CHIEF DISRUPTOR

ARMY

babcock™

GLOBAL EMC
ELECTROMAGNETIC SHIELDING & ANECHOICS
EST. 1994

TANIUM.

VARONIS

Capgemini

Cellebrite

EVERFOX

BT Means Business

CHIEF DISRUPTOR

ARMY

babcock™

GLOBAL EMC
ELECTROMAGNETIC SHIELDING & ANECHOICS
EST. 1994

TANIUM.

VARONIS

Capgemini

Cellebrite

EVERFOX

BT Means Business

WELCOME TO THE

Chief Disruptor
Army Counter-Intelligence and Security Conference

MORNING AGENDA

09:30 Opening Remarks

10:00 Plenary session: Army SMARTBase Concept

10:30 Coffee and Networking

11:05 Breakout Sessions
SESSION A: Physical Security - "Testing our Physical Security"
SESSION B: Personnel Security - "Security Issues that Emanate from our People"

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

12:40 Lunch and Networking

AFTERNOON AGENDA

13:45 Plenary session: Army Security Culture and Incidents

14:50 Breakout Sessions
SESSION A: Cyber Security - "Approaches to Defensive Cyber"
SESSION B: Resilience and Business Continuity - "What are we protecting and why?"

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

Opening Remarks

Richard Morgan

Founder, Chief Disruptor Defence

Lieutenant General Sharon Nesmith DCB

Deputy Chief of the General Staff

Major General John Collyer

Director Information and Army CIO

Kristina Evans

Head of Cyber and Security, British Army

Ministry of Defence
Ministry of Defence
Ministry of Defence
Ministry of Defence

Opening Remarks: Major General John Collyer – Director Information

ARMY

CHIEF DISRUPTOR

Ministry of Defence

babcock™

BT Means Business

EVERFOX

Cellebrite

TANIUM™

VARONIS

GLOBAL EMC
-ELECTROMAGNETIC SHIELDING & ANECHOICS-

Capgemini

National Protective
Security Authority

Strategic Command
Defence Digital

National Cyber
Security Centre

ARMY

Opening Remarks: Kristina Evans – Head of Cyber and Security

ARMY

CHIEF DISRUPTOR

Ministry of Defence

babcock™

BT Means Business

EVERFOX

Cellebrite

TANIUM™

VARONIS

GLOBAL EMC
-ELECTROMAGNETIC SHIELDING & ANECHOICS-

Capgemini

National Protective Security Authority

Strategic Command
Defence Digital

National Cyber Security Centre

ARMY

Plenary session:
Army SMARTBase Concept

Colonel David Duncan

Principal Security Advisor (Army)

Sally Wareham

Assistant Head Digitalisation, British Army

Craig Collins

Digital Lead Innovation Architect, British Army

ARMY SECURITY CONFERENCE

INTRODUCTION

The Army approach – what we mean by “next-gen” security?

- Putting the needs of the Army at the heart of all activity to ensure an appropriate level of security.
- Reduce strategic and operational risk to the mission and risk to the force.

Why we need to adopt this approach – an evolving strategic threat.

- **Cyber security** threats are increasing at a time when the Army is undergoing digital transformation to become a data centric organisation.
- **Physical security** threats can result in loss of capability, reputational damage and impact our licence to operate.
- **Personnel security** threats from adversaries and insiders requires a specific focus.
- **Resilience** of Army critical outputs to ensure continuity of operations.

The Army response – the Army Security Plan to delivery “next-gen” security.

- Address the strategic threat and reduce risk to the Army operating overseas and home.
- Security and counter-intelligence as an enabling function to support readiness, interoperability and
- operational advantage.
- Adopt a threat driven, data centric approach maximising technological advantage.

DIGITAL
TRANSFORM
Ai
THEIA

SMARTBase Concept

THEIA – SMARTBASE

DEFINITION AND VISION

PEOPLE, Process, Technology and Data Improving the Lived Experience

SMARTBase

Definition

- A SMARTBase is a military installation that leverages advanced technologies and data-driven solutions to enhance operational efficiency, security, and sustainability.

Vision

- To exploit innovation, research and experimentation that enables the base to meet its outcomes in a secure, efficient and effective manner whilst improving the lived experience for all
- Innovation site enablement for additional trials collaborating with other FLC's, Organisations and Partners

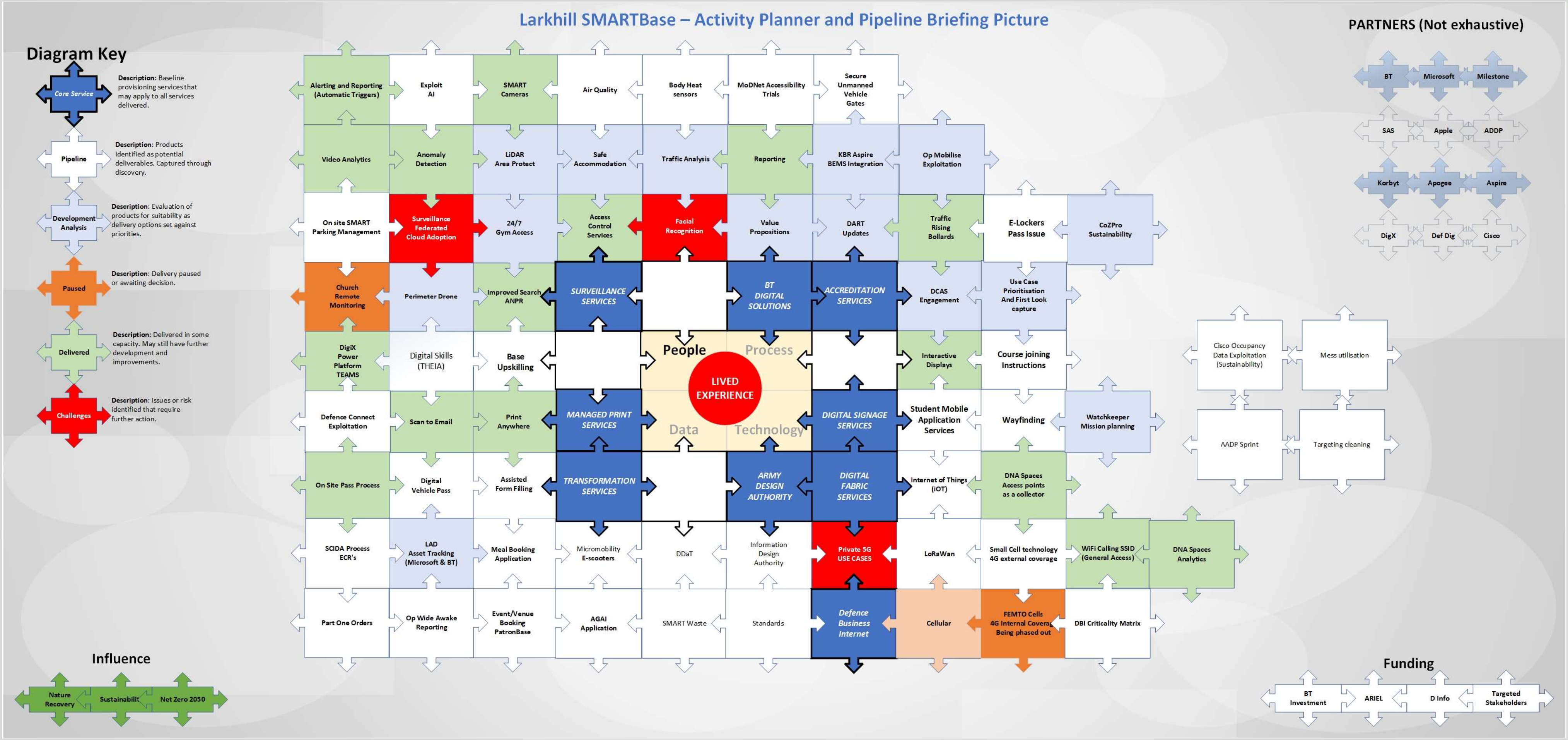
"Learn by Doing"

THEIA

THEIA – SMARTBASE

JIGSAW APPROACH (MORE THAN SURVEILLANCE)

SMARTBase



Larkhill SMARTBase – Activity Planner and Pipeline Briefing Picture

Diagram Key

- Core Service — **Description**: Baseline provisioning services that may apply to all services delivered.
- Pipeline — **Description**: Products identified as potential deliverables. Captured through discovery.
- Development Analysis — **Description**: Evaluation of products for suitability as delivery options set against priorities.
- Paused — **Description**: Delivery paused or awaiting decision.
- Delivered — **Description**: Delivered in some capacity. May still have further development and improvements.
- Challenges — **Description**: Issues or risk identified that require further action.

Alerting and Reporting (Automatic Triggers)	Exploit AI	SMART Cameras	Air Quality	Body Heat sensors	MoDNet Accessibility Trials	Secure Unmanned Vehicle Gates				
Video Analytics	Anomaly Detection	LiDAR Area Protect	Safe Accommodation	Traffic Analysis	Reporting	KBR Aspire BEMS Integration	Op Mobilise Exploitation			
On site SMART Parking Management	Surveillance Federated Cloud Adoption	24/7 Gym Access	Access Control Services	Facial Recognition	Value Propositions	DART Updates	Traffic Rising Bollards	E-Lockers Pass Issue	CoZPro Sustainability	
Church Remote Monitoring	Perimeter Drone	Improved Search ANPR	*SURVEILLANCE SERVICES*		*BT DIGITAL SOLUTIONS*	*ACCREDITATION SERVICES*	DCAS Engagement	Use Case Prioritisation And First Look capture		
DigiX Power Platform TEAMS	Digital Skills (THEIA)	Base Upskilling		People	Process		Interactive Displays	Course joining Instructions		
Defence Connect Exploitation	Scan to Email	Print Anywhere	*MANAGED PRINT SERVICES*	Data	Technology	*DIGITAL SIGNAGE SERVICES*	Student Mobile Application Services	Wayfinding	Watchkeeper Mission planning	
On Site Pass Process	Digital Vehicle Pass	Assisted Form Filling	*TRANSFORMATION SERVICES*		*ARMY DESIGN AUTHORITY*	*DIGITAL FABRIC SERVICES*	Internet of Things (iOT)	DNA Spaces Access points as a collector		
SCIDA Process ECR's	LAD Asset Tracking (Microsoft & BT)	Meal Booking Application	Micromobility E-scooters	DDaT	Information Design Authority	Private 5G USE CASES	LoRaWan	Small Cell technology 4G external coverage	WiFi Calling SSID (General Access)	DNA Spaces Analytics
Part One Orders	Op Wide Awake Reporting	Event/Venue Booking PatronBase	AGAI Application	SMART Waste	Standards	*Defence Business Internet*	Cellular	FEMTO Cells 4G Internal Coverag Being phased out	DBI Criticality Matrix	

LIVED EXPERIENCE

Cisco Occupancy Data Exploitation (Sustainability)

Mess utilisation

AADP Sprint

Targeting cleaning

PARTNERS (Not exhaustive)

BT	Microsoft	Milestone
SAS	Apple	ADDP
Korbyt	Apogee	Aspire
DigX	Def Dig	Cisco

Influence

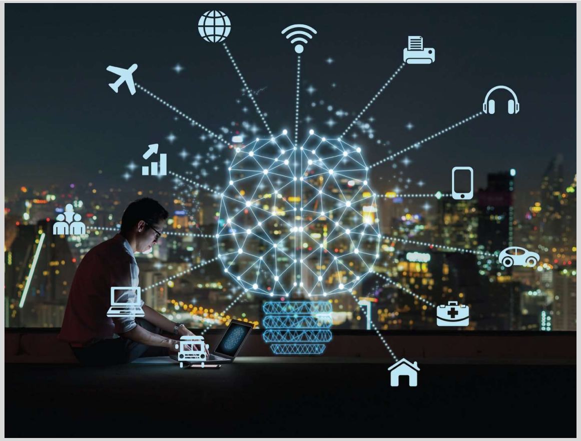
Nature Recovery | Sustainabilit | Net Zero 2050

Funding

BT Investment | ARIEL | D Info | Targeted Stakeholders

THEIA

THEIA – SMARTBASE
KEY COMPONENTS



Intelligent Infrastructure

- Enhanced communication networks (secure and resilient connectivity)
- Advanced energy management systems (renewable energy integration, energy-efficient buildings
- Smart grid technology for optimized energy distribution and consumption

Projected sales of main products in 2013
Distribution of market share among the major industry players
Share of market activity
Passive market share

Data and Analytics

- Real-time data collection and analysis for informed decision-making
- Internet of Things (IoT) devices and sensors to monitor base operations
- Predictive analytics for improved resource allocation and maintenance

Enhanced Security and Surveillance

- Advanced surveillance systems for perimeter security and threat detection
- Biometric identification and access control for enhanced personnel security
- Integration of artificial intelligence for proactive threat assessment

THEIA – SMARTBASE

Data Security

- Protecting sensitive military information from cyber threats
- Implementing robust cybersecurity measures and encryption protocols.

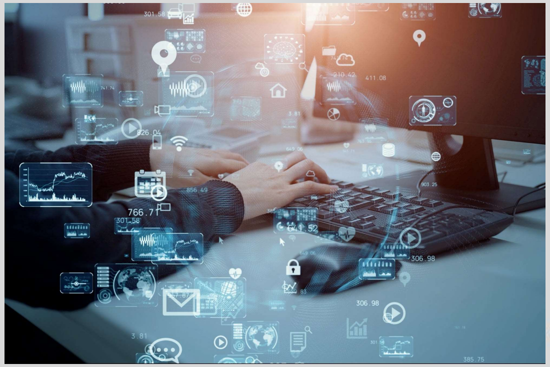
Legacy Infrastructure

- Upgrading existing infrastructure to support smart technologies
- Retrofitting older buildings with energy-efficient systems

Training and Adoption

- Providing comprehensive training to personnel for technology adoption
- Encouraging a culture of innovation and embracing new technologies

SMARTBase



THEIA

THEIA – SMARTBASE

BENEFITS

Operational Efficiency

Streamlined logistics and supply chain management

Optimal resource allocation for maintenance and repairs

Automation of routine tasks to free up personnel for critical operations

Enhanced Security

Early threat detection and rapid response capabilities

Secure and resilient communication networks

Real-time situational awareness through data integration and analytics

Environmental Sustainability

Reduced energy consumption and carbon footprint

Efficient waste management and recycling programs

Integration of renewable energy sources for power generation

THEIA – SMARTBASE

SURVEILLANCE DRIVING SITUATIONAL MANAGEMENT

SMARTBase

Single Pane of glass

Right Information to the right person

Operational manageme nt in one place

Regulatory & Statutory compliance

Actionable intelligence & insight

Foundation for future SMART services

European Commission GDPR General Data Protection Regulation

National Protective Security Authority

bsia british security industry association

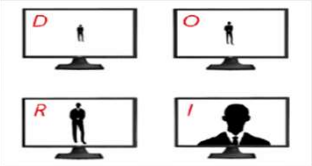
OFFICE OF THE BIOMETRICS AND SURVEILLANCE CAMERA COMMISSIONER

NDAA Compliant

ONVIF®

[dstl] The Science Inside

Martyn's Law

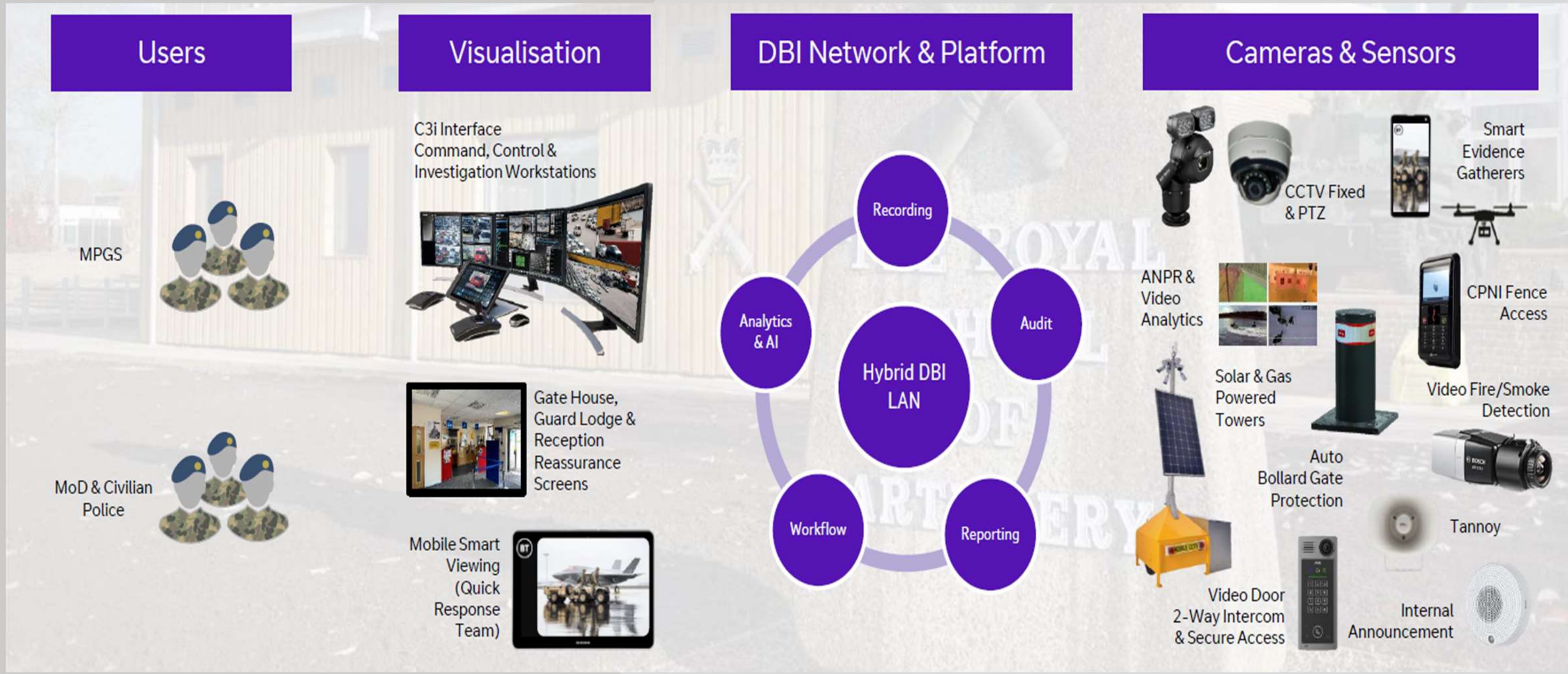


THEIA

THEIA – SMARTBASE

SURVEILLANCE CAPABILITY OVERVIEW

SMARTBase



Users
Visualisation
DBI Network & Platform
Cameras & Sensors
MPGS
MoD & Civilian Police
C3i Interface Command, Control & Investigation Workstations
Gate House, Guard Lodge & Reception Reassurance Screens
Mobile Smart Viewing (Quick Response Team)
Recording
Audit
Reporting
Workflow
Analytics & AI
Hybrid DBI LAN
CCTV Fixed & PTZ
Smart Evidence Gatherers
ANPR & Video Analytics
CPNI Fence Access
Solar & Gas Powered Towers
Video Fire/Smoke Detection
Auto Bollard Gate Protection
Tannoy
Video Door 2-Way Intercom & Secure Access
Internal Announcement

THEIA

THEIA – SMARTBASE

SURVEILLANCE - SPOTLIGHT

Surveillance

- **Milestone** – IP Video Management Software
- **BriefCam** – Video Analytics Platform

Video Content Analytics

- Video Synopsis enable rapid video review and search
- Real time alerting and reporting, automating response
- High quality and GDPR compliant export

Access Control Services

- **Gallagher – Site access**
- Secure unmanned entry
- PED Controlled Access

Informed User Communities

- DTE, Guarding Review and Dorset Innovation Park (BattleLab), Chicksands,
- Informed Navy and RAF trials

Attain Situational Awareness

Leverage advanced analytics for real-time notifications to balance sensitivity, accuracy

Accelerate Investigations

Review hours of video in minutes and rapidly pinpoint objects of interest

Derive Operational Intelligence

Derive quantitative insights for operational efficiency and data driven decision making

Real -Time Alerts

Face Recognition

Notifications

Line Crossing

Smart Alerts

Proximity Identification

People Counting

License Plate Recognition

SMARTBase

THEIA

Surveillance – The Future

THEIA – LARKHILL SMARTBASE

SURVEILLANCE – THE FUTURE

- **Centralised Monitoring and Control**
  - Virtual operations centre
  - Global or geographically located
  - Shared resources
- **Unmanned Entry/Exit points**
  - ANPR Check, colour, type, facial recognition
  - Body heat sensor
  - Digital pass checked
  - Automated triggers for event response
- **Internal facing cameras**
  - Tracking breaches and incidents
  - Drone trackers/Robotic Dogs
  - Signage displaying actions to be taken
  - Mobile app targeting communities
- **Enterprise Site access management services**
  - Stronger security posture
  - Improved user experience, singe solution
  - Data collection for insights
- **Data Fusion**
  - Surveillance, ACS, Printing, Browsing data ??
- **Army Efficiency Initiative**
  - 6 Pilot Sites

SMARTBase

THEIA

THEIA – SMARTBASE

LINES TO TAKE - OBSERVATIONS

Pilot

- This is a pilot and may not be the final solution. We know that there are areas where it isn't the complete package; this was about showing what technology could do to optimise the available workforce.

Access Control +

- Access control is but one part of it and there are significantly more opportunities alongside the Sy element.

Policy

- There is work to be done in terms of policy, permissions and authorities to maximise available tech; use of biometrics, facial and voice recognition, ANPR, etc.

Automation

- Automated perimeter monitoring and intruder detection has significant opportunity to maximise the available workforce.

THEIA – SMARTBASE

TAKEAWAYS

Technology

- SmartBases utilise technology to optimize military operations, enhance security, and promote sustainability.

Benefits

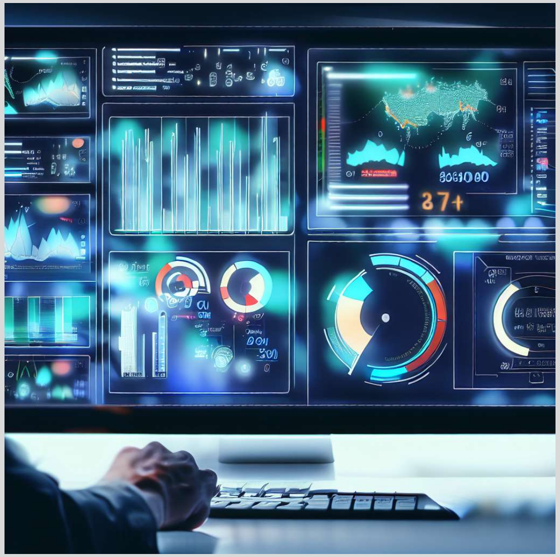
- They offer benefits such as operational efficiency, improved security, and reduced environmental impact.

Challenges

- Overcoming challenges like data security, legacy infrastructure, and training is crucial for successful implementation.

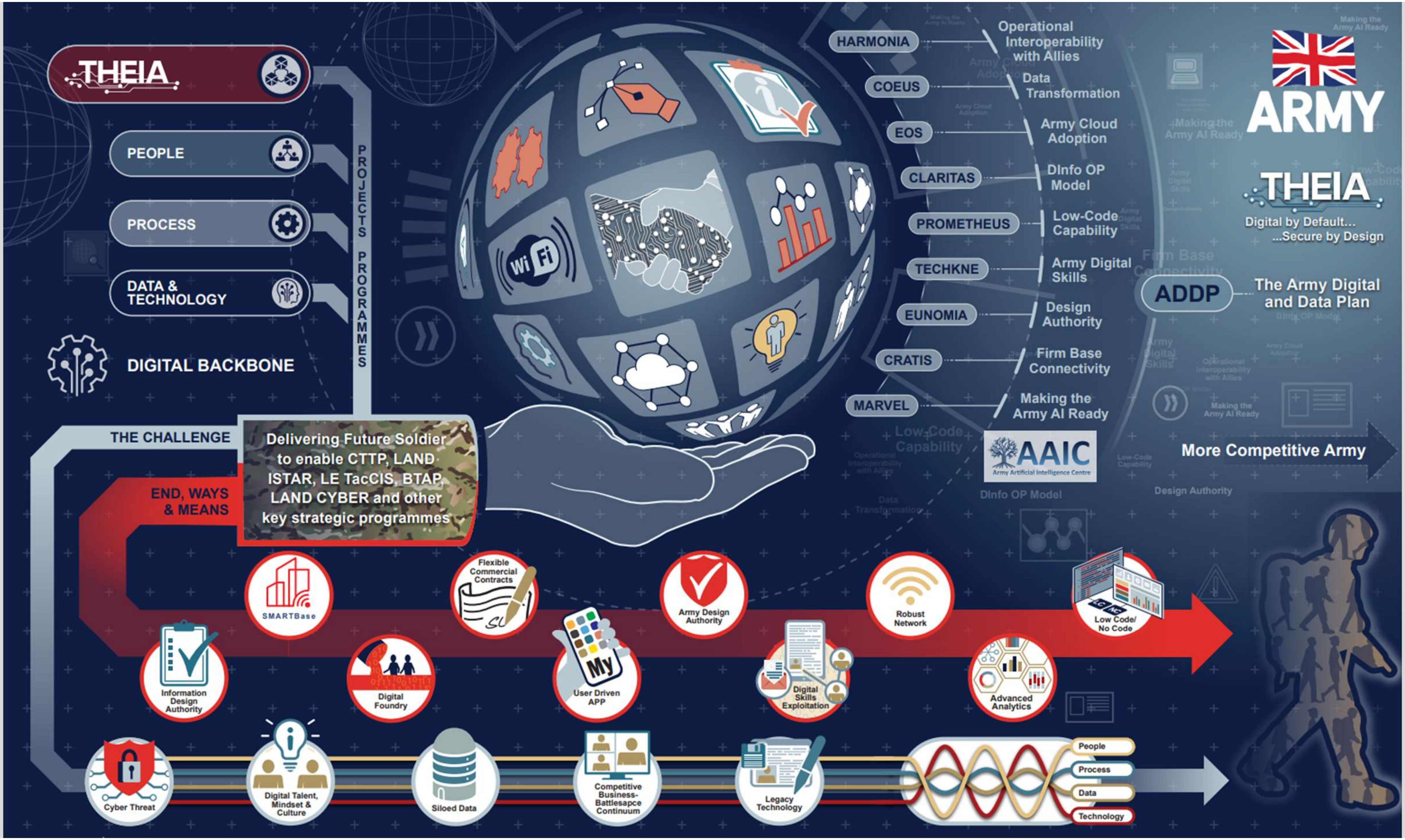
Embrace

- Embracing smart base concepts enables military installations to become more efficient, secure, and resilient.



SMARTBase

THEIA



THEIA

PEOPLE

PROCESS

DATA & TECHNOLOGY

DIGITAL BACKBONE

PROJECTS PROGRAMMES

THE CHALLENGE

Delivering Future Soldier to enable CTTP, LAND ISTAR, LE TacCIS, BTAP, LAND CYBER and other key strategic programmes

END, WAYS & MEANS

HARMONIA	Operational Interoperability with Allies
COEUS	Data Transformation
EOS	Army Cloud Adoption
CLARITAS	DInfo OP Model
PROMETHEUS	Low-Code Capability
TECHKNE	Army Digital Skills
EUNOMIA	Design Authority
CRATIS	Firm Base Connectivity
MARVEL	Making the Army AI Ready

AAIC
Army Artificial Intelligence Centre

ARMY

THEIA
Digital by Default...
...Secure by Design

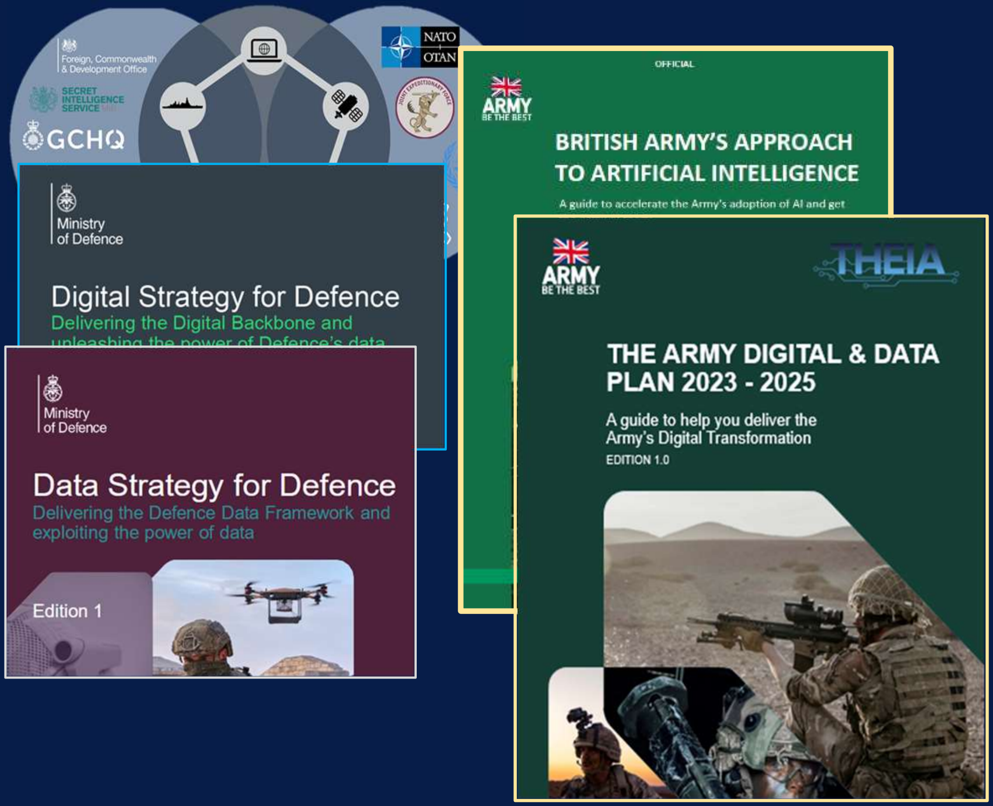
ADDP — The Army Digital and Data Plan

More Competitive Army

ADDP: The Context

ARMY

The plan aligns and supports the delivery of the Digital Strategy for Defence* primary outcomes. Again, these are key to ensure our plan's success.



Foreign, Commonwealth & Development Office
SECRET INTELLIGENCE SERVICE
GCHQ
NATO OTAN

Ministry of Defence

Digital Strategy for Defence

Delivering the Digital Backbone and unleashing the power of Defence's data

Ministry of Defence

Data Strategy for Defence

Delivering the Defence Data Framework and exploiting the power of data

Edition 1

OFFICIAL

ARMY BE THE BEST

BRITISH ARMY'S APPROACH TO ARTIFICIAL INTELLIGENCE

A guide to accelerate the Army's adoption of AI and get

ARMY BE THE BEST

THEIA

THE ARMY DIGITAL & DATA PLAN 2023 - 2025

A guide to help you deliver the Army's Digital Transformation

EDITION 1.0

Digital Backbone / Digital Ecosystem

A secure, singular, modern Digital Backbone connecting sensors, effectors and deciders across domains & with partners, driving integration & interoperability.

Digital Foundry & Army Digital Services (ADS)

A Digital Foundry unleashing the power of defence's data, exploiting Artificial Intelligence (AI) and other game changing technologies.

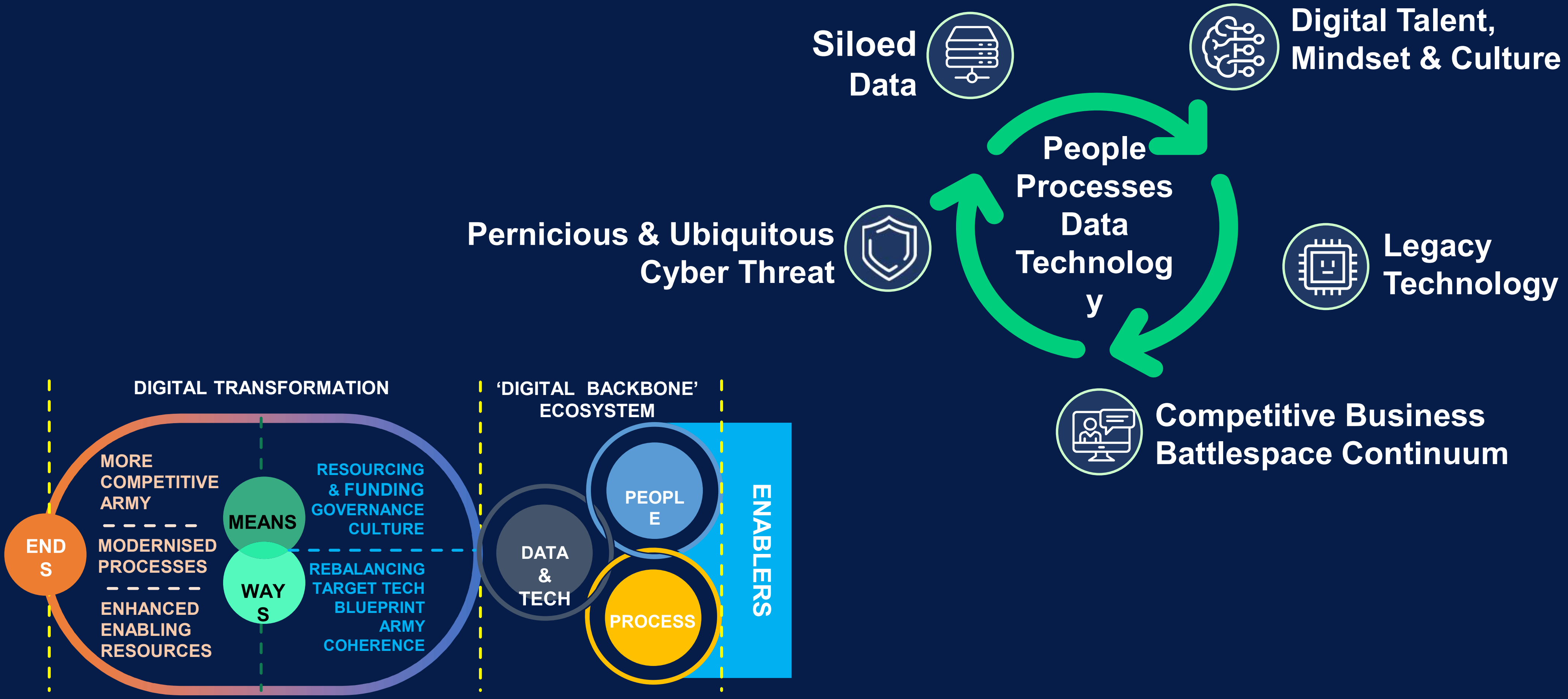
Digital Workforce

An empowered skilled & agile digital workforce.

OFFICIAL

THEIA

ADDP: The Challenge



Siloed Data

Digital Talent, Mindset & Culture

People
Processes
Data
Technolog
y

Pernicious & Ubiquitous Cyber Threat

Legacy Technology

Competitive Business Battlespace Continuum

DIGITAL TRANSFORMATION

END
S

MORE COMPETITIVE ARMY

MODERNISED PROCESSES

ENHANCED ENABLING RESOURCES

MEANS

WAY
S

RESOURCING & FUNDING
GOVERNANCE
CULTURE

REBALANCING
TARGET TECH BLUEPRINT
ARMY COHERENCE

'DIGITAL BACKBONE' ECOSYSTEM

DATA
&
TECH

PEOPL
E

PROCESS

ENABLERS

Surveillance – The Future

10:30-11:00

Coffee and Networking

Breakout Sessions

OLIVIER:

Physical Security - "Testing our Physical Security"

ST JAMES:

Personnel Security - "Security Issues that Eminate from our People"

CHIEF DISRUPTOR

ARMY

babcock™

GLOBAL EMC
ELECTROMAGNETIC SHIELDING & ANECHOICS

TANIUM

VARONIS

Capgemini

Cellebrite

EVERFOX

BT Means Business

CHIEF DISRUPTOR

ARMY

babcock™

GLOBAL EMC
ELECTROMAGNETIC SHIELDING & ANECHOICS

TANIUM

VARONIS

Capgemini

Cellebrite

EVERFOX

BT Means Business

Physical Security
"Testing our Physical Security"

Lieutenant Colonel Sam Roberts
CO 2 Military Intelligence Battalion

Major H
OC 21 Company, 2 Military Intelligence Battalion

Lee Rabjohn
Commercial Operations Director, Global EMC

Integrated Security

A physical, technical, personnel and procedural approach

Commanding Officer - Lt Col Sam Roberts

Officer Commanding 21 Company – Maj H

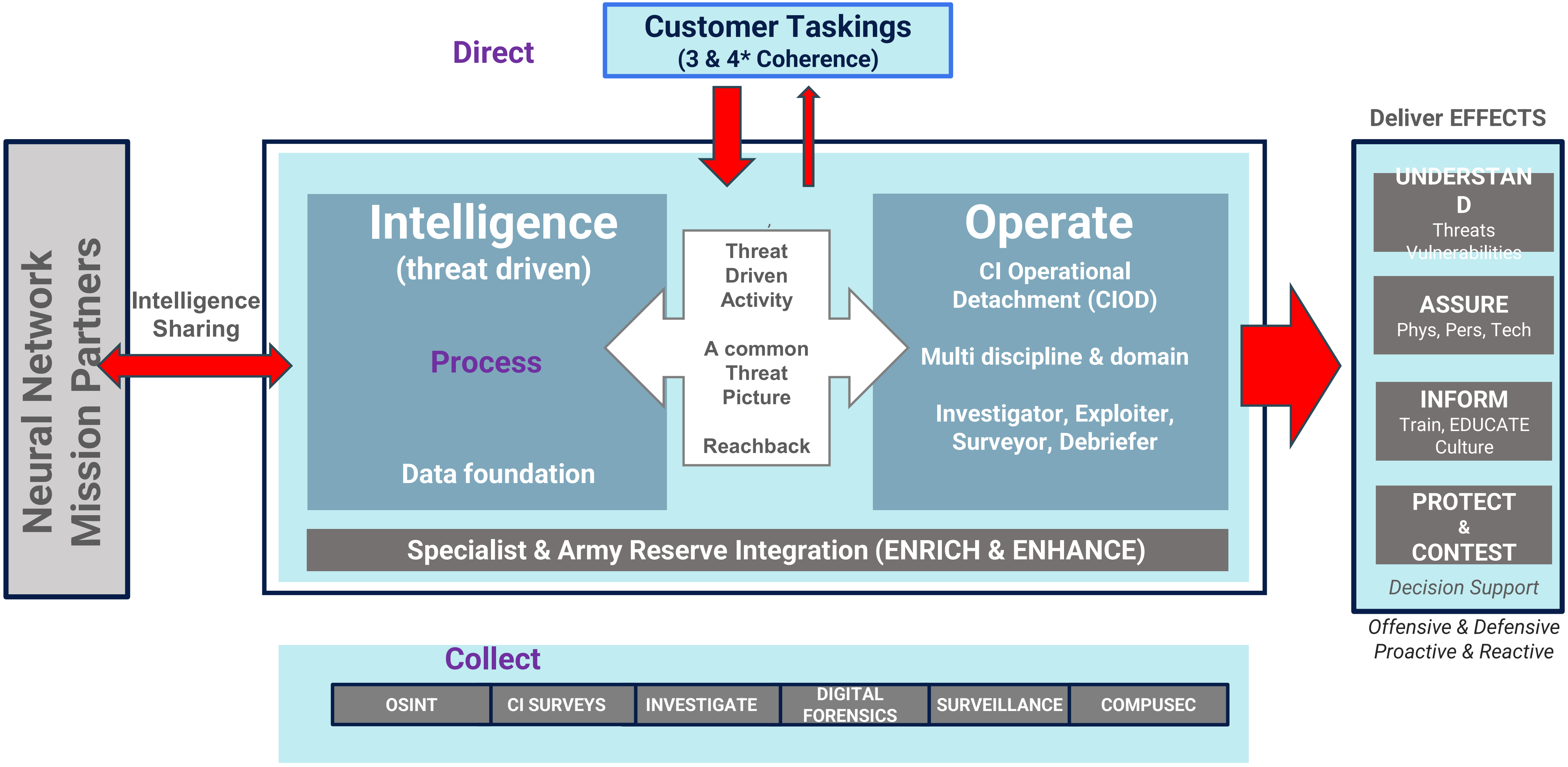
2MI Battalion Mission: **Counter threats** at **home & overseas** by delivering Exploitation & **Counter Intelligence** in support of **Army and wider Defence**

Context

- Counter Intelligence *and* Security
- Focus: PROTECT; Our people, our information, our equipment and our message
- Changing the narrative: ‘Operational Continuity – Secure to Operate’ – Next Generation
- Threat driven
- Multi domain – muti discipline
- Contest the adversary

An 'Int-Ops' integrated Operating Model

Mission: Counter threats at home & overseas by delivering Exploitation & Counter Intelligence in support of Army and wider Defence



Direct

Customer Taskings
(3 & 4* Coherence)

Neural Network
Mission Partners

Intelligence
Sharing

Intelligence
(threat driven)

Process

Data foundation

Threat
Driven
Activity

A common
Threat
Picture

Reachback

Operate

CI Operational
Detachment (CIOD)

Multi discipline & domain

Investigator, Exploiter,
Surveyor, Debriefer

Specialist & Army Reserve Integration (ENRICH & ENHANCE)

Deliver EFFECTS

UNDERSTAN
D
Threats
Vulnerabilities

ASSURE
Phys, Pers, Tech

INFORM
Train, EDUCATE
Culture

PROTECT
&
CONTEST

Decision Support

Offensive & Defensive
Proactive & Reactive

Collect

OSINT	CI SURVEYS	INVESTIGATE	DIGITAL FORENSICS	SURVEILLANCE	COMPUSEC

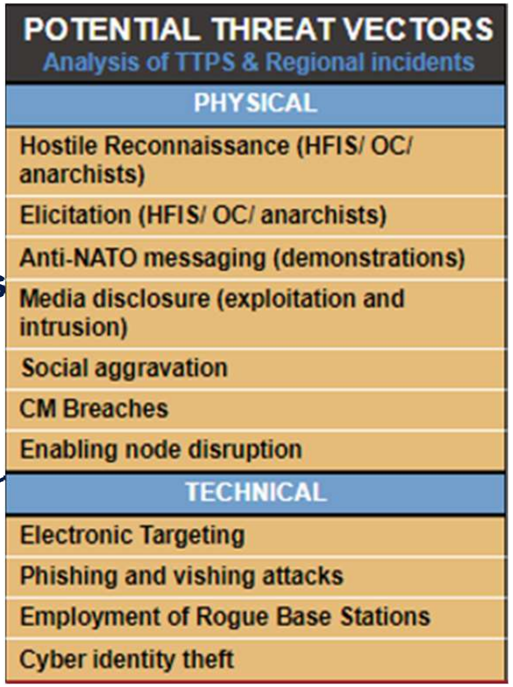
Vignettes – OC 21 MI Company

- Layering and a systems enterprise approach: no “1 size fits all”
- Threat/impact-led assurance by CIOD

- New <u>and</u> traditional workforce requirements
  - Skills to manage, monitor and (timely) react
  - 'computer says no’
  - Access control scope – perimeter vs critical ass

- Data storage and exploitation
  - Secure controlled storage
  - Real time analytics & retrospective investigatior
  - Multi-site / history aggregation

- Technical security resilience and compliance
  - Power supplies
  - Bearer wireless
  - Supply chain
  - Procedural access controls and separation from the IoT

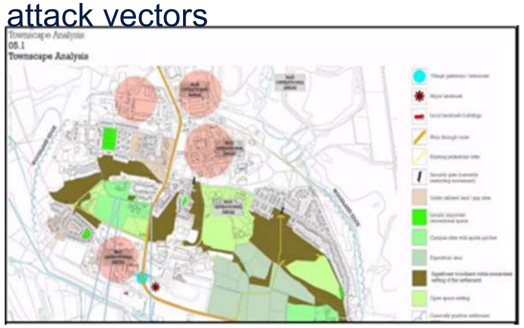


POTENTIAL THREAT VECTORS Analysis of TTPS & Regional incidents
PHYSICAL
Hostile Reconnaissance (HFIS/ OC/ anarchists)
Elicitation (HFIS/ OC/ anarchists)
Anti-NATO messaging (demonstrations)
Media disclosure (exploitation and intrusion)
Social aggravation
CM Breaches
Enabling node disruption
TECHNICAL
Electronic Targeting
Phishing and vishing attacks
Employment of Rogue Base Stations
Cyber identity theft

Example – activity/event-specific threat-led detailing of attack vectors and compromise to inform risk management and drive mitigation measures

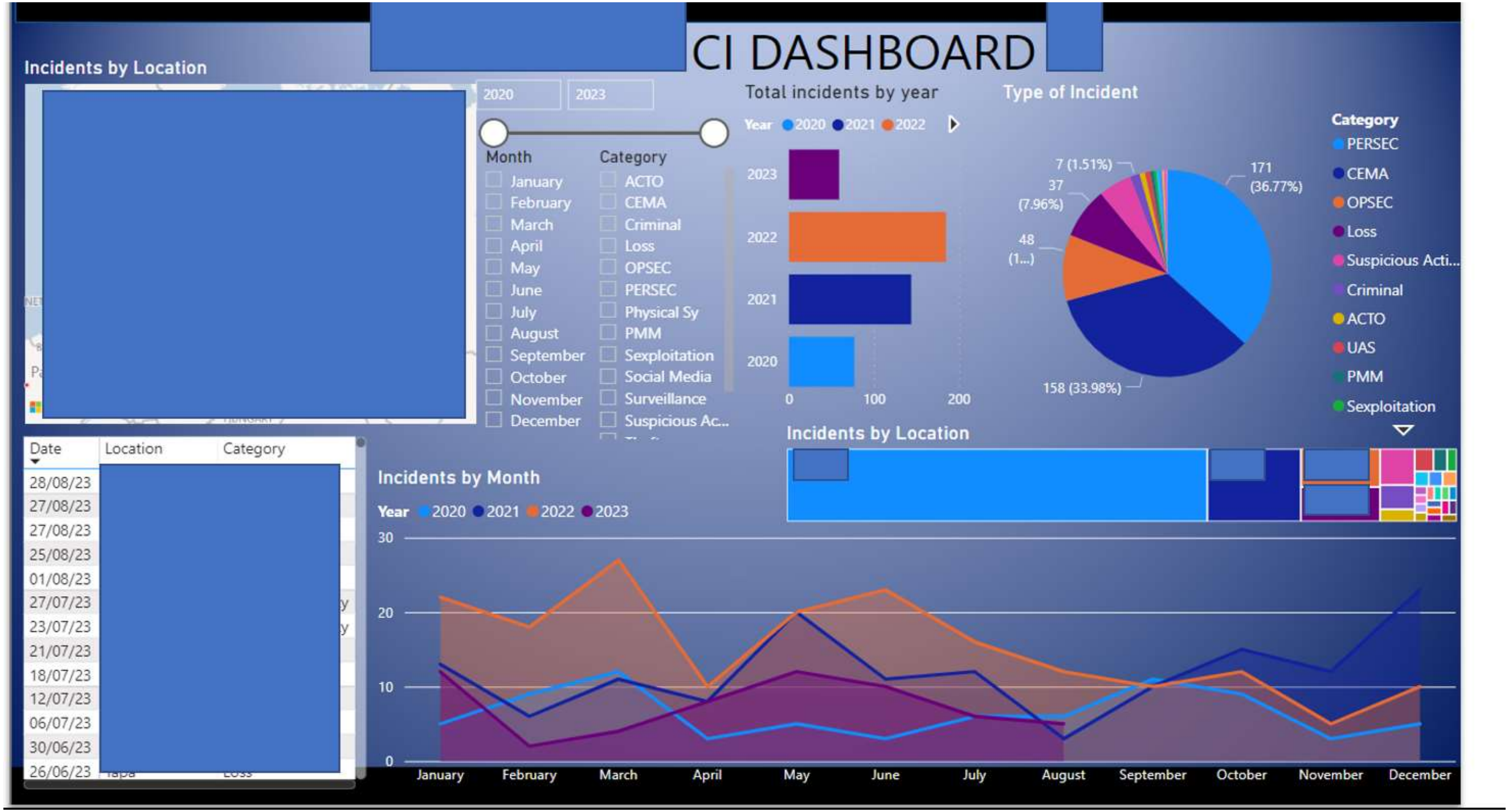
[redacted]

Social Media vulnerabilities: deliberate and unaware compromises = start-points for personnel and procedural attack vectors



Local Government planning data highlights key locations and infrastructure = start-points for disruption

Data Centric (how we are using data to become threat driven)



Date	Location	Category
28/08/23	[redacted]	[redacted]
27/08/23	[redacted]	[redacted]
27/08/23	[redacted]	[redacted]
25/08/23	[redacted]	[redacted]
01/08/23	[redacted]	[redacted]
27/07/23	[redacted]	[redacted]
23/07/23	[redacted]	[redacted]
21/07/23	[redacted]	[redacted]
18/07/23	[redacted]	[redacted]
12/07/23	[redacted]	[redacted]
06/07/23	[redacted]	[redacted]
30/06/23	[redacted]	[redacted]
26/06/23	[redacted]	[redacted]

Testing our Physical Security:

Understanding and Mitigating Radio Frequency Threats

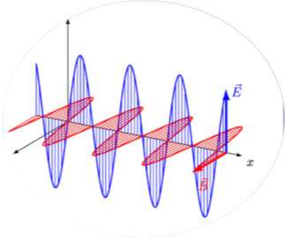
Lee Rabjohn – Commercial Operations Director

Global EMC Ltd

RF Shielding & EMC Specialists

RF Threats:

A Growing Concern



Physical Security Threat Perceptions

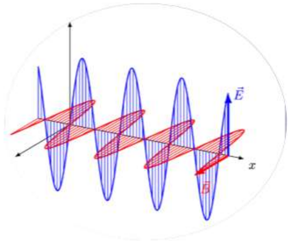
- Beyond bricks, mortar and secure doors.

Issue:

- Importance of understanding and addressing radio frequency threats.
  - Operational
  - Commercial

RF Threats:

A Growing Concern



The Threat:

- Unprotected electrical and electronic devices, such as Laptops, printers and PC screens emit unintentional RF emissions.
- These RF emissions can be captured, analysed and the data/information re-created, compromising the electromagnetic security (EMS) of sensitive data.
- RF Attacks are also a threat – examples;
  - MDMc
  - GPS
  - EMP

RF Threats:

Why the RF Threat Matters?

- **Disruption** of communications.
- **Compromised** security.
- Privacy **breaches**.
- Economic **impact**.
- Operational security.
    - Commercial / Non-Commercial threats, risks and structures.

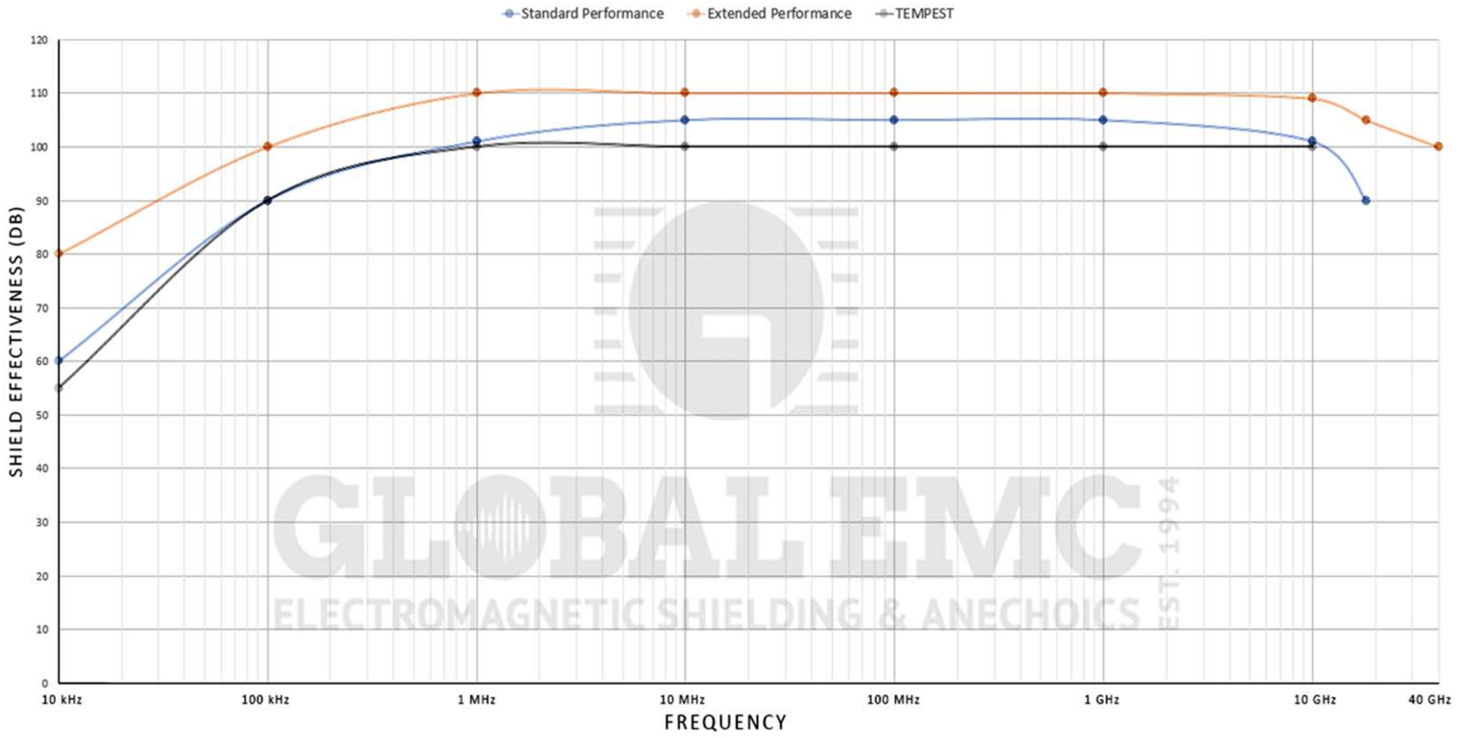
“Operational Continuity is key”

Therefore, the importance of regular security assessments is essential.

RF Threats:

Regulatory Framework

An **RF shielded room** is tested to **BS EN 50147-1** to determine its shielding effectiveness



The measure of **RF shielding performance** is known as “shielding effectiveness”.

100 dB in planewave and microwave frequencies is generally regarded as a **very high level of shielding**.

RF Threats:

Mitigating Strategies

- Encryption and secure communication protocols.
- Frequency hopping and diversity techniques.
- Monitoring and detection systems.
- Annual testing and calibration .

- Development of **RF secure facilities** – Global EMC’s core competencies
  - Secure Comms/Speech Rooms.
  - SCIF’s – Secure Compartmented Information Facility
  - Deployable Containers.
  - Deployable shielded equipment and materials – self build.
  - Forensic Evidence Boxes.
  - Forensic Rooms.

RF Threats:

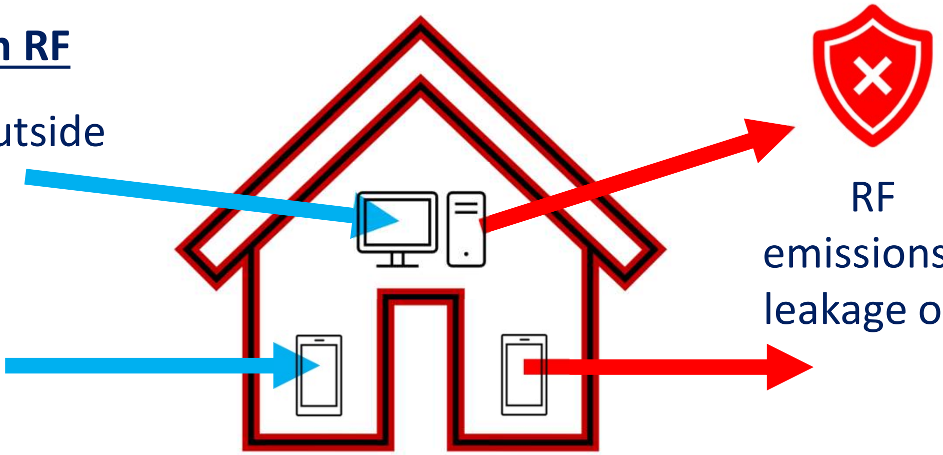
Mitigating Strategies

Summary

Unprotected from RF threats:

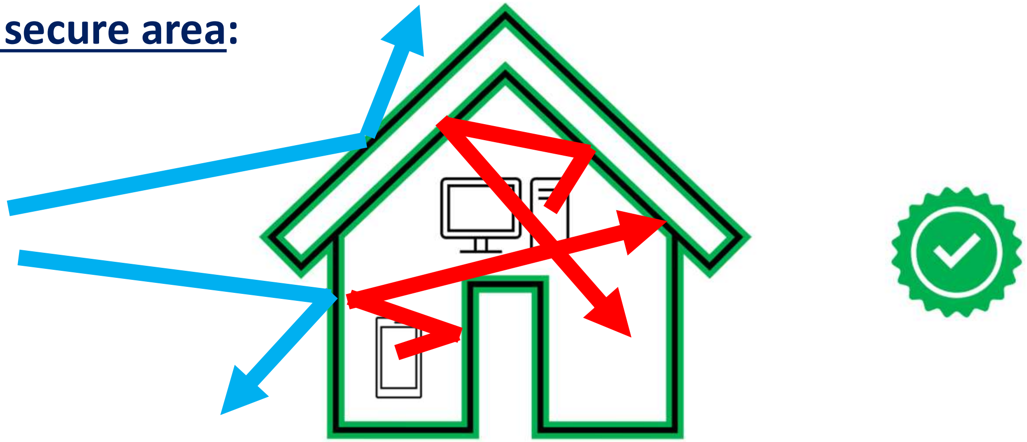
RF attacks from outside threats:

- MDMc
- GPS
- EMP



RF emissions – leakage out

RF Protected secure area:



GLOBAL EMC
ELECTROMAGNETIC SHIELDING & ANECHOICS

RF Threats:

Future Trends and Challenges

What lies ahead:

- Emerging technologies and their impact on RF Threats.
- The normalizing of the “Connected world”.
- Anticipated challenges in the evolving landscape.

Capability Development:

- Portable.
- Transportable.
- Deployable.
- Commerciality - Leasable.

Testing our Physical Security

- Awareness and Preparedness.
- Threat Mitigation - RF Testing.
  - RF threat analysis.
  - Signal testing at certain frequencies at an agreed range.
- Regulation.
- Trends & Challenges.
- Capability Development.

GLOBAL EMC
ELECTROMAGNETIC SHIELDING & ANECHOICS EST. 1994

MADE *in* BRITAIN

We always put the customers' requirements first in everything we do; working with each individual customer to develop a bespoke solution to meet their exact specification, on time and within budget.

Questions?

- What else can we add/do to increase the Multi-Domain/Discipline effect?
- Outsourcing/Subcontracting: Data, Intelligence, Operations. Risks and opportunity
- Security *versus* Counter Intelligence – can we separate the two?
- The challenge of resourcing and retaining the workforce – Cyber, physical, tech etc
- Risk balance: Intelligence gain vs operational risk
- Capability development – the approach?
- Data systems and the advance of tech – how can we stay ahead?

CHIEF DISRUPTOR

ARMY

babcock™

GLOBAL EMC
ELECTROMAGNETIC SHIELDING & ANECHOICS
EST. 1994

TANIUM.

VARONIS

Capgemini

Cellebrite

EVERFOX

BT Means Business

CHIEF DISRUPTOR

ARMY

babcock™

GLOBAL EMC
ELECTROMAGNETIC SHIELDING & ANECHOICS
EST. 1994

TANIUM.

VARONIS

Capgemini

Cellebrite

EVERFOX

BT Means Business

Personnel Security "Security Issues that Emanate from our People"

Colonel David Duncan

Principal Security Advisor (Army)

Matt Lock

Technical Director UK, Ireland and Middle East, Varonis

Ministry of Defence

Army Security Conference - Personnel security

"Security Issues that Emanate from our People"

ARMY

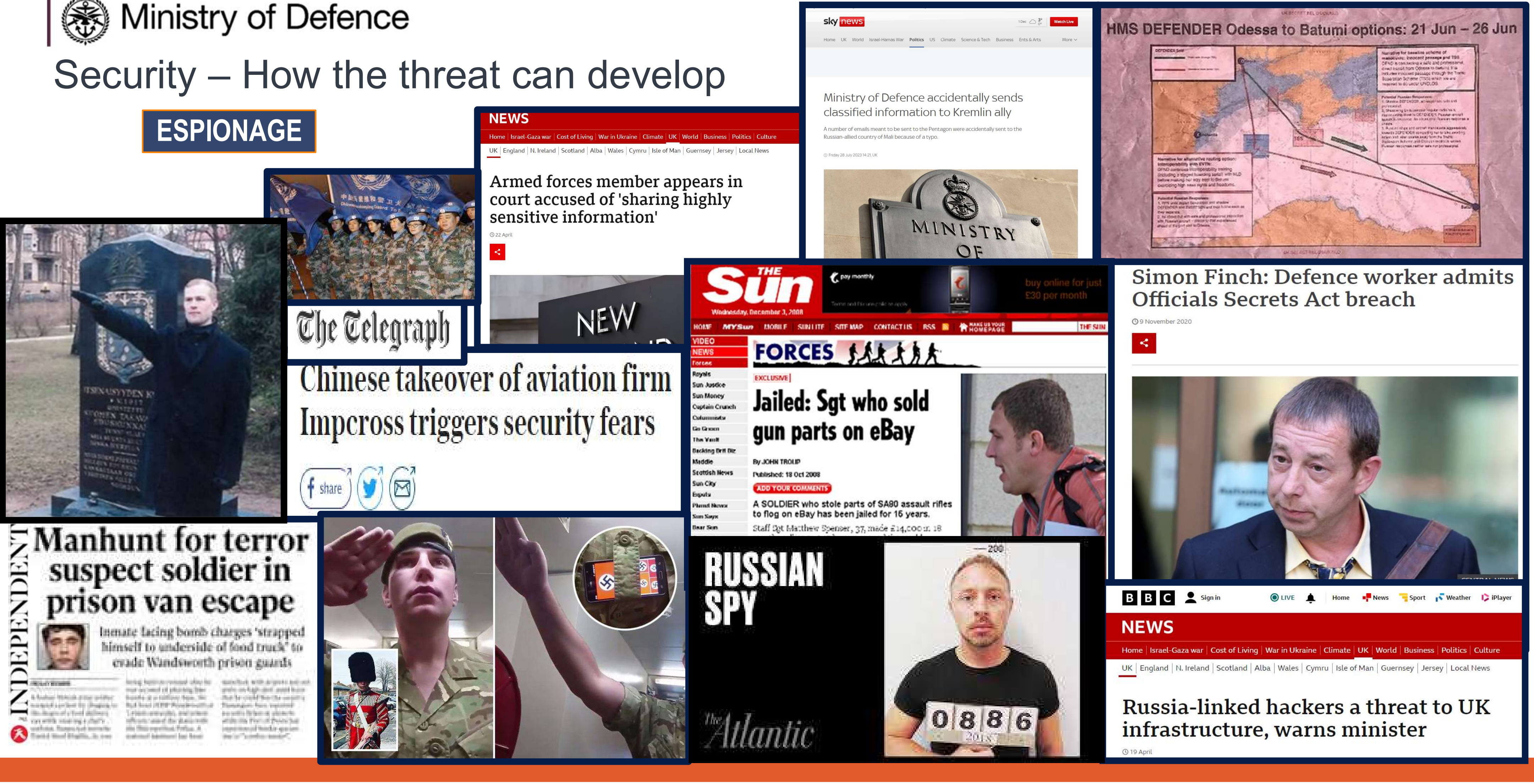
- Examples of the personnel security threats to our people – individuals at risk.
- Discuss some of the threats posed by our people – individuals posing a risk.
- How to address the threat?

Ministry of Defence

Security – How the threat can develop

ESPIONAGE

THE INSIDER – BOTH CONSCIOUS AND UNWITTING



NEWS

Home | Israel-Gaza war | Cost of Living | War in Ukraine | Climate | UK | World | Business | Politics | Culture

UK | England | N. Ireland | Scotland | Alba | Wales | Cymru | Isle of Man | Guernsey | Jersey | Local News

Armed forces member appears in court accused of 'sharing highly sensitive information'

22 April

sky news

Home UK World Israel-Hamas War Politics US Climate Science & Tech Business Ents & Arts More

Ministry of Defence accidentally sends classified information to Kremlin ally

A number of emails meant to be sent to the Pentagon were accidentally sent to the Russian-allied country of Mali because of a typo.

Friday 28 July 2023 14:21, UK

The Telegraph

Chinese takeover of aviation firm Impcross triggers security fears

share

THE Sun

Wednesday, December 3, 2008

HOME MY Sun MOBILE SUN LITE SITE MAP CONTACT US RSS MAKE US YOUR HOMEPAGE THE SUN

VIDEO
NEWS
Forces
Royals
Sun Justice
Sun Money
Captain Crunch
Columnists
Go Green
The Vault
Backing Brit Biz
Maddie
Scottish News
Sun City
Espaňa
Planet News
Sun Says
Dear Sun

FORCES

EXCLUSIVE

Jailed: Sgt who sold gun parts on eBay

By JOHN TROUP

Published: 18 Oct 2008

ADD YOUR COMMENTS

A SOLDIER who stole parts of SA80 assault rifles to flog on eBay has been jailed for 16 years.

Staff Sgt Matthew Spencer, 37, made £14,000 in 18

Simon Finch: Defence worker admits Officials Secrets Act breach

9 November 2020

INDEPENDENT

Manhunt for terror suspect soldier in prison van escape

Inmate facing bomb charges 'strapped himself to underside of food truck' to evade Wandsworth prison guards

RUSSIAN SPY

The Atlantic

BBC Sign in LIVE Home News Sport Weather iPlayer

NEWS

Home | Israel-Gaza war | Cost of Living | War in Ukraine | Climate | UK | World | Business | Politics | Culture

UK | England | N. Ireland | Scotland | Alba | Wales | Cymru | Isle of Man | Guernsey | Jersey | Local News

Russia-linked hackers a threat to UK infrastructure, warns minister

19 April

Ministry of Defence

Threat – Context

Today, the UK acts as Ukraine’s ally, providing it with military aid in the form of equipment and specialists, i.e. de facto is leading an undeclared war against Russia.

That being the case, any of its public officials (either military, or civil, who facilitate the war) can be considered as a legitimate military target.

- Dmitry Medvedev, Deputy Chairman of the Security Council of Russia, 30 May 23

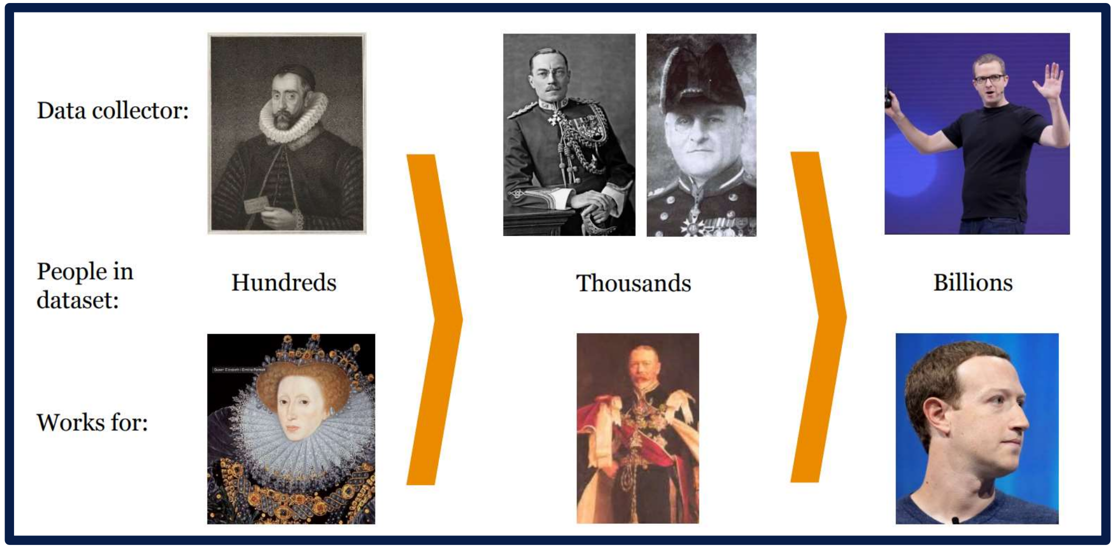
ARMY

Ministry of Defence

Threat – Context

- **Information is the lifeblood of Defence, data is the Army’s second most important asset after its people.**

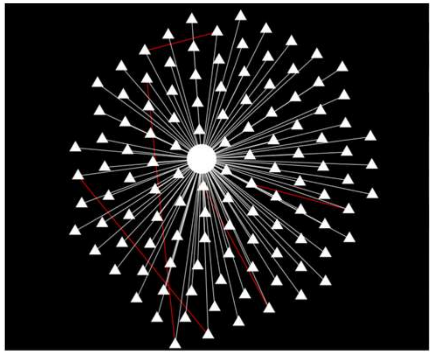
- **One of the greatest challenges is understanding that we are at risk.**



Data collector:

People in dataset: Hundreds › Thousands › Billions

Works for:



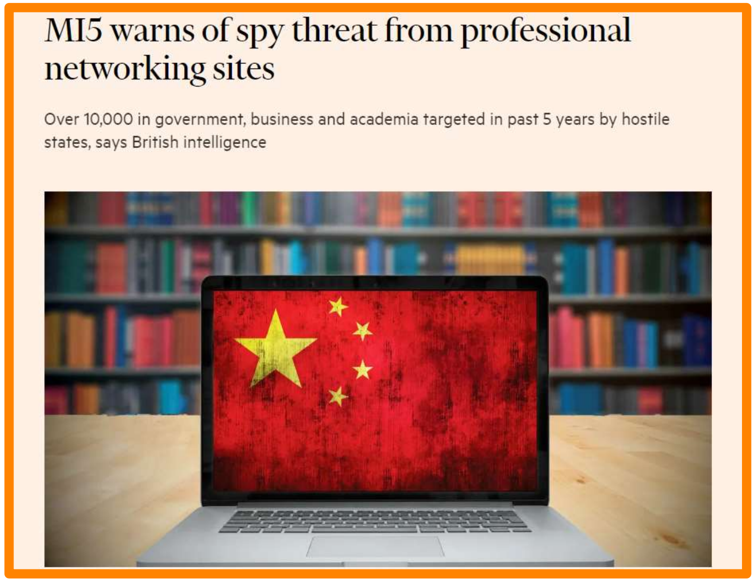
Front page and one article in The Guardian: potentially over 200 third-party sites contacted

ARMY

Ministry of Defence

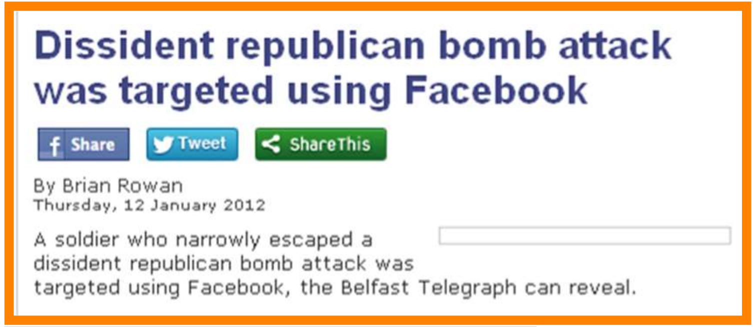
Security – Individuals at risk

- Open access to personal, operational and wider Army information from our personnel.
- Individuals and groups at risk.
- Wider extended community.



MI5 warns of spy threat from professional networking sites

Over 10,000 in government, business and academia targeted in past 5 years by hostile states, says British intelligence



Dissident republican bomb attack was targeted using Facebook

By Brian Rowan
Thursday, 12 January 2012

A soldier who narrowly escaped a dissident republican bomb attack was targeted using Facebook, the Belfast Telegraph can reveal.

Sunday Life

Life SPECIAL REPORT

HONEYTRAP

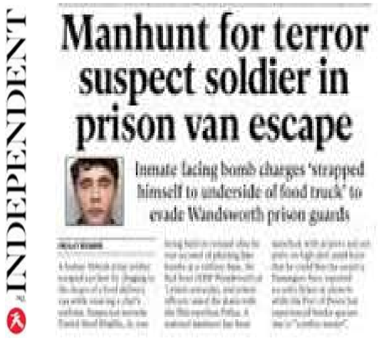
HOW NI SOLDIERS AND COPS ARE PUTTING THEIR LIVES IN DANGER ON LONELY HEARTS INTERNET SITE

Ministry of Defence

Security – Individuals posing at risk

How to address the threat?
Better understand our staff:

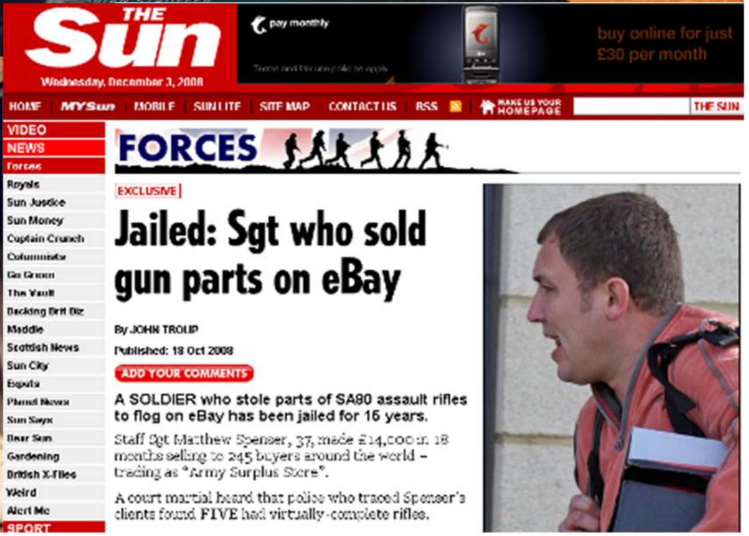
- Behaviours
- Motivation
- Associations


INDEPENDENT

Manhunt for terror suspect soldier in prison van escape

Inmate facing bomb charges 'strapped himself to underside of food truck' to evade Wandsworth prison guards

SECURITY QUIZ
How well do you know the insider threat?
Measure your knowledge of data breaches, stolen secrets and network sabotage.
BRIAN STAUFFER



Jailed: Sgt who sold gun parts on eBay

By JOHN TROUP

Published: 18 Oct 2008

A SOLDIER who stole parts of SA80 assault rifles to flog on eBay has been jailed for 16 years.

Staff Sgt Matthew Spenser, 37, made £14,000 in 18 months selling to 245 buyers around the world – trading as "Army Surplus Store".

A court martial heard that police who traced Spenser's clients found FIVE had virtually-complete rifles.

Questions

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

Doctor Simon Wiseman
Chief Technology Officer, Everfox

Bogdan Grigorescu
Senior Technical Lead – Architecture & Quality Engineering, eBay

12:40-13:45

Lunch and Networking

Plenary session:
Army Security Culture and Incidents

Sarah Hannam

SEO Warning, Advice, Reporting Point (WARP)

Jessica Benton

HEO Security Culture, British Army

Vic Djondo and Ashley Lloyd

Security Culture & Education, BT Group

Ministry of Defence

Army Security Culture and Incidents

What’s a WARP?

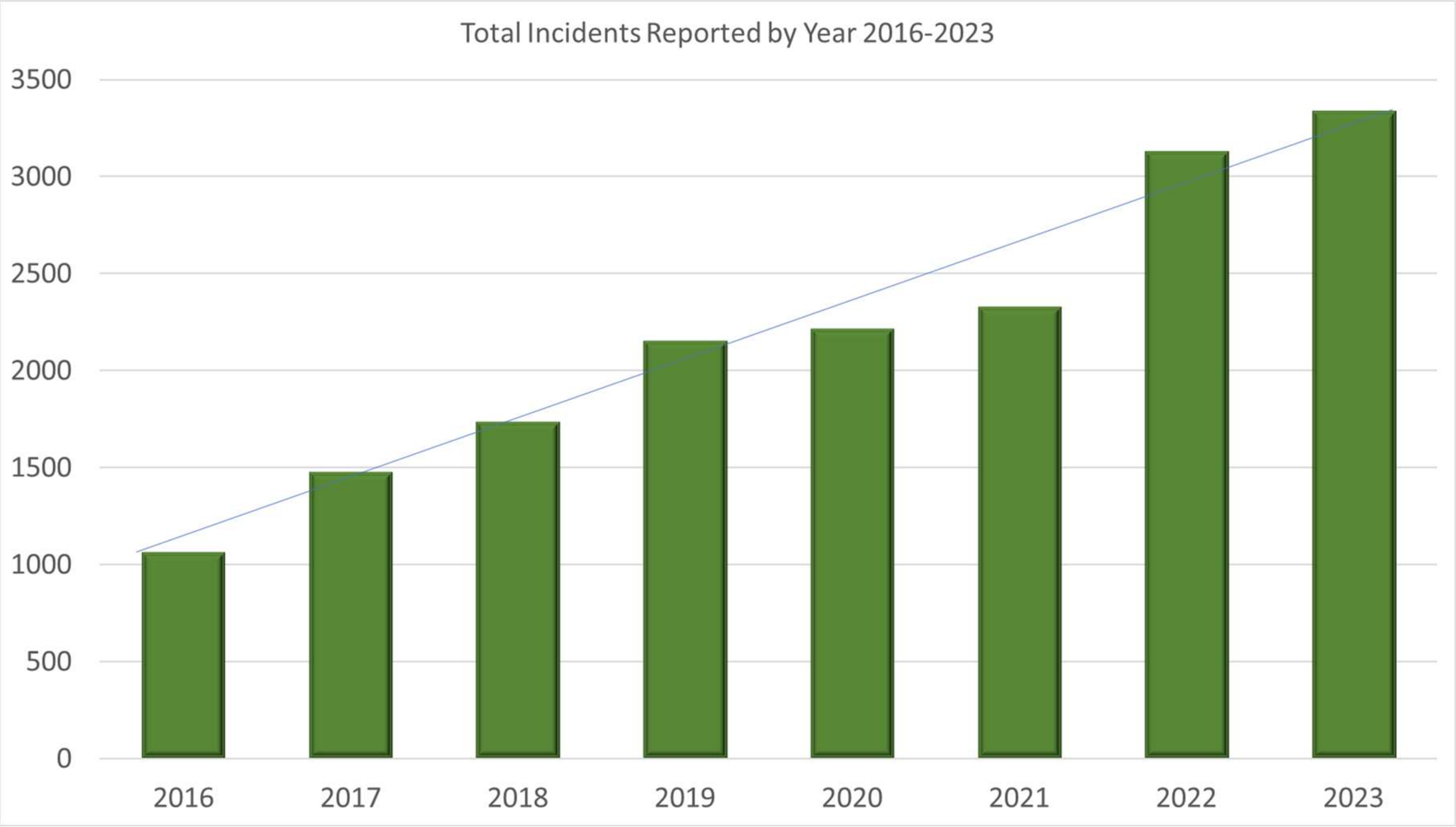
Warning
Advice
Reporting

ARMY

Ministry of Defence

Army Security Culture and Incidents

Reporting Figures

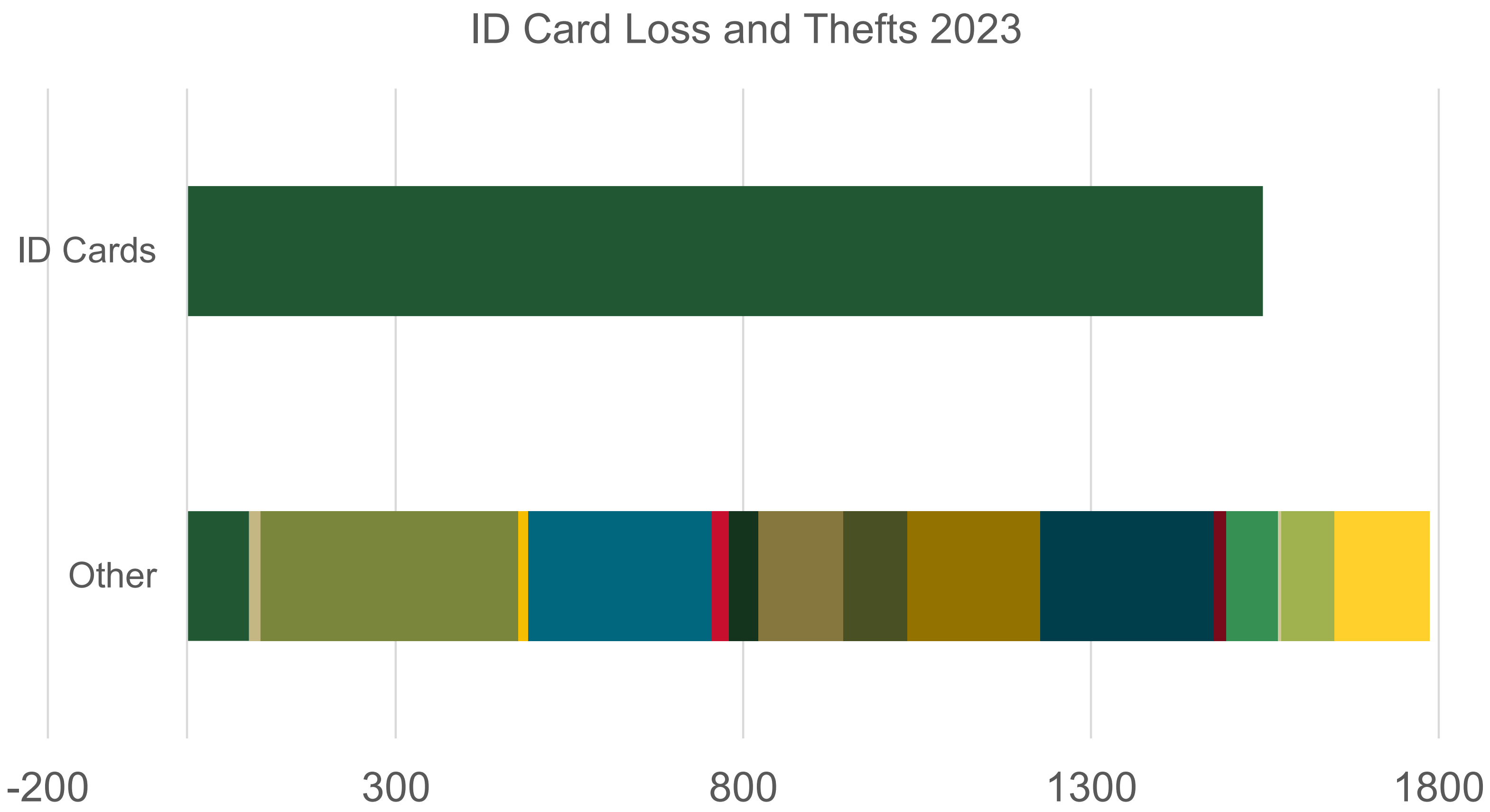


ARMY

Ministry of Defence

Army Security Culture and Incidents

2023 Security Incidents

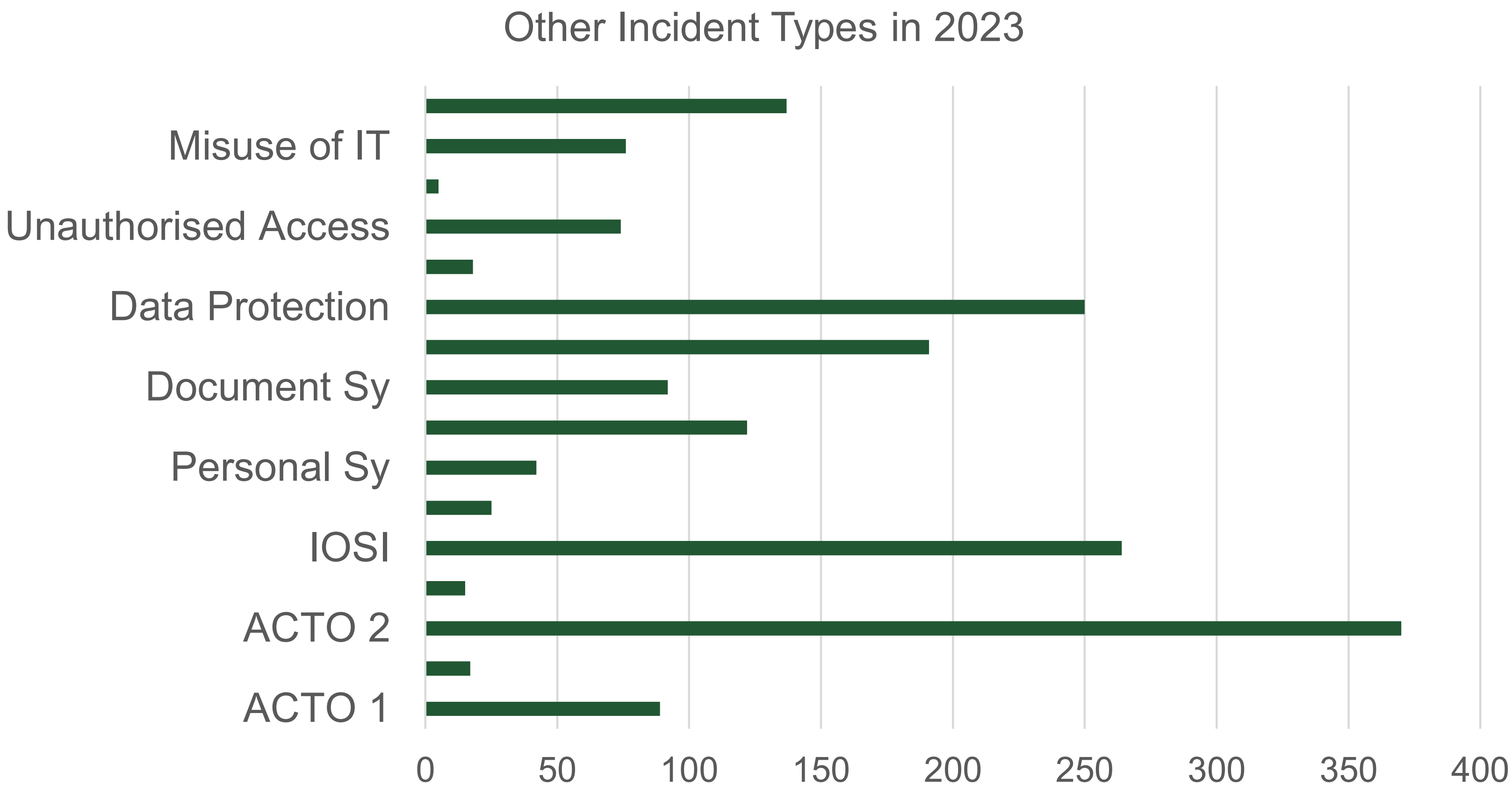


ARMY

Ministry of Defence

Army Security Culture and Incidents

2023 Security Incidents

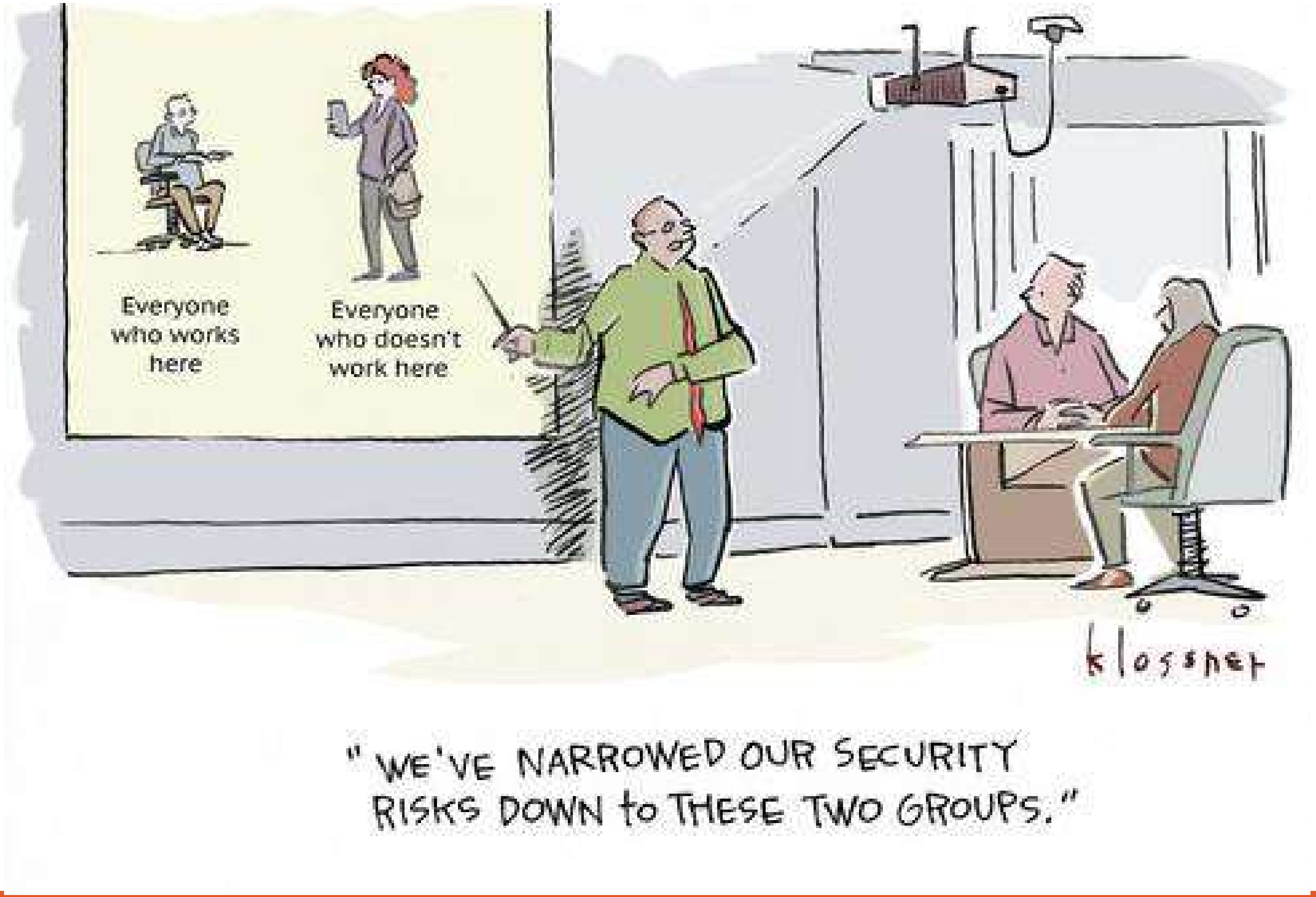


ARMY

Ministry of Defence

Army Security Culture and Incidents

Causes



"WE'VE NARROWED OUR SECURITY RISKS DOWN to THESE TWO GROUPS."

ARMY

Ministry of Defence

Army Security Culture and Incidents

Issues

ARMY

Army Security Culture

- What is Security Culture?
  - Security culture refers to the collective values, attitudes, and behaviours regarding security within an organisation.
- Why is it important?
  - Security culture is the foundation of effective security measures.
  - It influences employee awareness, vigilance, and adherence to security protocols.
  - A strong security culture reduces the likelihood of security breaches and enhances overall resilience.

Ministry of Defence

Army Security Culture

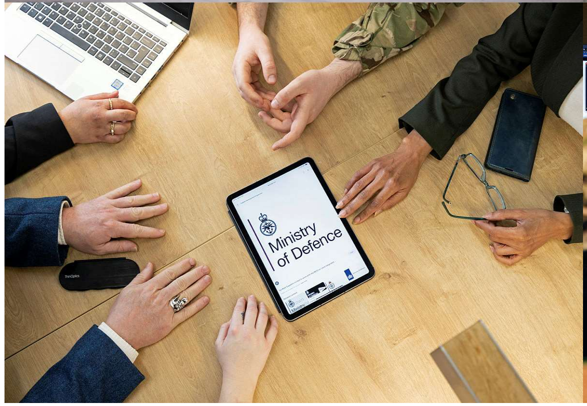
Large and Diverse Workforce

- Officers
- Soldiers
- Trainees
- Cadets
- Civil Servants
- Contractors
- English as a second language
- Office-based vs. non office-based
- Socio-economic background

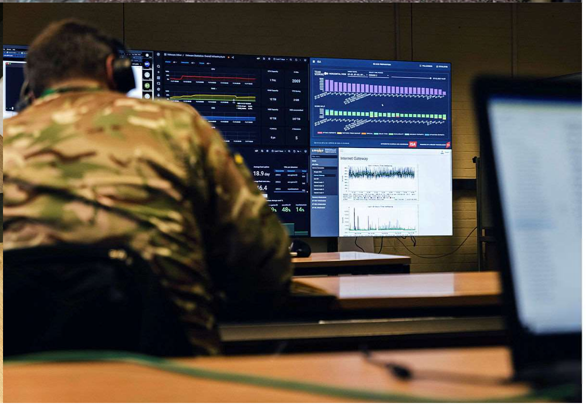
Not “One-Size Fits All”

UK MOD © Crown copyright 2023

UK MOD © Crown copyright 2021



UK MOD © Crown copyright 2023



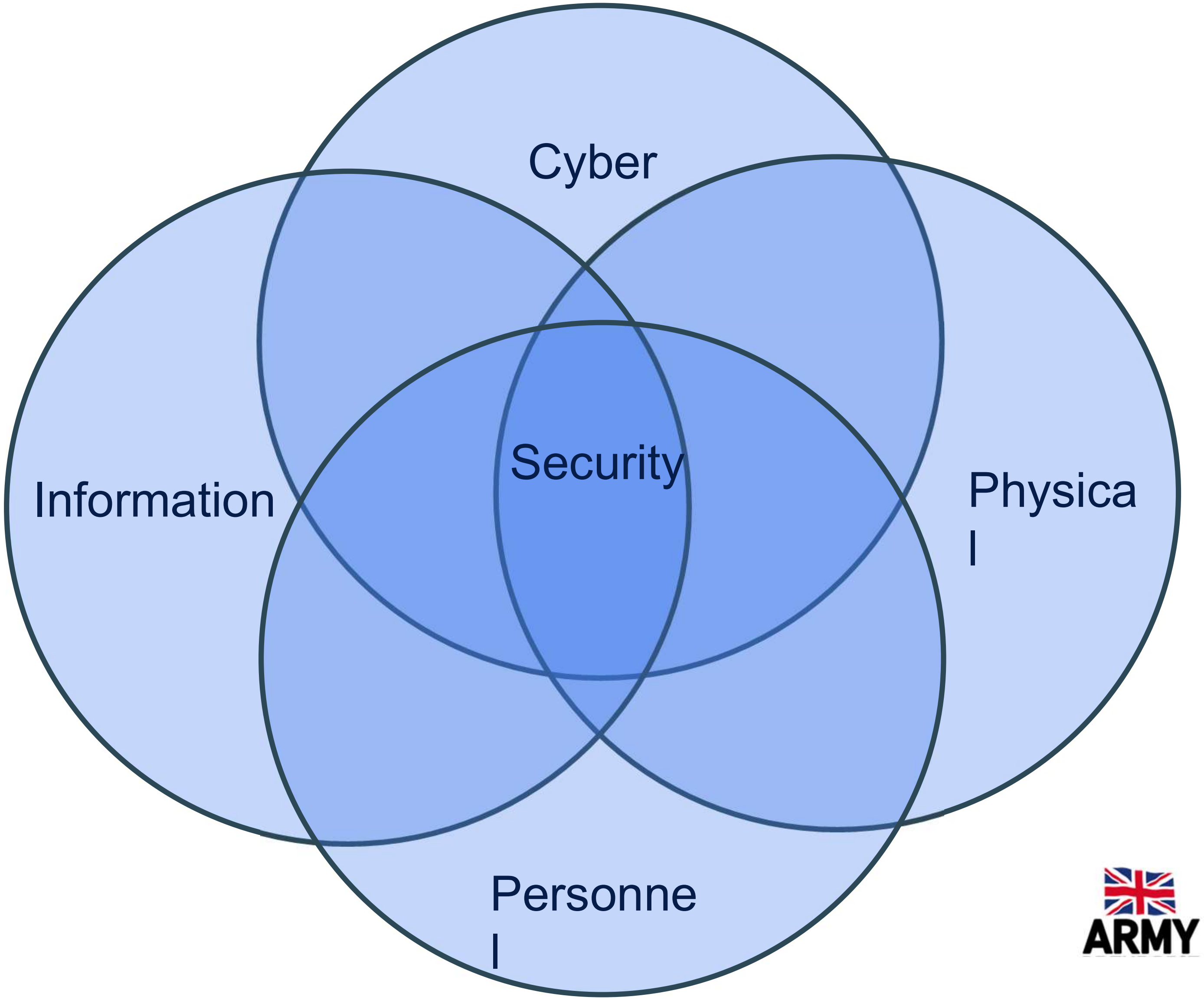
UK MOD © Crown copyright 2021

ARMY

Ministry of Defence

Army Security Culture

Next-Generation approach:



ARMY

Security Culture and Incidents

Industry perspective on security risk and building a culture of security

Vic Djondo & Ashley Lloyd, BT Group

BT Group

What is Security Culture?

Awareness vs. Behaviour vs. Culture…

Security Awareness

Security awareness is a poor way to measure risk.

Security Behaviour

Measuring security behaviour is a great measure of risk for known behaviours.

Security Culture

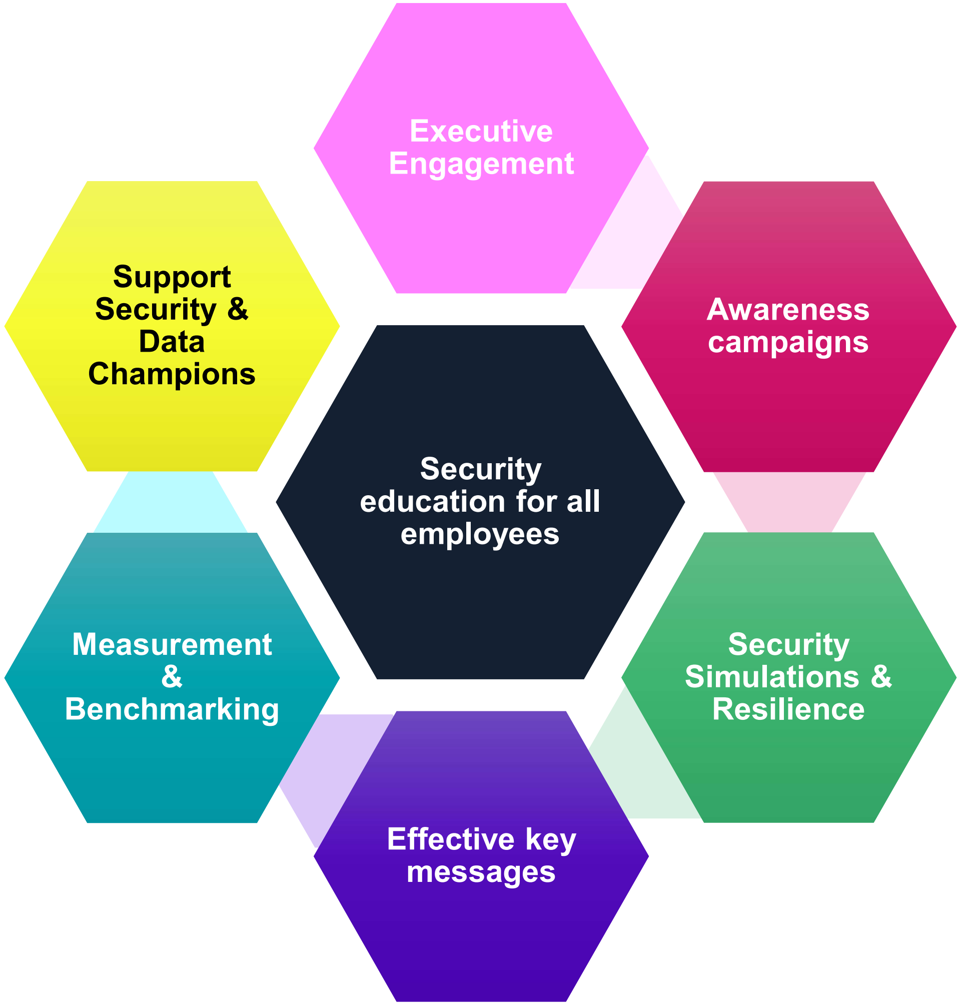
Measuring security culture is a great predictor of risk for unmeasured behaviours.

Ensure security is part of BT DNA

“A positive and professional culture of security that supports openness and fosters a motivated, engaged and productive workforce to protect BT and its customers.”

Security Culture & Education

The BT Group approach



Executive Engagement

Support Security & Data Champions

Awareness campaigns

Security education for all employees

Measurement & Benchmarking

Security Simulations & Resilience

Effective key messages

Breakout Sessions

ST JAMES:

Cyber Security -

"Approaches to Defensive Cyber"

OLIVIER:

Resilience and Business Continuity -

"What are we protecting and why?"

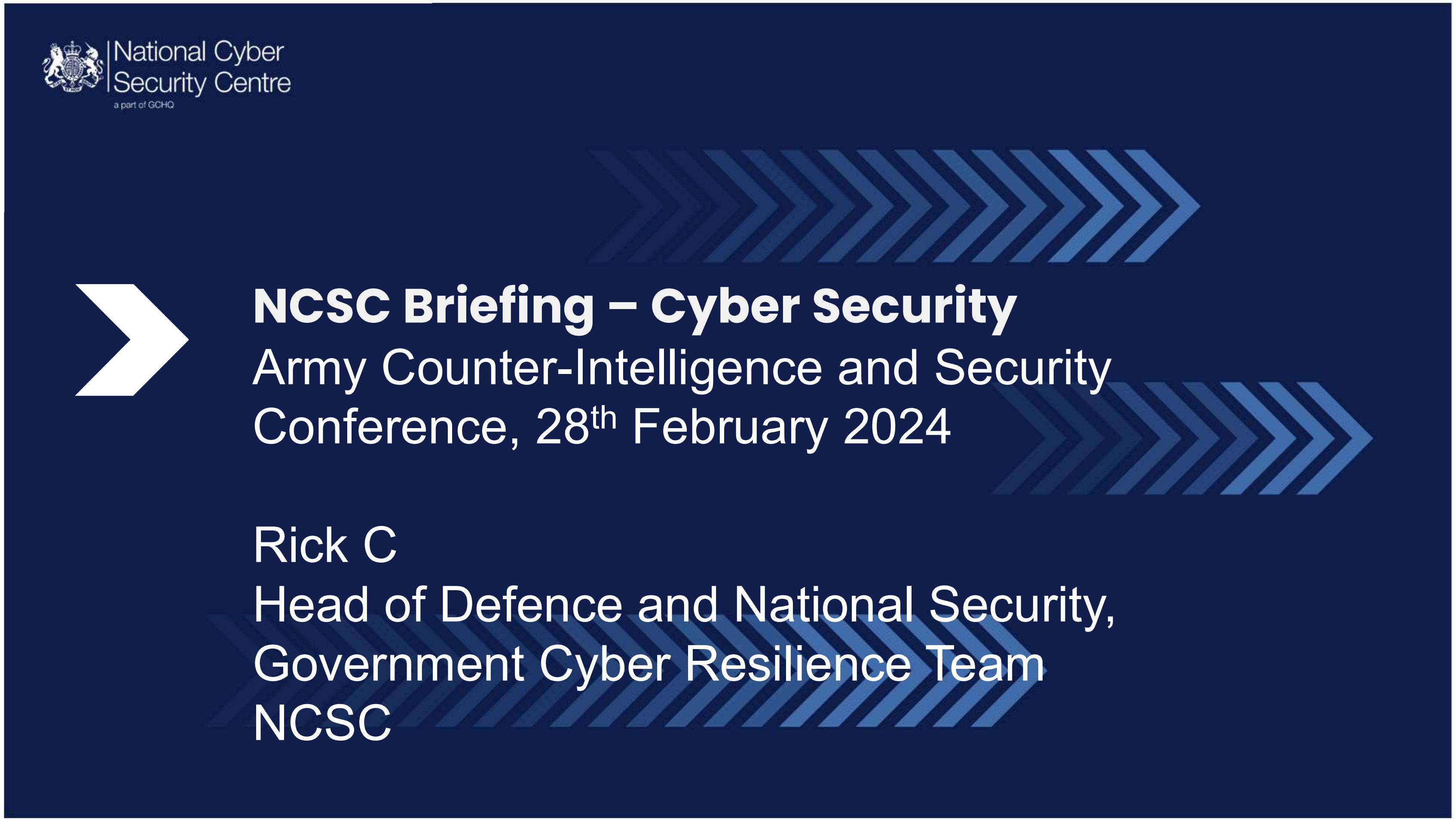
Cyber Security
"Approaches to Defensive Cyber"

Rick C
Head of Government and National Security, Government and Cyber Resilience Team National Cyber Security Centre (NCSC)

Kristina Evans
Head of Cyber and Security, British Army

Major Peter Malan CISSP
HEO Defensive Cyber and Electromagnetic Activities

Doug Davidson
Senior Director & Cybersecurity Lead for Aerospace & Defence, Capgemini



National Cyber Security Centre
a part of GCHQ

NCSC Briefing – Cyber Security

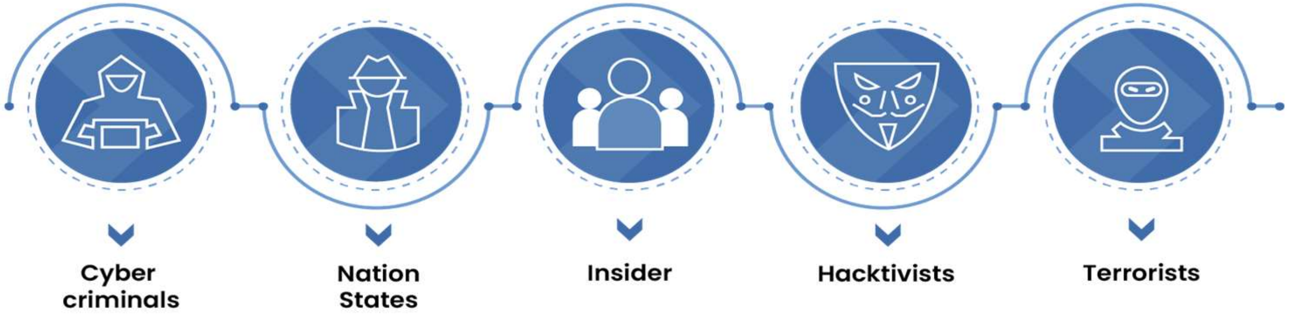
Army Counter-Intelligence and Security Conference, 28th February 2024

Rick C
Head of Defence and National Security,
Government Cyber Resilience Team
NCSC

The Cyber Threat – derived from NCSC's Decoding 2023 Report

From hostile state actors to organised criminal groups, cyber space offers a place to enact, enable or conceal malicious action to inflict harm to our society, economy and national security. This includes reducing Strategic Advantage and restricting Operational Independence.

Cyber-crime ransomware remains one of the most serious cyber threats to the UK, but for UK Defence Sector which includes the MOD, the Armed Services (including of course the British Army) and the Defence Industrial Base (DIB) we are particularly concerned about Nation State threat to sensitive information of both a strategic and tactical nature. **We are also not just concerned about Confidentiality, but also Integrity and availability of information; we are also concerned about interdiction in the supply chain.**



Nation State 'Threat from FIS'

The Nation States we are most concerned about from a cyber perspective include **Russia**, **China**, **DRRK** and **Iran**. It is clear the UK defence sector is a priority target for state sponsored cyber actors. Foreign intelligence Services (FIS) will highly likely target the UK defence sector for military intelligence and to steal UK intellectual property to enhance their own capabilities. They will also wish to access and/or deny us communication in the Battlespace.

And these are not the only Nation States with an interest.

Intent is key: our adversaries want to deny us strategic advantage by whatever means: espionage, IPR theft, denial of communications, supply chain interdiction. We need to make sure that Strategic Advantage is maintained.

Unlike 5 Eyes these FIS operate without legal constraint or proportionality; for them, the ends justify the means.

Nation States: ‘The Usual Suspects’

China has continued to demonstrate itself to be a highly sophisticated and capable cyber actor. The Chinese intelligence services, along with a growing number of freelancers and contractors, have continued to conduct cyber espionage and data collection on a global scale. China is a systemic competitor to the UK, with a whole-of-state approach to enhancing its cyber capabilities. As the Chinese state’s worldview continues to conflict with that of the West, it is almost certain the UK will be subjected to increased cyber targeting by actors associated with the Chinese state.

Russia remains a highly capable and motivated threat actor. Russian cyber espionage operations continue to pose a threat to the UK – particularly to the government and defence sectors, and the parts of civil society that work closely with them. Public exposure of Russian cyber activity this year continued to harden the operating environment, but Russian state cyber actors will almost certainly continue to evolve.

Iran continues to grow its cyber espionage expertise while supplementing its traditional cyber playbook with cyber-enabled information operations. Though Iran’s cyber activity has likely been focused on the Israel/Hamas conflict since October, it remains willing to target the West in cyber espionage operations to fulfil its strategic requirements.

The **DPRK** continues to use cyber operations to further state priorities through revenue generation and gathering information. They continue to target cryptocurrency exchanges and will almost certainly continue to do so into 2024. UK organisations and individuals remain at risk from these campaigns.

China Threat

China's cyber capabilities have evolved over the past decade into a sophisticated and persistent threat. This evolution will almost certainly continue, and China will remain a top-tier cyber threat over at least the next five years.

China is a systemic competitor to the UK and presents an "epoch-defining challenge" through its whole of state approach to enhancing its cyber capabilities. As the Chinese state's world view continues to conflict with that of HMG and our like-minded allies, it is almost certain we will be subjected to increased cyber targeting by actors associated with the Chinese state..

Throughout 2023, China has continued to demonstrate itself to be a highly sophisticated and capable cyber actor. The Chinese intelligence services, along with a growing number of freelancers and contractors, have continued to conduct cyber espionage and data collection on a global scale. Sectors targeted include government, **defence** and telecommunications. This included the reported compromise of Microsoft accounts by a China-based actor, tracked as Storm0558, which reportedly affected approximately 25 organisations, including government agencies.

Chinese state cyber activity is not limited to espionage and intelligence collection. Reporting in 2023 highlighted Chinese state-linked targeting and successful compromising of US CNI, both on the mainland and the territory of Guam, since at least 2021. **Microsoft assessed the group responsible, which it tracks as Volt Typhoon, is developing capabilities that could disrupt critical communications infrastructure between the US and Asia in future crises.**

China is particularly interested in AUKUS the trinational agreement which will give Australia access to nuclear powered submarines, the joint UK-Japan-Italy Global Combat Air Programme, and Op HIGHMAST the Carrier Strike Group visit to the South China Sea in 2025.

Russia Threat

Russia remains a highly capable and motivated threat actor. While the emphasis on Ukraine remained this year, Russian state cyber actors maintained their global cyber espionage activity. For example, Microsoft reported that SVR intrusion set APT29 used Microsoft Teams lures in a social engineering campaign. The group reportedly targeted around 40 organisations globally, in sectors including government, Non-Governmental Organisations (NGOs), technology and media. Russian cyber espionage operations continue to pose a threat to the UK, **in particular to the government and defence sectors,** and the parts of civil society that work closely with them.

But public exposure of Russian cyber activity also continued in 2023, with the release of several public advisories and attributions. Cyber security industry blogs published this year also revealed Russian state cyber actors using novel techniques in their operations in Ukraine. While this kind of exposure helps to counter the threat, these examples also illustrate the range of capabilities at Russia's disposal, from phishing campaigns to bespoke tools and techniques. Russian state cyber actors will almost certainly be able to adapt and evolve their operations in response to public exposure.

Anything relating to UK Military involvement in Eastern Europe will illicit high interest and activity in Cyber Space

- March 23: Vulkan files leak
- May 23: Snake malware advisory
- November 2023: Mandiant Sandworm/Energy Report
- December 23: Star Blizzard Attribution
- February 24: Living of the Land Advisory
- February 24: Midnight Blizzard Advisory (Cloud Access)

Cybercrime – Ransomware attacks

Cybercrime continues to impact organisations in the UK and worldwide, with ransomware remaining one of the most acute threats to the UK. It is almost certain that there was an increase in ransomware and data extortion attacks in 2023 from the previous year.

Double extortion Refers to an attack where cyber criminals exfiltrate data from a victim's network before encrypting it with ransomware. Cyber criminals then demand that that a ransom is paid to prevent cyber criminals from publishing or selling on the stolen data and for the victim's network to be decrypted.

The fact that HMG does not pay Ransomware has not prevented governmental and quasi-governmental organisations being impacted as illustrated by the British Library incident**. If cyber criminals can carry out a Ransomware attack on UK Defence then they will.**

Conclusion on Threats

Nation states especially Russia and China will remain a significant cyber and espionage threat to Defence related information

Nation states will target defence personnel on social media (such as LinkedIn). Anyone who has access to sensitive information will be considered a target. Since the goal is often theft of intellectual property, defences must be robust and monitoring of networks needs to be vigilant.

Defence sector IT chains remain a strategic vulnerability.

Cross-sector threats, in particular, financially motivated ransomware attacks will represent the most likely disruptive threat to the Defence industry. Successful attacks will cause business disruption and put intellectual property at risk.

Russia and China in particular will target the Defence sector for the following reasons:

➢ Insight into strategic capabilities

➢ Understand resources and gaps

➢ Current operations and future plans

➢ Insight into cleared personnel

Not just the usual four! We only know what we are actively looking for.

Dealing with the Threat

Quite simply MOD and wider government need to continue to **get better at developing and delivering systems that are secure.**

Risk management must be centred on the business – security as an enabler

- Risk appetite red lines
- Threat modelling and attack trees
- Use controls wisely outcomes based not compliance based
- Gain assurance through a mix of approaches
- Through life security

Topics to consider

- Identification of assets
- Incident response
- People focussed security operations
- Secure by design

Accreditation Certificates do not deter attackers, designed in cyber security does.

NCSC’s Five principles for the design of cyber secure systems

1. Establish the context before designing a system
Before you can create a secure system design, you need to have a good understanding of the fundamentals and take action to address any identified short-comings.

2. Make compromise difficult
Designing with security in mind means applying concepts and using techniques which make it harder for attackers to compromise your data or systems.

3. Make disruption difficult
When high-value or critical services rely on technology for delivery, it becomes essential that the technology is always available. In these cases the acceptable percentage of ‘down time’ can be effectively zero.

4. Make compromise detection easier
Even if you take all available precautions, there’s still a chance your system will be compromised by a new or unknown attack. To give yourself the best chance of spotting these attacks, you should be well positioned to detect compromise.

5. Reduce the impact of compromise
Design to naturally minimise the severity of any compromise.

Thank you

Rick C

Rick.C@ncsc.gov.uk

@NCSC

in National Cyber Security Centre

CyberHQ

Ministry of Defence

Cyber Security

Major Peter Malan CISSP - SO2 Defensive Cyber and Electromagnetic Activities

ARMY
BE THE BEST

Resilience and Business Continuity
"What are we protecting and why?"

Major Michelle Churcher
HEO Counter-Intelligence Operations and Plans

Dorian
National Protective Security Authority (NPSA)

Owen Sudlow
Group Technology Director, Babcock International Group

15:35-16:05

Coffee and Networking

Panel Discussion

K.D

MOD Chief Security Officer

Kristina Evans

Head of Cyber and Security, British Army

Air Commodore Mike Wilson

Head GRC CyDR, MOD

Matt Lock

Technical Director UK, Ireland and Middle East, Varonis

Doug Davidson

Senior Director & Cybersecurity Lead for Aerospace & Defence, Capgemini

Owen Sudlow

Group Technology Director, Babcock International Group

Closing Remarks

Major General John Collyer
Director Information and Army CIO

Kristina Evans
Head of Cyber and Security, British Army

Richard Morgan
Founder, Chief Disruptor Defence

Closing Remarks: Major General John Collyer – Director Information

ARMY

CHIEF DISRUPTOR

Ministry of Defence

babcock™

BT Means Business

EVERFOX

Cellebrite

TANIUM™

VARONIS

GLOBAL EMC
-ELECTROMAGNETIC SHIELDING & ANECHOICS-

Capgemini

National Protective
Security Authority

Strategic Command
Defence Digital

National Cyber
Security Centre

Closing Remarks: Kristina Evans – Head of Cyber and Security

ARMY

CHIEF DISRUPTOR

Ministry of Defence

babcock™

BT Means Business

EVERFOX

Cellebrite

TANIUM™

VARONIS

GLOBAL EMC
-ELECTROMAGNETIC SHIELDING & ANECHOICS-

Capgemini

National Protective Security Authority

Strategic Command
Defence Digital

National Cyber Security Centre

CHIEF DISRUPTOR

ARMY

babcock™

GLOBAL EMC
ELECTROMAGNETIC SHIELDING & ANECHOICS

TANIUM.

VARONIS

Capgemini

Cellebrite

EVERFOX

BT Means Business

CHIEF DISRUPTOR

ARMY

babcock™

GLOBAL EMC
ELECTROMAGNETIC SHIELDING & ANECHOICS

TANIUM.

VARONIS

Capgemini

Cellebrite

EVERFOX

BT Means Business