing the need for strong business planning and alignment with user needs. Increasing investment and defence strategies offer opportunities, but success depends on building trusted relationships, improving communication, and adapting culture and procurement processes to support faster, effective innovation.



Panel Three & Panel Four



Digital Skills for Defence in the New Era



Claire Fry highlighted the need for an integrated defence ecosystem combining diverse talent and fostering a culture of innovation and collaboration. She praised ongoing digital skills programs and new career models, stressing that strong partnerships are vital to meeting future challenges and securing the nation's safety.



AI Skills & Talent: Crafting the Agile workforce for tomorrow

Heidi Edwards leads AI skills in defence, focusing on building AI literacy and safe use through tailored training programs. Her AI Centre of Expertise has trained 5,000 staff and grown a community of 1,600 members. She highlighted the success of Chat MOD, a widely used AI chatbot supporting defence operations.



Reducing the Cyber Risk to Defence and beyond

Eleanor Fairford stressed urgent cyber threats and the need to harden critical systems, enforce supplier security standards, and embed secure-by-design practices. She highlighted the importance of collaboration across the CISO network and supply chain to reduce cyber risk



Digital Foundry: Our journey on accelerating software deployment into frontline capabilities



David Tagg-Oram described Defence Digital's secure, resilient platform enabling fast, user-focused software and AI delivery. Key aims: support warfighters, integrate with allies, ensure resilience, and boost industry collaboration. A new portal will simplify access soon.

Digital Sovereignty - The key to securing collaboration across hybrid multicloud environments

Tim Phipps explained that most cloud breaches come from human error and misconfigurations. He stressed controlling data and encryption keys outside the cloud, secrets and API management, and using confidential computing to protect data in use. He highlighted the importance of preparing for breaches with data discovery, threat monitoring, and recovery plans. Lastly, he emphasised making workloads portable for flexibility and that cloud security requires teamwork and ongoing effort.



Panel Five



Ministry
of Defence



Continually Improving Commercial Practices for Digital Acquisitions



Victoria Cope discussed accelerating defence procurement to meet emerging threats by working closely with industry. She emphasised innovation, collaboration with SMEs and startups,

and a cultural shift toward speed and flexibility. Key initiatives like Asgard and the Defence Tech Scaler support this mission-focused approach. Commercial strategy is crucial for delivering timely defence capabilities, and ongoing partnership is encouraged.

How do we accelerate our efforts to harness AI



Hugh Woodward highlighted AI as vital for the UK's military future, stressing rapid, safe adoption through collaboration across defence, government, and industry. The Defence AI Centre coordinates efforts to harness AI's power and set standards. He warned that without swift action, the UK risks falling behind adversaries.



Digital Superiority: Outpacing the Threat Through Digital Acceleration

Luca Leone and Gareth Hetheridge emphasised that to achieve digital superiority by 2035, the UK defence sector needs steady funding, faster innovation adoption, and integrated teams focused on delivering digital solutions. They highlighted the importance of evolving procurement to prioritise digital, using agile methods, and empowering decentralised leadership. Citing Ukraine's rapid tech adoption as an example, they stressed that speed and collaboration are essential to stay ahead of threats and protect forces.

Day One Summary

Day One of the conference highlighted the urgent need for the UK defence sector to embrace digital transformation through sustained funding, agile innovation, and closer collaboration between industry and the Ministry of Defence. Speakers emphasised the importance of integrating digital technology at the core of defence programmes, adopting flexible commercial models, and empowering decentralised leadership to accelerate delivery and adaptability. Drawing on lessons from global examples like Ukraine, the consensus was clear: success depends on rapid iteration, effective adoption of new technologies, and a unified approach to safeguarding national security in an unpredictable and fast-changing world.



Ministry
of Defence

Panel Six

Insights into the realities of the conflict in Ukraine



Elizabeth Bullock spent three years in Ukraine during the war, witnessing its harsh realities and the resilience of Ukrainians. She challenged myths about language and loyalty, explained the frontline fighting, and noted normal life elsewhere despite attacks. Elizabeth also highlighted the ongoing hybrid warfare involving propaganda, cyber attacks, and other tactics.

Defence Reform: The benefits for the Ministry of Defence, Industry and the UK



Giles Ahern outlined the UK's ongoing defence reform to improve efficiency, simplify complex systems, and enhance collaboration across the Ministry of Defence. Key changes include streamlined leadership, integrated military command, and closer ties with industry and academia for better capability development. Cultural and financial shifts are major challenges. The reform aims to deliver stronger defence capabilities, better value, and improved support for personnel and industry partners.

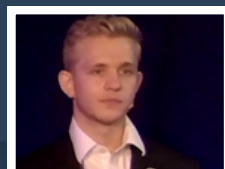
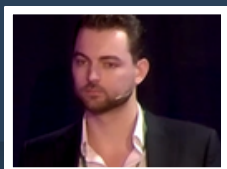
Collaborating to Secure the Supply Chain - Defence Cyber Certification



Air Cdre Mike Wilson outlined efforts to improve cyber resilience in the UK defence supply chain. He introduced Secure by Design for building security into defence products and the Cyber Security Model v4 to assess supplier resilience. He also announced the Defence Cyber Certification scheme to recognise strong cybersecurity practices. Despite challenges, he urged immediate action to reduce risk and protect frontline personnel.

A Vanguard Perspective on the 2025 Strategic Defence Review

TDI Vanguard's Edward Gunning, Ollie Organ and Rhodri Andrews urged defence to modernise by attracting Gen Z through better branding, flexible careers, and faster recruitment. Data and AI must be harnessed with fewer barriers, empowering young talent to drive innovation and build a future-ready force.

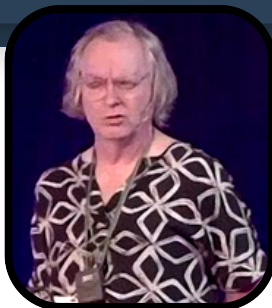


Panel Seven



The role of Academia and Innovation in Supporting MOD and UK Defence Industry

Dr Adam Zagorecki emphasised rapid tech change in defence, especially AI and cyber security, requiring skilled leaders. Universities must adapt with flexible programs and strong industry collaboration to develop talent and maintain UK's defence capabilities.

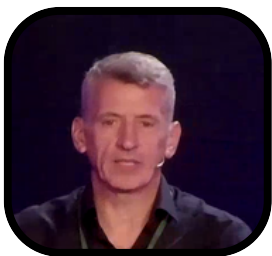


Streamlining Data to Decisions: Delivering Real Situational Intelligence at the Speed of Command

Victoria Needham explained how Apache Kafka powers real-time data processing in defence and beyond, improving situational intelligence by delivering

actionable insights. Kafka modernises legacy systems, supports cyber defence, supply chain, and edge use cases, acting as a digital backbone that connects frontline devices to data centres and enhances AI with quality data.

Gartner - A Future Perspective



Michael Spiteri outlined how by 2030, AI and innovation will reshape work and organisations with faster, horizontal decision-making systems. He emphasised AI's role in augmenting—not replacing—humans, the rise of edge computing, and the need

for strong governance to manage risks like data trust. Success will depend on agility, ecosystem partnerships, and better AI adoption beyond incremental improvements.



Quantum computing from future vision to near term reality

Richard Hopkins highlighted that quantum computing could break current encryption by 2035, creating risks and opportunities. IBM is working on both advancing quantum tech and protecting against its threats.

Caroline Cantrell explained IBM's tools to detect vulnerabilities and implement quantum-safe security, stressing the need to start preparing now.



The Implications for Team Defence in the New Post SDR Era

Chris Parker stressed the need for culture change in MOD to encourage risk-taking, faster decisions, and better industry collaboration. He urged involving smaller innovators, improving relationships through more frequent awareness meetings, and addressing budget waste via independent brokerage. Chris highlighted the importance of collaboration in defence's digital space and efforts to improve industry access to MOD resources. The focus is on openness, agility, and teamwork to drive progress.

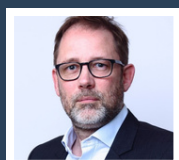


Day Two Summary

Day Two focused on rapid tech change in defence, highlighting the need for skilled leaders, flexible education, and stronger ties between academia and industry. Key themes included the risks and opportunities of quantum computing, the urgency of quantum-safe security, and the role of real-time data in modern defence. AI and innovation are expected to transform decision-making by 2030, requiring governance, agility, and collaboration. A cultural shift in defence was urged to support faster decisions, risk-taking, and broader industry engagement.

Panel Chairs

We would like to thank our panel chairs for their valuable contributions and expert guidance in leading thoughtful and engaging discussions throughout the conference.



Panel One Chair

James Mansfield
Sopra Steria

Panel Two Chair

Graham Curtis
Accenture UK



Panel Three Chair

Alan Walker
1EQ

Panel Four Chair

Justin Walker
Thales UK



Panel Five Chair

Tony Harris
tlmNexus



Panel Six Chair

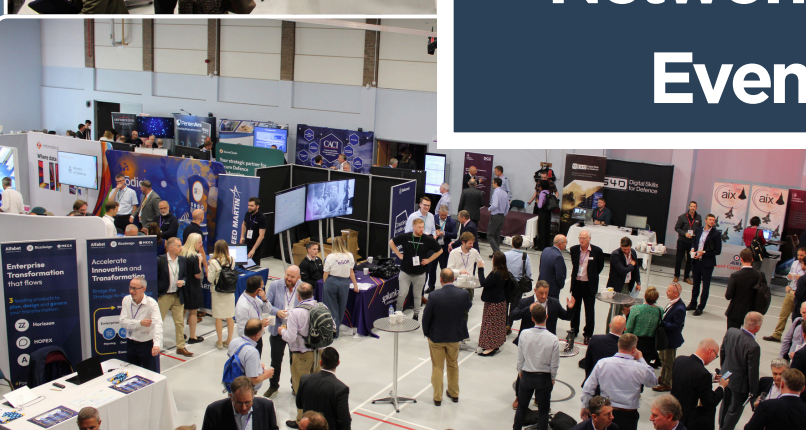
Jim Scott
Lockheed Martin UK

Panel Seven Chair

John Dee
Somerford



Network Extra Evening



THALES

 **eQ Technologic**

kahootz

Event Sponsors

 **tImNexus**

 **CISCO**

 **SOMERFORD
CONFLUENT**

 **VAST**

 **aws**

Exhibitors

 **Armour
Comms**

 **CACI**

 **HELYX™**

 **RED
SCIENTIFIC**

 **DAIC
DEFENCE AI CENTRE**

 **Defence
Capability
Centres | DEC
DIGITAL ENGINEERING CENTRE**

 **TFD Global**

 **Bizzdesign**

Netcompany

 **WHITETREE**

 **LOCKHEED MARTIN**

 **elastic | The Search
AI Company**

EVERFOX

 **splunk>
a CISCO company**

 **evodia**

 **AllanWebb**

 **IBM**

 **DCC
Defence Cyber Certification**

 **Babcock**

 **PHOENIX**

 **SecureCloud+**

 **TIA | TIA GROUP**

 **Informatica**

 **PentenAmio**

MOD Zone

 **DCC
Defence Cyber Certification**

 **Ministry
of Defence
Digital Commercial**

 **DAIC
DEFENCE AI CENTRE**

 **Ministry
of Defence
Digital Skills for
Defence**

 **Defence
Capability
Centres | DEC
DIGITAL ENGINEERING CENTRE**

 **Ministry
of Defence
RAF Nexus**

Supporting

 **SMG
EVENTS**

 **e50K
STRATEGIC ADVISORY**

 **UK
AFCEA
WEST**

 **cityforum
cutting through**

 **Cranfield
University**

 **WOMEN IN
DEFENCE
CHARTER**