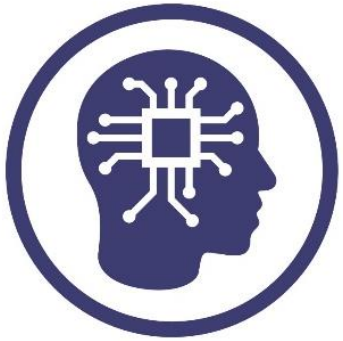


Challenges around socio-technical AI Systems in Defence: A Practitioners Perspective

PROFESSOR STEVEN MEERS

Head of AI Lab, Defence Science & Technology Laboratory, UK MOD

Visiting Professor, Centre for Machine Intelligence, University of Southampton

DSTL/PUB124219

Dstl delivers Defence and Security S&T across UK Government

- MOD Executive Agency
- 4,000 employees, 5 Divisions, 22 Capability Areas
  e.g. Cyber, Space, Human Sciences, Advanced Materials
- ~£650M income, 50% spent externally
- CAST (Home Office S&T) joined Dstl in April 2018
- Defence and Security Centre of Excellence for S&T
  - Cross-Government Collaboration: HMGCC, GCHQ, PHE etc

Cyber & Information Systems

Decision Support & Analysis

Counter-Terrorism & Security

Chemical & Biological Defence

Platform Systems

Sensitive & Specialist Research

Advice, Analysis & Assurance

Maintain Sovereign Capability

Support Operations

Trusted Government Interface to Suppliers, Academia

Develop & Exploit knowledge / IP

We must harness AI for defence & security in a manner that is **moral & ethical**, reinforces **international norms** and **counters irresponsible use**

"Future progress in AI has the potential to be a **transformative national security technology**, on a par with nuclear weapons, aircraft, computers, and biotech"

Artificial Intelligence and National Security, Belfer Center for Science & International Affairs

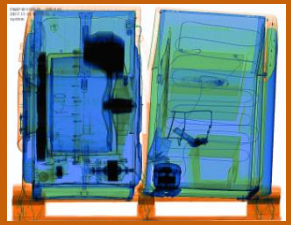
Image used with permission unsplash.com

COMMAND & CONTROL

LOGISTICS

INTELLIGENCE+ SURVEILLANCE

HOMELAND SECURITY

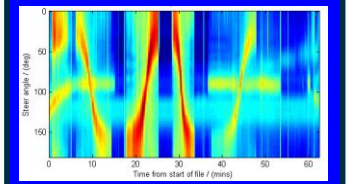


NETWORK DEFENCE

COUNTERING FAKE NEWS

POWER PROJECTION

OCEANOGRAPHY



CHEMICAL & BIOLOGICAL DEFENCE

SURVIVABILITY

KNOWLEDGE MANAGEMENT

BUSINESS OPERATIONS

Coalition Assured Autonomous Resupply

CHALLENGE

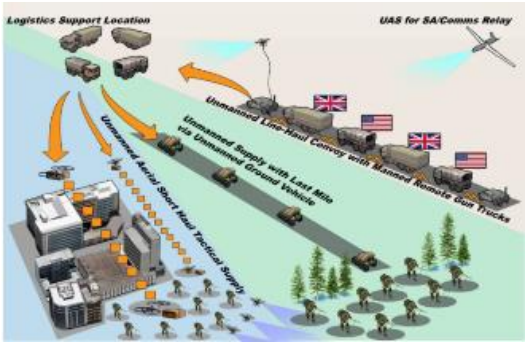
- Rapidly developing, demonstrating and evaluating autonomous systems technologies in tactical logistics applications for frontline users In particular for the hazardous “last mile resupply”

APPROACH

- 4-year UK-US collaborative endeavour
- Dstl-led Defence Accelerator (DASA) 2-phase competition launched April 2017
- ~£8M Industry contracts (including 2019 Capstone)
- Phase 2 MOD partnership with Dept for Int’l Development & UKRI
- Conducted 2 major field experiments with a range of industry and academia consortia

BENEFIT

- Project Theseus to accelerate to operational experimentation as ‘prototype warfare’ pilot
- Established joint US/UK experimentation programme



Predictive Maintenance for Type 45

CHALLENGE

- With high demand for deployed capability, the Royal Navy needs to reduce the logistics burden, increase availability, and reduce maintenance costs for its ships, submarines and aircraft

APPROACH

- Programme NELSON, decisionLab, Dstl, Defence & Security Accelerator have developed an AI-enabled predictive maintenance application
- Data is collected from over 4500 sensors on T45 ship systems, and provided to the application by the NELSON data platform
- Machine learning techniques are used to forecast sensor values into the future and flag anomalies, indicative either of sensor failures or component degradation

BENEFIT

- The application is deployed to HMS DEFENDER, demonstrating the ability to work with third parties to develop advanced applications and deploy to warships
- De-risks the application of AI techniques to predictive maintenance for future platforms

NELSON

SAPIENT - Autonomous sensing

CHALLENGE

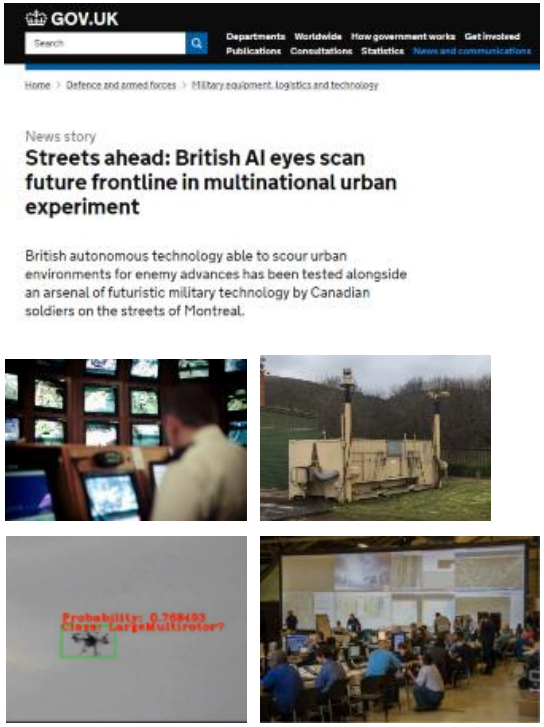
- Human operators are unable to effectively monitor large numbers of sensor inputs for a protracted period of time

APPROACH

- Developed SAPIENT (Sensing for Asset Protection with Integrated Electronic Networked Technology)
- SAPIENT is an open & modular architecture that enables smart sensors to make their own decisions about what they are sensing and react accordingly
- Demonstrated in base protection, urban operations & counter-UAS scenarios

BENEFIT

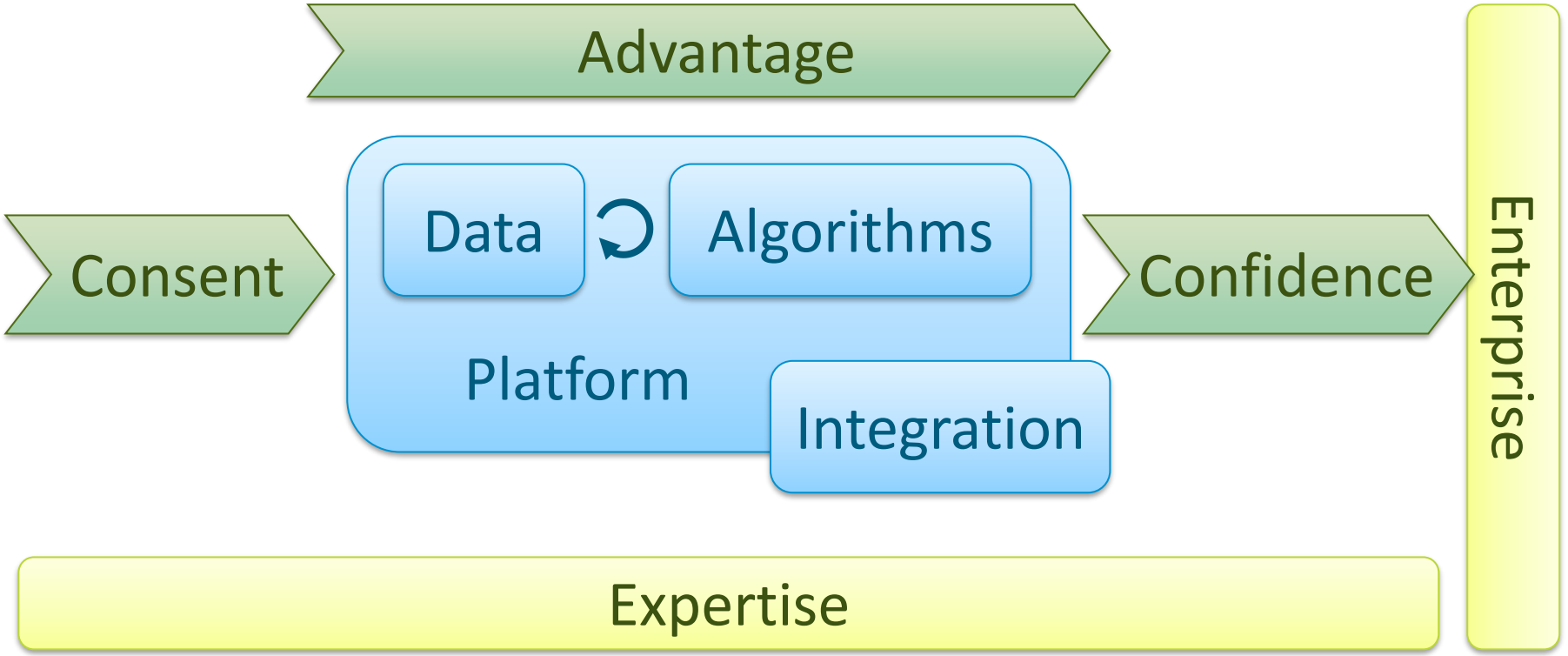
- Exploited by Army HQ as one of the underpinning technologies for the Future Integrated Tactical ISTAR
- Used in international Contested Urban Environment experiment and now being taken forward via an collaborative project with international partners
- Created an “open market place” for sensing systems



The AI Paradox

It is deceptively easy to launch AI pilots with initially powerful results.

At the same time, it is fiendishly hard to deliver those solutions at scale across a large enterprise.



Air Information Experimentation Centre

NAVYX

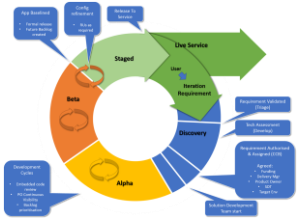
Prototype warfare

Centre for Intelligence Innovation

NELSON

The Alan Turing Institute

Dstl & ATI work on military AI ethics



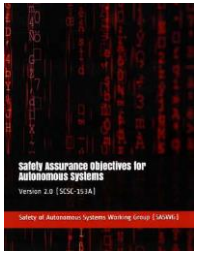
Agile approaches & action research

Ministry of Defence

UK MOD AI ethics policy development

Advantage

- User-centric design
- Cost-benefit analysis
- Threat understanding
- Agile/DevOps



Safety assurance objectives

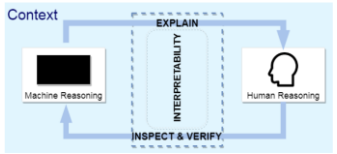
US DOD AI Principles

Consent

- Legal frameworks
- Ethics & responsible AI
- Policy & risk appetite
- Public perception

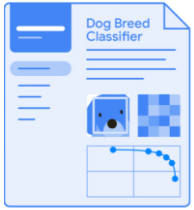
Confidence

- Trustworthiness
- Safety & "certifiability"
- Assurance & resilience
- Explainability



Conversational Agents

Synthetic data generation



Model Cards

Defence specific algorithm development

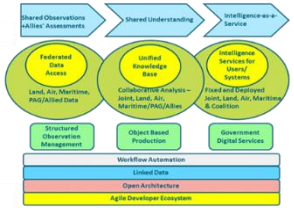
Information Based Security Architecture

Data

- Data quality & format
- Availability & sensitivity
- Privacy & usage rights
- Data bias & provenance

Algorithms

- Selection/effectiveness
- Robustness/complexity
- Performance limits
- Intellectual property



Single Intelligence Environment

Platform

- Cloud, on-prem, edge
- Open architectures
- Standards & interfaces
- Security

Integration

- Systems integration
- Human machine interface
- Interoperability

Technology Demonstrator Programmes

Inclusion Ignites Innovation

Diverse workforce

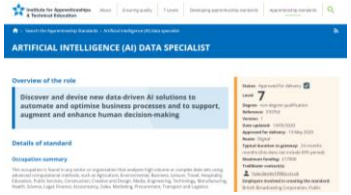
$$\max_{\pi} Q_{\pi}(s,a) = \max_{\pi} \{E_{s',a'}\,[r_{t+1} + \gamma Q(s',a') | \, s_t = s, a_t = a]\}$$

Learning & development scheme

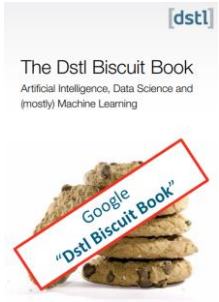
Strategic Command
Defence Digital

Agile Acquisition

Experimentation



AI Apprenticeships



AI primers

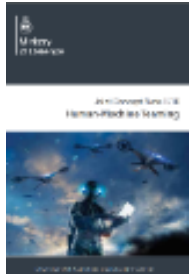
Expertise

- Suitably qualified and experienced people
- Diversity
- Learning and development
- Flexible commercial relationships
- Recruitment and retention
- Reskilling

Enterprise

- Strategy & governance
- Financial & commercial frameworks
- Acquisition
- Concepts and doctrine
- Experimentation
- Force structures
- In-service support

Defence AI & Autonomy Unit



Human machine teaming Joint Concept Note

AI building blocks

- Looking for external validation of this approach
  - Email ai_lab@dstl.gov.uk, Subject: AI building blocks
- Being used as a framework for
  - Scientists and engineers
  - S&T planners
  - Policy makers
  - Programme managers
  - Military desk officers
- Underpinned by a set of best practice guides to provide detailed advice

Image: Wikipedia

Key messages

- UK MOD sees AI as a **transformative national security technology** however the **“AI paradox”** is limiting the pace of change

- A **socio-technical approach** helps **address the barriers** to operationalising AI technologies within the Defence & Security environment

- Building blocks provide a **structured framework for socio-technical development** of AI systems
  - Feedback welcome to ai_lab@dstl.gov.uk

Questions?