Governance of Army Security

The Chief of the General Staff (CGS) is the Army Senior Risk Owner (SRO) and sets the Army's security risk appetite. Director Information (D Info) is the Senior Security Risk Coordinator (SSRC), the Senior Information Risk Owner (SIRO) for the Army and manages TLB risk on behalf of CGS. D Info is also the Functional lead for intelligence and security within the Army. Head of Cyber and Security (Hd CySy) is the Army Chief Security Officer, incorporating the role of Chief Information Security Officer (CISO). Assistant Head (AH) Counter-Intelligence and Security, is the Army Principal Security Advisor (PSyA), and professional head of security providing physical, cyber and personnel security policy, assurance and advice as well as overseeing Army Counter-Intelligence & Security operational activity. The operational chain of command is responsible for Security Risk Management, fully supported by Home Command in the Firm Base, with Counter-Intelligence & Security specialists embedded across the force as required.

Summary

The focus remains on reducing risk to the Army operating overseas and at home. The Army will ensure an appropriate effort enables the Field Army and JHC to fight and win wars on land and is fully supported and enabled by Home Command. A next-generation approach supports readiness, improves interoperability and protects critical advantage, enabling the Army to protect the UK.

Complete the survey

Agenda

08:40 Registration, breakfast and networking

09:30 Opening Remarks

10:00 Plenary session: Army SMARTBase Concept

10:30 Coffee and Networking

11:05 Breakout Sessions

Session 1: Physical Security -
"Testing our Physical Security"
Room: Olivier 2nd floor

Session 2: Personnel Security -
"Security Issues that Emanate from our People"
Room: St James

11:55 Plenary session:
"What threats does industry see coming and what tools do they have to combat them?"

12:40 Lunch and Networking

13:45 Plenary session: Army Security Culture and Incidents

14:50 Breakout Sessions

Session 1: Cyber Security -
"Approaches to Defensive Cyber"
Room: St James

Session 2: Resilience and Business Continuity -
"What are we protecting and why?"
Room: Olivier 2nd floor

15:35 Coffee and Networking

16:05 Panel Discussion

16:50 Closing Remarks

17:05 Break

19:00 Pre-dinner Drinks and Networking

19:45 Dinner

Explore the agenda in full

ARMY COUNTER-INTELLIGENCE AND SECURITY CONFERENCE

Chief Disruptor · Army · babcock · BT Means Business · Varonis · Everfox · Cellebrite · Tanium · Capgemini · Global EMC – Electromagnetic Shielding & Anechoics

Information Directorate Counter-Intelligence and Security branch

Context

The Army (our people, capability, and information) is a high priority target for a range of hostile actors, both at home and overseas, seeking to understand and contest freedom to operate.

The pace of geopolitical and technological change combined with environmental and financial constraints and a growing global economic divide, sees the threat landscape evolving more rapidly than ever. Threat convergence between the UK and deployed operations and rapid technological change sees the British Army exposed to a more significant, but less well understood security threat than at any other time in our history.

Exploitation of the electro-magnetic spectrum and cyberspace, along with digitisation and rapid adoption of technology, including within our personal lives further represent a technically complex and evolving challenge to security. To counter this multi-faceted and dynamic threat and to ensure resilience, the Army must maintain a constant state of vigilance, awareness, and active preparedness.

The Army will put culture, education, deterrence, leadership, and collaboration at the heart of security, modernising to best support Army critical outputs. This is a whole force approach (military, civil servant, contractor and industry), integrated across Defence and with Partners Across Government.

Army Security Plan

The Army's Security Plan drives an operational approach to protect systems, personnel, cyberspace, and capability at home and overseas, supporting the orchestration and delivery of land power. It will enhance physical, cyber and personnel security controls, protections, including a pervasive security culture to support continuity of operations and freedom of manoeuvre for land forces. This requires a deliberate shift to a more operationalised footing.

The Army Security Plan will be delivered and overseen through an incremental business improvement approach. Not a formal capability programme, it coheres new and existing lines of effort in a focused approach referred to as "next-generation security".

Security (including counter-intelligence) and resilience are essential enablers for protecting the conceptual, moral and physical components of fighting power. The Army Security Plan, will develop next-generation security by:

- *Focusing on criticality of outputs to guide operational security priorities to reduce threat, risk and harms.*
- *Adopting a dynamic approach to the apportionment of finite resources focused on cyber, physical and personnel security threats.*
- *This will be underpinned by the ongoing security culture change programme.*

Three Year Outlook

Next-generation approach to security.

The Army will align the security effort to Army outputs. Security is a command-led activity to ensure continuity of operations. It maximises the benefits of technology and drives a more dynamic threat focused response to risk reduction. The following key deliverables are central to the concept of next generation security:

- **A focus on what is critical, not on process: ensure the most valuable assets are protected and appropriately resilient. Securing the Army contribution to Defence Outputs.**
- **Underpinned by data, the adoption of a threat driven approach to understand and contest the convergence of physical, cyber and personnel security threats.**
- **Consider counter-intelligence and security as a routine operation at home and overseas.**
- **Professionalisation of the Army Security Function.**
- **Audit and Assurance to enable continuous improvement**