Royal Academy of Engineering

Government Office for Science

Research topics 2026

Topic 01 - Scene characterisation using passive radar

Key words:
Passive Radar, Signals of Opportunity (SoOp), Emerging RF Sources, RF Scene Characterisation, Urban Remote Sensing · Through-wall Sensing · RF Propagation · Infrastructure Validation · Disaster Response · Wireless Channel Exploitation · Machine Learning. ·

Research topic description, including problem statement:
Characterising scenes in dense urban environments remains a challenge when conventional active sensors, such as LiDAR or SAR, are constrained by deployment practicalities, regulatory limits or the need for covert operation. Passive radar systems, which make use of existing ambient radio frequency (RF) transmissions, known as **signals of opportunity (SoOp)**, offer a compelling alternative. These signals may include VHF broadcast radio, digital television, Wi-Fi, cellular signals (4G/5G/6G), smart city or campus IoT networks and other emissions likely to be present in an RF-dense, urban environment. This research will enable those responsible for the architecture or operation of government buildings to better understand and mitigate the risks from emerging passive radar sensing techniques.

We invite proposals to investigate the effectiveness of passive radar for extracting meaningful structural or environmental information from urban scenes. A particular focus is on understanding the **relative merits and limitations of different SoOp** including prevalent, **emerging or future signal types**.

Whilst the concept of using passive radar for general detection is well established, its **utility for detailed scene characterisation**, such as inferring internal structures, layouts or materials of buildings remains an open question. Challenges include understanding how different signal types interact with building materials, what kind of resolution is achievable in cluttered RF environments and how signal properties affect penetration, reflection and detection.

Examples of Scenes of Interest:

- Characterising a building's **structural composition** and understanding its effects on signal propagation.
- Investigating the impact of a building's **internal layout** and features.
- Assessing the accuracy and reliability of passive radar for **measuring features' physical dimensions**.
- Exploring how **infrastructure such as cables, pipes or HVAC systems** affect signal propagation.

- Investigating the accuracy with which **human occupancy** could be determined or quantified.

Example approaches:
Proposals may pursue experimental, simulation-based or analytical approaches. Possible directions include:

- **Experimental Studies**: Deploy passive radar systems to test various SoOp, including 5G, DVB-T, Wi-Fi, IoT or emerging technologies in representative urban environments to evaluate their sensing capabilities.
- **Simulation and Modelling**: Use ray-tracing or EM modelling tools to predict signal propagation and interaction with common construction materials and urban layouts.
- **Signal Processing Algorithms**: Develop or apply techniques for structure inference and imaging from passive radar data, including machine learning, compressed sensing or tomographic reconstruction.
- **Time-scale Performance Analysis**: Investigate how sensing performance varies when systems operate in near real-time compared with scenarios allowing for long-term integration over hours to months, seeking to improve characterisation accuracy.
- **Multi-signal Analysis**: Comparative assessment of SoOp types in terms of penetration depth, spatial resolution and sensitivity to structural features.

Example Techniques:

- **Synthetic Aperture Passive Radar (SAPR)**: Obtaining high-resolution data on surface structures.
- **Multi-static Passive Radar (MSPR)**: Employing multiple receivers around a building's periphery to enhance detection accuracy of internal features and track changes from different angles.
- **Machine Learning for Signal Processing**: Identifying subtle structural changes within large data sets over time.

Topic 02 - Instant RF lockdown: a Faraday-on-demand system for prisons and secure facilities

Key words:
RF suppression, communications security, contraband mobile phones, Faraday cage, prison technology.

Research topic description, including problem statement:
Illegal communication through smuggled mobile phones remains one of the most persistent threats to prison safety and public protection.

This topic explores the concept of an instant RF lockdown mechanism a system or process capable of cutting off all radio frequency communication in a designated area *on demand*, creating a temporary Faraday-like effect. The challenge is to design this capability in a scalable, safe, and legally compliant way that can be activated in response to security incidents, drone incursions, or intelligence-led operations.

Example approaches:
- Engineering deployable or room-scale RF-shielding systems (e.g., flexible or switchable materials that can block signals when energised).
- Development of low-cost, localised Faraday enclosures using smart materials or metamaterials.
- Exploring electromagnetic “red button” architectures that allow instant local lockdown.
- Assessing RF leakage patterns and modelling containment zones to inform dynamic activation.
- Evaluating health and legal implications under Ofcom and HMPPS operational constraints.
- The use of RF metamaterials.

Topic 03 - Printed power supplies - new materials and technology

Key words:
Power Supplies, Batteries, Materials, Energy, Miniaturise, Printable, Fuel Cells, Supercapacitors.

Research topic description, including problem statement:
We propose a 2-year postdoctoral research project to explore the development of printed batteries and power supplies for wearable devices. Building on the promising demonstration of printed batteries, this research aims to advance the technology and investigate its potential for consumer applications.

The project will focus on:

- Material development: Investigate new materials and configurations for printed batteries, optimizing their performance, energy density, and stability.
- Device design and fabrication: Explore various device architectures and printing techniques to improve battery performance and enable consumer-friendly printing.
- Wearable device integration: The commercialisation of integrated printed into small electronic body-worn devices is encouraged, assessing their feasibility and user experience.
- Alternative power supply options: Investigate 3D printing and other techniques to create novel power supply configurations, such as supercapacitors or fuel cells.
- Consumer-centric design: Consider the user experience and develop guidelines for consumers to print their own batteries using the developed materials and devices.

The research will be conducted in close collaboration with industry to ensure the project's relevance, applicability and to avoid duplication. The expected outcomes include:

- A range of printed battery configurations with improved performance and energy density
- Novel power supply options using 3D printing and other techniques
- Design guidelines for consumer-friendly printing of batteries and power supplies
- Integration of printed batteries into wearable devices, demonstrating their feasibility and user experience.

This research has the potential to enable the widespread adoption of wearable devices, providing consumers with convenient, affordable, and sustainable power solutions. The project's findings will be disseminated through academic publications, industry reports, and patent filings, ensuring the research has a significant impact on the field.

By supporting this research, we can unlock the potential of printed batteries and power supplies, driving innovation in the wearable technology sector and beyond.

Example approaches:

Consumers are becoming more attracted to both wearable and portable technology. This requires power in very small and portable forms, perhaps on extremely thin media such as fabric or paper. To transfer materials to a medium such as fabric or paper, printing has for some time been an accepted method. This would allow either garment suppliers to add power supplies to their products, or for consumers to retro fit them themselves. It could also allow consumers to create their own small power supplies if they had the right printing equipment.

Topic 04 - Exploring how unusual investment could be detected using open-source data, data visualisation tools and AI

Key words:
AI, Data visualization tools, open-source data, economic security, NSI Act, 17 mandatory sectors, investment, economist, data scraping.

Research topic description, including problem statement:
Investment into technology businesses is both an opportunity for growth and exploitation. The National Security and Investment Act (NSI) gives the government powers to scrutinise and intervene in business transactions, such as takeovers, to protect national security, while providing businesses and investors with the certainty and transparency they need to do business in the UK.

Within investment, it is difficult to identify and target areas of national security concern within investment in both a timely and cost-effective manner. This can be particularly evident when the investment is obfuscated by layers of different investors. Research needs to be done into the way companies are able to be divided into sectors and those that could be particularly vulnerable to outside hostile investment. By being able to classify companies into mandatory sectors, it will be possible to help identify those that need the most protection and monitor the different types of investment that might occur. Additionally identifying the type of data that would best help solve these problems and researching the way it could be utilized, will enable further research into what the investment picture in the UK looks like. Ultimately using AI to identify patterns and flag potential future outcomes is one way of using the latest technology to help inform decision making.

Researching how different pre-existing sources of open-source data could be defined, analysed and best presented to ensure the maximum recognition within different government organisations would enable a greater understanding of hostile actors and the methods used to avoid detection. By also using AI it could be possible to pull out areas of concern that are not so easily identifiable by human analysis and bring these concerns to light/attention. Using AI, it could be possible to work out whether an investor is considered high-risk without the need for analysis by government departments including the Competition and Markets Authority (CMA). This would provide monetary public saving, whilst also helping automate manual processes.

Example approaches:

The researcher would carry out a piece of work to identify out of the 17 mandatory sectors which companies would be associated with them. This could be through company website scraping, identifying company numbers/unique codes or using other methods. Also identify sources of data that when placed together could help build a comprehensive picture of what investment is occurring within the UK.

Then using a data visualization application and AI, build a tool that could be easily used by multiple collaborators. The tool would have clear flagging of concerning investment/data, either by AI or by collaborators, and enable traceability of investment using open-source data.

Topic 05 - Origami antennas with self actuation

Key words:
Origami Antennas, Deployable Antennas, Self-actuation.

Research topic description, including problem statement:
Origami is the traditional Japanese art of paper folding, where flat sheets of paper are transformed into intricate three-dimensional sculptures without using cuts, glue, or other materials. Having originated with simple forms like cranes and flowers, origami has evolved to include incredibly complex designs, geometric patterns and modular structures. This ancient practice combines artistic expression with mathematical principles, making it both a artistic craft and a subject of scientific study in many engineering fields. In electromagnetics, the idea of Origami antennas has recently emerged, where a 3-dimensional antenna is formed from a series of folds in 2-dimensional sheet, bringing various application benefits such as tuneability, reconfigurability and the ability to deploy the antenna.

One application that has been a particular focus of deployable origami-type antennas is space/satellite antennas, where large, highly directive antennas are folded down to reduce the size of the payload at launch and then deployed once they reach orbit (e.g., NASA's Starshade project). Other scenarios that would benefit from such an approach to antenna design include military communications and ad-hoc networks. The antenna requirements in these scenarios differ significantly when compared to satellite communications. For example, while space antennas prioritize high gain (>30 dBi) and can tolerate single-deployment mechanisms, terrestrial military antennas must balance moderate gain (10-20 dBi) with multi-band operation (VHF through Ka-band) and survive hundreds of deployment cycles. The antenna structures may be complicated and extremely sensitive to variation in physical form, requiring robust designs that maintain electrical performance despite mechanical tolerances and environmental stresses. Additionally, terrestrial applications often demand rapid deployment and redeployment capabilities, operation across multiple frequency bands, and the ability to withstand repeated folding cycles without degradation. They may have to function reliably in harsh conditions while maintaining portability and ease of use by non-specialized personnel. The inherent advantages of origami-based designs including predictable folding patterns, high compaction ratios and self-locking mechanisms make them superior to traditional telescoping or umbrella-type deployable antennas, particularly when complex aperture shapes or conformal designs are required.

Reconfigurable origami antennas leverage controlled folding states to dynamically alter electromagnetic properties across multiple dimensions. These structures can potentially achieve frequency reconfiguration by changing their effective electrical length through folding angles, enabling operation across octave bandwidths, pattern reconfiguration by morphing between omnidirectional and directive states through aperture reshaping, beam steering through asymmetric folding or rotating faceted surfaces without traditional phase shifters, and polarization agility by adjusting the orientation of radiating elements from linear to circular polarization.

However, a number of research challenges remain. Material selection presents a critical challenge where substrates must exhibit sufficient flexibility for repeated folding while maintaining stable dielectric properties, low loss tangents and minimal hysteresis effects. Conductive materials face the additional burden of surviving stress concentrations at fold lines without cracking or delaminating. The complex form of such antennas, which combine mechanical folding kinematics with electromagnetic behaviour, lead to interesting questions regarding how to design these antennas for specific scenarios. System designs must also consider the effect of the accompanying electronics and RF front end. Actuation methods remain a formidable challenge, as traditional approaches using motors or manual intervention are impractical for many applications.

Emerging solutions include shape-memory alloys that suffer from slow response times and high-power consumption, electroactive polymers with limited force generation, and magnetically-controlled origami requiring external field generators. The integration of these actuation mechanisms without compromising antenna performance or adding excessive weight and complexity is an interesting area of research. Potential solutions may take a hybrid approach, combining multiple actuation strategies and self-folding materials responsive to environmental stimuli.

Example approaches:

We are interested in proposals that cover one or more of the following topics:

- Frequency tunable, pattern reconfigurable and beam steering origami antennas
- Design methods and techniques for origami antennas
- Antennas that fold to an extremely low form factor
- Advanced materials and manufacturing techniques for origami antennas (shape-morphing alloys, liquid metals, 4D printing) and Origami antennas with self-actuation.

References:

- S. I. H. Shah, et al., "Lightweight and Low-Cost Deployable Origami Antennas—A Review," in IEEE Access, vol. 9, pp. 86429-86448, 2021
- Y. Yang *et al*., "A Review of Multimaterial Additively Manufactured Electronics and 4-D Printing/Origami Shape-Memory Devices: Design, Fabrication, and Implementation," in *Proceedings of the IEEE*, vol. 112, no. 8, pp. 954-999, Aug. 2024
- Mishra, A.K. *et al.*, R.F. (2024), Robotic Antennas Using Liquid Metal Origami. Adv. Intell. Syst., 6: 2400190.

Topic 06 - Optically transparent antennas & metasurfaces

Key words:
Optically Transparent Antennas, Antennas, Metasurfaces, Indium Tin Oxide, ITO, Optically transparent conductors, Invisible antennas, Materials, Graphene.

Research topic description, including problem statement:
Recent years has seen the development of optically transparent antennas (OTAs) that can be seamlessly placed onto transparent materials (such as glass, Perspex, PET) without introducing significant absorption of light within the visible spectrum. The development of OTAs has been driven by a need to provide seamless coverage of wireless networks within buildings and offices. This has become especially relevant as devices begin to implement mm-wave RF systems as the radio waves at these frequencies are unable to propagate through typical materials (glass, brick, plaster) without suffering absorption or scattering effects.

OTAs antennas are often made using Indium Tin-Oxide (ITO) which has an optical transmittance of around 75% for wavelengths of 400-760nm, with a sheet resistance of around 5Ω/sq. Alternative conductive oxides such as Al-doped Zinc Oxide have also shown promise along with conductive (silver) nano-wire meshed structures. It is important to understand the trade-offs of different approaches, whilst also consider the latest innovations and materials (i.e. graphene) both in terms of performance and practical implementation (i.e. availability, ease of manufacture and cost).

Examples in the literature often present antenna structures such patches that utilize the glass substrate to support the antenna. However, the presence of feedlines and connectors reveal the presence of the antenna. It is also possible to still see an antenna “shadow” as the absorption of the conductor (i.e. ITO) differs to that of the background substrate (the glass). This effect could be minimised by also engineering the optical transparency of the supporting substrate (i.e. the glass) to match that of the conductive material and seamlessly integrating these together. Alternative antenna structures such as leaky-wave antennas [Zhou, 2025] and loops may be considered to improve performance and coverage or reduce the overall antenna form.

Passive metasurfaces can be designed to eliminate reflection and maximize transmission of radio waves through various materials [Chu, 2021, Zhuang 2025]. Optically transparent metasurfaces designed in such fashion could be printed over glass windows to enable wireless network coverage in environments that are otherwise difficult to reach, through illumination of the metasurface-window from

a remote location. These OT metasurfaces may also be designed to block transmission at specific frequencies [J. Ge].

Example approaches:

We are interested in research proposals that address one or more of the following areas:

- Optically transparent conductive RF materials (i.e. alternatives to ITO, silver nano-wires)
- Optically transparent antenna structures (alternatives to the planar patch arrays) looking at optimising both the antenna visibility and controlling radiation performance
- Optically transparent transmission-metasurfaces to enhance RF network coverage within enclosed environments
- OTAs on different types of glass (e.g. clear windows, tinted windows, double glazing etc.)
- The effectiveness of OTAs on other opaque materials

References

- Z. Zhou, Y. Zhang, Z. Kuang, Y. Li and Z. David Chen, "An Optically Transparent Near-Zero-Index Grating Metamaterial for Enhanced On-Glass Millimeter-Wave Radiation," in *IEEE Transactions on Antennas and Propagation*, vol. 73, no. 6, pp. 4092-4097, June 2025
- J. Ge *et al*., "Optically Transparent Metasurface With Multispectral-Compatible Camouflage and Millimeter-Wave Transmission Window," in *IEEE Transactions on Microwave Theory and Techniques*, vol. 73, no. 9, pp. 5686-5695, Sept. 2025
- Chu, H., Zhang, H., Zhang, Y. *et al.* Invisible surfaces enabled by the coalescence of anti-reflection and wavefront controllability in ultrathin metasurfaces. *Nat Commun* **12**, 4523 (2021)
- Y. Zhuang, Z. Zhu, T. Deng and X. Huang, "RFGlass: Optically Transparent Transmissive Metasurface for Coverage Expansion," in *IEEE Communications Magazine*, vol. 63, no. 5, pp. 24-31, May 2025.

Topic 07 - Quantum magnetometers for super low frequency magnetic field detection

Key words:
Quantum, Magnetometry, Sensors, Super Low Frequency, Weak Signal Currents.

Research topic description, including problem statement:
To build, optimize and assess the magnetic field sensitivity of Quantum Magnetometers in the sub 10KHz range.

Its intended application is the detection and characterization of weak signal currents at close range (<30cm) flowing in electronic circuitry, which may also be screened.

Example approaches:
Prior work has demonstrated that Optically Pumped Magnetometers (OPMs) have the potential to offer fT/√Hz sensitivities at 100's of Hz and tunable to 100's of KHz.

Topic 08 - Investigating security and assurance of building automation and control systems (BACS)

Key words:
Building automation, control systems, security architecture, physical security, digital twins, Internet of Things (IoT).

Research topic description, including problem statement:
Problem statement - The UK has schemes to assess enterprise systems (e.g. Cyber Essentials Plus and the CAF), and for assurance of digital physical security systems (e.g., CAPSS). BACS are complicated cyber-physical systems and their security is generally not adequately addressed by the above UK schemes. Through this research NPSA seeks to collect evidence which may be used in future to develop a BACS assurance scheme. Evidence is sought regarding potential cyber-physical vulnerabilities inherent in BACS, to include the physical layer (e.g., sensors and actuators) and the presence of legacy components (i.e., hardware, software, firmware) and legacy master/reference data.

Description – With pressures to reduce costs, achieve greater energy efficiency, monitor building occupancy/utilization and maintain safe and secure working environments, the sophistication of BACS has significantly increased. This partly reflects digitalization of control systems, but also the need to manage increasingly complex interactions between building systems. From a security perspective the situation is exacerbated by adoption of IoT technologies, often based on consumer quality components, and innovations such as digital twins of built assets. The latter, often cloud-based, may offer unintended insights into the pattern-of-life of buildings and their users.

From energy efficiency and emissions reduction perspectives some innovations require continuous third-party access to building systems for control and monitoring purposes. For example:

- adoption of demand side response (DSR),
- provision of energy management services linked to on-premises renewable generation and battery storage,
- deployment of heat networks.

The third parties may require varying levels of access to building systems and seek to install remotely accessed monitoring, physical sensors and actuators.

In addressing the problem statement, proposals should consider how relevant information will be collected and set out an appropriate methodology to support

identification of weaknesses in the design, deployment and use of BACS. While this research may assist the future development of an assurance scheme, NPSA's priority is collect evidence on which any future scheme may be based.

Note – this research is not to intended address development or use of digital twins, as the focus is on BACS. However, it can consider connectivity to digital twins, along with the nature of the information embodied in and/or data collected from the building/built asset.

Example approaches:

In building the proposed evidence base, NPSA anticipates that the researcher will employ some of the following approaches in their work plan:

- Undertake a literature survey of research regarding the security of BACS
- Search for and build a repository of published vulnerabilities regarding BACS, including elements used in IACS
- Investigate security measures deployed in operational BACS and create anonymized case studies
- Stakeholder interviews to understand security perspective of those who design, install, commission and operate BACS.
- Investigate security measures deployed in operational BACS and create anonymized case studies.

Research proposals should explain which approaches the researcher intends to employ and how they will identify and engage with stakeholders to collect evidence.

Topic 09 - Attitudes and barriers to adoption of security-minded information management

Key words:
Security mindset, data sharing, open data, data aggregation, data quality, provenance.

Research topic description, including problem statement:
Problem statement – This topic is intended to explore the barriers to adoption of the UK's National Protective Security Authority (NPSA) advice regarding security-minded practice and behaviour, of which data sharing and communication are a priority. In a world where it is common for people to share a wide range of personal information via social media, there appears to be a diminished awareness of the potential value of information. Consequently, there are increased security risks related to inappropriate data sharing or disclosure by businesses, despite advice published by NPSA.

Description – As the UK's technical authority for personnel and physical security, NPSA develops security guidance to assist organisations in designing, building, operating and managing the critical national infrastructure (CNI). Evolving business practices and the presumption that sharing data creates innovation and value are encouraging many CNI organisations to publish information that hitherto would have remained private. The situation is exacerbated by misunderstandings regarding the Open Data Institute's (ODI) data spectrum regarding the openness of data and by the organisations' supply chains. Consequently, insufficient attention is paid to the current and/or future value of data or information, e.g., data in context, resulting in disclosure of material that can materially harm the data owning organisation.

In engineering sectors, adoption of digital engineering practices, e.g. design collaboration using cloud-based computer aided design (CAD) software, has led to a dramatic increase in the volume of information and technical data shared between organisations. Coupled with the adoption of a culture of greater openness and sharing of organisations' information, e.g., adoption of policies such as Ofgem's presumed open policy. These developments potentially undermine good security practices by increasing the quantity and quality of data available to those conducting hostile reconnaissance or espionage or simply wanting to obtain competitive advantage.

This research seeks to explore the attitudes, awareness, and understanding of organisations and their managers regarding the risks inherent in data/information sharing. Of particular interest are the barriers to adoption of security advice

provided by NPSA regarding security-minded information management and communications. This research is primarily focused on the sharing of information relating to built or engineered assets and infrastructure, including their design and use, and associated patterns of life. Whilst the research may touch upon GDPR/Data Protection Act issues, this should not be the primary focus of a research proposal. While GDPR and the Data Protection Act set out to ensure individuals' privacy and protection of sensitive personal data/information, there is currently no equivalent regulation or legislation approach for other data/information.

Aspects that could be investigated include:

- Understanding by organisations and individuals of risks arising from sharing data and information with third parties, e.g., understanding the difference in risk profiles of intended recipients compared to anyone who can access the data (e.g., those without a legitimate need for access),
- Understanding by organisations and individuals of data aggregation and its potential to magnify data sharing risks and create a latent intelligence risk,
- How organisations and individuals assess the sensitivity of data and information, and the difference between classifying documents, data files, and sharing of streamed data,
- Developing an understanding of the differing perceptions of information/data risks within an organisation, e.g., perceptions at different levels of seniority, by different job roles (e.g. data scientists, technologists, administrators, etc.)
- Understanding 'risky-shift' in relation to classification and/or sensitivity assessment by groups and/or individuals, and the extent to which groupthink may influence such decision-making,
- The identification, understanding, adoption and use of methods or techniques to establish information needs,
- The assessment of the provenance of data and information.

Example approaches:

- Undertake a literature survey of research regarding the sensitivity of non-PII data/information
- Development of case studies illustrating how misuse of published/open data contributed to hostile reconnaissance
- Investigate practices regarding the classification of sensitive non-government information by data owners, with the aim of identifying best practices.
- Stakeholder interviews to understand the perspective of owners/curators of sensitive non-PII data/information
- Identification and demonstration of measures that can be deployed to desensitize non-PII data/information prior to sharing
- Stakeholder interviews regarding their understanding and use of existing NPSA guidance regarding security-mindedness.

Topic 10 - Indicators of military stress and resilience: distinguishing chronic and acute adaptations

Key words:
Epigenome · Exposome · Stress Biology · DNA Methylation · Military Health · Resilience Biomarkers · Non-invasive Sampling · Molecular Wellbeing · Veterans.

Research topic description, including problem statement:
Military personnel experience distinctive combinations of physical, psychological and environmental stressors that differ profoundly from those of the civilian population. The extremes of training, deployment and operational tempo, particularly within special forces, impose unique physiological and psychological loads that may leave persistent molecular signatures.

Recent advances in epigenomics suggest that environmental and behavioural exposures are recorded in the chemical modifications that regulate gene expression. These **epigenetic markers**, including DNA methylation, histone modification and non-coding RNA, can act as durable indicators of cumulative experience, stress load and recovery. They therefore provide a potential route to measure, objectively and longitudinally, *how much stress is useful and adaptive versus how much is damaging*? We invite proposals to identify and characterise **epigenomic indicators** that help to address this question.

Particular interest lies in differentiating **acute versus chronic** stress signatures, understanding their **durability after service** and evaluating how **environmental and geographical exposures** (e.g. deserts, jungles, high altitude, polar or maritime stations) may leave lasting imprints that can be measured. The overarching aim is to support personnel wellbeing and readiness through a molecular understanding of resilience and overload.

Example approaches:
Proposals may pursue a combination of experimental, analytical and computational approaches. Ethical approval must be sought from within the University, where appropriate, e.g. for collection and analysis of human DNA samples. Additional samples relating to military staff can be facilitated through OCSA. Possible research directions include:

- **Epigenomic Profiling:** Compare DNA methylation and related epigenetic marks across cohorts (civilians, regular forces, special forces, veterans) to identify loci or pathways associated with cumulative stress and adaptation.

- **Longitudinal Studies:** Track epigenetic changes through training, deployment and recovery phases to distinguish reversible (acute) from enduring (chronic) markers.
- **Integration with Physiological Data:** Correlate epigenetic patterns with cortisol levels, heart-rate variability, inflammatory markers or psychological measures to build multi-layered models of stress response.
- **Environmental and Geographic Exposure Analysis:** Investigate whether residence or operations in extreme or remote environments leave characteristic molecular "signatures" linked to hypoxia, UV exposure, isolation, or nutritional constraints.
- **Non-invasive Sampling Innovations:** Develop or validate minimally invasive bio sampling methods such as saliva, hair, breath condensate, urine or faecal DNA, that are suitable for repeated or field-based collection and compatible with epigenome-wide analysis.
- **Predictive Modelling:** Apply machine-learning or systems-biology approaches to identify combinations of epigenetic features that classify population groups or predict resilience versus vulnerability.

Topic 11 - Energy harvesting to power IoT sensors

Key words:
Energy harvesting, power harvesting, solar power, IOT sensors, long term power, solar power, biofilms, triboelectric generators, piezoelectric, radio frequency energy harvesting.

Research topic description, including problem statement:
The increased power demands of future edge AI sensors in a data-rich connected smart world are pushing requirements beyond classical batteries and requires a hybrid store and harvest approach. To increase the longevity of self-sustaining systems operational lifetime whilst maintaining reasonable form factors requires changes in how systems are powered. It is not feasible to just continually scale the size of the battery system to create an enduring system. Integration of alternative power sources such as those provided through energy harvesting systems can help to supply the required power whilst not significantly impacting the size of the system.

The system should be scoped as to function within a building, so any energy harvesting techniques would need to factor that in. Whether that be solar cells harnessing indirect sunlight, piezoelectric and triboelectric nanogenerators harnessing energy from pressure changes and vibrations or alternative biobased solutions.

A successful project would demonstrate an energy harvesting technology which could:

- Generate / harvest energy at a power of 10 mW ;
- Must be an enduring solution, lifetime >10+ years whilst requiring no maintenance ;
- Not impacting on the environment / operating location with additional noise, signal / waste emissions, safety;
- Be compatible with a system form factor of: 50 cm^{-3} .

Example approaches:
Integration of piezoelectric elements into places of repeated pressure or vibration, e.g. flooring, for kinetic energy harvesting. Depending on the use scenario the inconsistent energy generation profile may need to be assessed.

Perovskite / organic solar cells for capture of indoor solar energy. Optimization of absorption energies would need to be studied to tailor the energy band gap to efficiently absorb indirect/indoor solar energy.

Bioengineering based solutions could include: Use of polymer-based biofilms for production of energy harvesting devices such as triboelectric nanogenerators. Biological fuel cells, such as enzymatic or microbial fuel cells, can generate powers in the region of 4 Wm^{-2} and can be integrated with biocompatible sensors to produce as self-sustaining system [1].

Carbon-fibre based thermos cells for conversion of building low grade heat into electricity.
Meta materials combined with classical energy harvesting techniques to enhance performance or enable unusual or unexpected application.

References:

- [1] J. Environ. Manag., 307 (2022), Article 114525.

Topic 12 - Preparation, quantification and characterisation of trace explosive samples

Key words:
Trace, quantification, explosive.

Research topic description, including problem statement:
To understand the capability of explosive trace detection solutions, specific amounts of explosive material are pipetted on to swabs or surfaces for detection systems to interrogate. This allows the limit of detection (LOD) of a system to be determined but isn't very realistic when it comes to finding real traces. The thumb print test takes a known amount of explosive deposited on a surface and then stamps a standardised thumb on to it. It is then imprinted onto different surfaces or swabs multiple times, to create more realistic residues, decreasing the residual amount with each print. The current challenge of this technique is whilst the print is more realistic, the quantity of explosive within the print is unknown. So, whilst both tests combined provide a qualitative measure for how well a trace detection system performs, ideally, we require a method that combines the quantitative nature of the LOD technique with the more realistic thumb print test.

As such, although we have methods for quantifying the amount of explosive on surfaces this method is destructive (solvent extraction followed by GC/LC-MS analysis) and resource intensive. We are not able to quantify mass loading before testing a surface. We therefore require a quick, non-destructive, technique that could be used to determine mass loading on a range of different surfaces. It would also be useful to understand the surface coverage, crystal form, particle size and other characteristics.

Separately, but as part of the same topic, we would also be interested in investigating innovative techniques to enable more representative, realistic and reproducible trace contamination to be deposited onto surfaces for T&E purposes.

We could provide some examples of surfaces of interest and range of mass loadings we would need capability for.

Example approaches:
The focus of this project is to leverage emerging technology to develop a low cost, low burden solution to quantify the amount of explosive residue on various substrates. Approaches should include the development of a prototype system.

Topic 13 - Detection and defeat of uncrewed-aerial systems using novel communication or navigation techniques

Key words:
Drones, Counter-Drones, UAS, C-UAS, Detect, Track, Identify, Effector, Defeat

Research topic description, including problem statement:
The proliferation of drone technology has brought significant advancements in various sectors. However, this rapid growth has also introduced a range of new security challenges. The Home Office Counter-Drones Unit (CDU) plays a pivotal role in coordinating counter-drones policy with stakeholders across government to understand and address the increasing risk of Uncrewed-Aerial Systems (UAS). Drones are becoming increasingly capable of being used to conduct hostile and illegal activities. Drones have become a preferred tool for smuggling contraband into prisons, allowing criminals to bypass physical barriers, and deliver directly to prisoners. Small-UAS have been widely used by both sides of the Russia/Ukraine Conflict, to conduct reconnaissance and direct attacks. The conflict has driven rapid innovations in drone technology that has been widely shared online. In recent months drone sightings have caused significant disruptions at airports across Europe. These examples illustrate some of the increasing security challenges posed by drones.

Alongside increasing use, drone technology also continues to evolve rapidly. Increasingly, both commercial and home-made drones are operating on the cellular network, making use of increasing autonomy, or other novel communication or navigation techniques (such as fibre-optic controlled drones in Ukraine). These technologies are able to reduce the effectiveness of certain traditional Detect, Track and Identify (DTI) and defeat systems, and therefore, there is a growing need to investigate and support emerging research to both detect and defeat drone incidents.

This research topic has two key aspects:

1. Detection of drones operating using communications and navigation approaches beyond the traditional 2.4Ghz and 5.8Ghz WiFi bands. A pressing challenge in this domain are drones operating on the cellular network, but we are also interested in detecting drones operating autonomously or using other novel communications or navigation technologies.
2. Low-collateral defeat of such drones. Options for UK law enforcement to stop (and ideally capture) a hostile drone, without introducing significant risk to the public or infrastructure.

These are significant challenges being seen by both UK and international partners. Home Office CDU will be able to provide access to current policy direction, and access to operational partners to help shape the direction of any research and how it might ultimately contribute to the UK's efforts to detect and respond to drone incidents to protect UK citizens and interest.

Example approaches:

As above. This is a very fast-moving area, research will need to be adapted in line to reflect technology advances.

Topic 14 - Behavioural futures: modelling public trust in tech-enabled security and crime prevention/fighting

Key words:
AI-enabled surveillance, public trust, behavioural modelling, digital, foresight, societal resilience, adaptive policy, ethical AI, scenario analysis, lawful access, crime detection, national security, technology, prevention and detection of crime, investigatory powers, relevant legislation.

Research topic description, including problem statement:
The increasing integration of AI and other technologies into national security and crime prevention/fighting (particularly in surveillance, border control, and digital identity systems) raises critical questions about public trust, legitimacy, and long-term acceptance. While technical capabilities advance rapidly, public attitudes are shaped by complex socio-political dynamics and can evolve unpredictably.

Recent research by CETaS (Alan Turing Institute) shows that public perceptions of technology-enabled crime fighting already vary: some people are comfortable with machine analysis, while others prefer human intervention. Public acceptance and perceived legitimacy are dynamic, shifting with exposure, incidents, governance safeguards, and communication. As seen in early online banking fraud, behaviour and risk perceptions can adapt over time, potentially moderating initial harms. The Intelligence Community would benefit from evidence-based forecasts of these changes to inform capability rollouts, communications, and safeguards.

This project has two main elements. First, it will assess the current landscape and baseline views: as criminal techniques become more sophisticated and lawful access to data is hindered by private and secure technologies, what level of machine or human intervention does the public find acceptable in preventing and fighting serious crime? Key questions include: Are there crimes where tech-enabled intrusion is more acceptable? What minimum standards do people expect for investigations and evidence collection? What is the preferred human-tech balance in detection and investigation?

Second, building on this foundation, the project will model how public perceptions of AI and other technology-enabled security measures (e.g., facial recognition, predictive policing, digital ID systems) may shift under future scenarios, such as political instability, economic shocks, or rapid technological adoption. It will explore how behavioural adaptation, like increased digital literacy or desensitisation to surveillance, might moderate perceived harms, reshape societal responses, and influence government action.

The central problem is the lack of robust, evidence-based foresight into how public attitudes toward security technologies evolve over time, and how this evolution impacts the effectiveness, legitimacy, and ethical deployment of such systems.

Example approaches:

- Public responses**:** Polling, focus groups, peer review, research review, market research**.**
- Scenario Modelling: Develop plausible future scenarios using horizon scanning and expert input to explore how societal attitudes may diverge.
- Behavioural Simulation: Use modelling or system dynamics to simulate public responses to AI-enabled security interventions over time.
- Longitudinal Analysis: Incorporate historical case studies (e.g., online banking fraud adaptation) to understand behavioural shifts and resilience mechanisms.
- Mixed-Methods Research: Combine qualitative foresight techniques with quantitative modelling to capture both narrative and statistical dimensions of behavioural change.

Topic 15 - Foreign influence in UK politics

Key words:
Foreign influence, democracy, lobbying, national security, transparency.

Research topic description, including problem statement:
The UK welcomes open and transparent engagement from foreign powers. We know that foreign powers will sometimes use third parties, such as businesses, lobbying and advisory groups to conduct engagement and influencing activity on their behalf. There is a democratic and national security need to understand what efforts are being made by foreign governments to shape the decision-making of the UK government, and who is influencing our policy and policymakers.

Using the UK Government's definition of political influencing activity as set out in the recently-launched Foreign Influence Registration Scheme (FIRS) (those acting under contracts (informal, formal or financial) to undertake activity on behalf of a foreign government, where the purpose of that activity is to influence a decision of a Minister or Government department, MP or political party), this project would develop an assessment rooted in behavioural and social science research of the extent and nature of foreign-directed political influencing activity in the UK.

It should deliver a framework incorporating factors driving this activity at different levels: conditions within the perpetrating state (e.g. authoritarianism vs other types of regime), the international system (e.g. geographic proximity), the bilateral relationship with the UK, and the perceptions/reality of conditions in the target state (permissive/low-transparency business environment). In other words, are there countries the UK should expect more influencing activity from and how countries' approaches to political influencing activity differ. The FIRS definition necessarily puts the work of third parties such as lobbying firms or strategic communications consultancies at the centre of this research. Having a better understanding of which countries the UK experiences more influencing activity from and how that activity is conducted would be of interest to the public as well as the government.

Example approaches:
- Use open-source information and databases such as Office of the Registrar of Consultant Lobbyists, UK Government data, Parliamentary publications, and strategic consultancy/PR websites to identify patterns of influence or recurring actors across multiple countries.
- Conduct a literature review on relevant behavioural and social science research (lobbying and policy making, strategic influence in legislative lobbying, disclosing foreign influence in lobbying, soft power in the context of great

power competition). Ground the work in the appropriate theoretical approach, engage in hypothesis testing, data collection and evidence-based inferences to produce a paper.

- The project should produce c.4 illustrative and accessible case studies to highlight the difference in how states seek to engage in political influence based on their characteristics. This could cover China, a FVEYS country (eg Australia/US), an EU country (eg Germany), a Middle Eastern state (e.g Saudi Arabia).
- The project could include a collaborative hypothesis-generation workshop early on to generate hypotheses and test sample assumptions such as:
    - All countries carry out some level of political influence in the UK using third parties.
    - Those countries with closer diplomatic and economic ties are more likely to conduct influence activities in the UK but less likely to use third parties.
- There could be an opportunity to provide Home Office's FIRS data for analysis in light of the project's findings – though this material could be redacted from the final project and the HO would reserve the right to review any findings that relate to FIRS prior to publication.

References:

The Foreign Influence Registration Scheme (FIRS) is the jumping off point for this research. This scheme came into force in 2025 as part of the National Security Act. It provides crucial additional powers to protect our democracy, economy and society. It does three things: provides transparency of foreign state influence in the UK, gives the police and MI5 a critical new disruptive tool with criminal offences for those who fail to comply with the scheme, and deters those who seek to harm the UK. By requiring registration from those carrying out certain activities at the direction of foreign powers, the scheme will make it more difficult for foreign powers to operate covertly in the UK.

More information can be found here: Guidance on the Foreign Influence Registration Scheme: political influence tier.

Topic 16 - Engineering biology for sustainable power generation

Key words:
Power sources, batteries, energy harvesting, engineering biology, synthetic biology, microbial fuel cells, soil microbial battery, electrogenic bacteria, bio-electricity, Internet of Things, low-power devices, sustainable energy, remote sensing.

Research topic description, including problem statement:
Reliable, long-duration power remains a constraint for distributed sensing systems, particularly when deployed in environments in which battery replacement is impractical. Power sources such as lithium batteries, solar panels or harvesting from ambient energy each have limitations relating to endurance, maintenance or environmental dependence. There is therefore strong motivation to explore **bio-derived, self-sustaining power systems** in which naturally occurring or engineered microorganisms generate electricity directly from soil or organic matter.

Engineering-biology approaches, such as microbial fuel cells (MFCs) or soil microbial fuel cells (SMFCs), offer compelling alternatives. These systems harness the metabolic activity of electrogenic bacteria found within soil or an organic substrate, passing the electrons they release through an external circuit to generate electricity. Recent work [1] has field-demonstrated proof-of-concept systems capable of powering water purification.

Significant limitations remain, however, including low power density, variable output, stability whilst operating under field conditions and the challenge of interfacing with IoT electronics or power-management systems. The goal of this research topic is to develop and test **engineering-biology power systems** that can power IoT devices sustainably under real-world conditions.

Example approaches:
- Microbial/biological engineering [2]: Identify, engineer or enrich electrogenic microorganisms (e.g. Geobacter, Clostridiaceae) for improved current output, stability in variable environments and compatibility with low-nutrient or waste-substrate operation.
- Electrode and materials engineering [3]: Develop novel electrode materials (e.g. bio-char, activated carbon from biomass waste, carbon felt/stainless steel composites) and architectures (i.e. electrode spacing, surface area, stack configuration) to optimise electron transfer and durability of microbial fuel cells.

- Power harvesting and electronics integration: Design or adapt low-voltage, low-current energy-harvesting circuits and power-management systems to better suit the output characteristics of MFCs, suitable for powering power IoT sensor nodes, data logging or wireless communications.
- Field-deployment and sustainability assessment: Test MFC systems under realistic or tactical conditions (e.g. outdoor, variable soils and temperatures), evaluate long-term performance, maintenance needs, environmental impacts and lifecycle sustainability. Explore techniques such as stacking of cells and modular design to scale output and increase robustness.
- Application demonstration: Implement a demonstrator IoT node (sensor or communication device) powered by a microbial battery, measure operational lifetime, reliability and feasibility in a resource-constrained scenario.

References:

- [1] Dziegielowski, J, "*Development of a functional stack of soil microbial fuel cells to power a water treatment reactor: From the lab to field trials in North East Brazil*", Applied Energy (2020).
- [2] Jiang, Y-B, "*Characterization of Electricity Generated by Soil in Microbial Fuel Cells and the Isolation of Soil Source Exoelectrogenic Bacteria*", Front Microbiol (2016)/
- [3] Mutuma, B, "*Valorization of biodigestor plant waste in electrodes for supercapacitors and microbial fuel cells*" Chemical Physics (2021)
- [4] Hess-Dunlop, A, "*Towards Deep Learning for Predicting Microbial Fuel Cell Energy Output*" Electrical Engineering and Systems Science (2024)
- [5] Dziegielowski, J, "*Towards effective energy harvesting from stacks of soil microbial fuel cells*", Journal of Power Sources (2021).

Topic 17 - Human intuition and gut instincts in artificial intelligence

Key words:
Intuition, instincts, emotion, cognition, bias-reduction, information processing, decision-making, intelligence, law enforcement.

Research topic description, including problem statement:
Research demonstrates that professionals in law enforcement, defence, and intelligence use evolutionary ancient and implicit processes such as gut instinct and intuition in making decisions (often described in terms of sixth-sense, hunches)[1-5]. The reliability of these, especially of the more cognitively oriented intuition (essentially automated and pre-conscious information processing), tends to improve with time and experience. A significant risk of encouraging too great a reliance on instinct and intuition without the pre-requisite experience is the potential of encouraging ethically and professionally problematic biases, especially among novice and early career professionals. Over the past 20-years, the legitimacy of many implicit emotional and cognitive processes has been correctly challenged on this basis. During the same time, awareness of the risks of replicating human biases in AI systems grew as those technologies were refined, and significant improvements resulted, offering the potential for fast and unbiased decision making. However, given that AI is starting to play a role in law enforcement, defence, and intelligence, and that the line between professionally helpful gut instincts and intuitions on the one side and professionally unhelpful and unethical emotional and cognitive biases on the other, can be blurred even among human decision makers. How will AI replicate the helpful while removing the harmful? Further, if this is achieved, what role might AI play in training human professionals to better deploy their instinctive and intuitive capabilities without bias?

Problem statement - AI presents opportunities in law enforcement, defence, and intelligence. These range from: 1) fast and economic data analysis to 2) bias reduction to 3) accelerated development of human capabilities. Re 1 and 2, it has been argued that AI systems introduce 'data-driven, pattern-recognition methods that challenge the authority of subjective expertise by offering seemingly more objective, reproducible outputs'[6]. To counter this proposal, while AI might enhance the speed and scalability of information processing and reduce bias, by failing to model implicit human decision-making processes, it might reduce the reliability and effectiveness of these same processes, a possibility requiring some analysis. Re 3, the potential for AI to model expert human decision-making and play a role in optimizing this in human professionals is yet to be explored. There is potential for AI to be used to assist reducing the risk of cognitive biases when making risk-based decisions in both group/committee settings or following exposure of opinions of

others. Could AI facilitate decision making following the input of information and consider different viewpoints more objectively, without incorporating biases?

Example approaches:

Research would fall into three empirically discrete but overlapping strands, each at the interface of the applied behavioural sciences and digital engineering/technology.

Strand 1: Modelling instinctive and intuitive decision making in AI systems:

- Research to identify the role of gut instinct and intuition in law enforcement, defence, and intelligence, allied to an expert commentary as to how these might be incorporated into AI systems.
- Research to model gut instinct and intuition in AI systems allied to an expert commentary as to the degree to which emotional and cognitive heuristics are relied upon in law enforcement, defence, and intelligence, have been or might be accommodated.

Strand 2: Examining tensions between bias reduction and optimal instinctive/intuitive decision making in AI systems:

- Research in reducing biases in AI allied to an expert analysis of the degree to which decreased prejudices might also reduce the reliability of information processing and decision making in the relevant sectors.

Strand 3: Use of AI in training instinctive and intuitive decision making in novice (human) professionals:

- Research into expert decision making in law enforcement, defence, and intelligence, and identification of which of these skills and capabilities are traditionally trained via formal education and which are acquired via experience.
- Research in the existing or potential use of AI in the training of professional decision-making in law enforcement, defence, and intelligence – as well as in professions characterized by similar emotional, cognitive, and behavioural demands.
- A set of data-led recommendations as to opportunities presented by AI in the context of training and/or enhancing instinctive and intuitive decision making in relevant sectors.

References:

- Campeau H, Keesman LD. “You can't really turn it off”: The police “sixth sense” as cultural schema. *Sociological Forum* 2024;39(3):267-80.
- Carroll A. Good (or bad) vibrations: clinical intuition in violence risk assessment. *Advances in Psychiatric Treatment* 2012;18(6):447-56. https://doi.org/10.1192/apt.bp.111.010025 [published Online First: 2018/01/02]
- Frantz R. Intuition and behavioural economics: A very brief history. Handbook of Research Methods in Behavioural Economics: Edward Elgar Publishing 2023:321-31.
- Gigerenzer G. Expert Intuition Is Not Rational Choice. *The American Journal of Psychology* 2019;132(4):475-80. https://doi.org/10.5406/amerjpsyc.132.4.0475
- Stubbs G, Friston K. The police hunch: the Bayesian brain, active inference, and the free energy principle in action. *Front Psychol* 2024(1664-1078)
- Kingsley J, Eunice M. From gut feeling to algorithmic precision: redefining expertise in criminal profiling with ai. Unpublished manuscript, 2025.

Topic 18 - The role of machine learning (artificial intelligence) in behavioural detection

Key words:
Artificial intelligence, personnel security, insider risk, risk detection, risk mitigation, behavioural detection, behavioural indicators, hostile reconnaissance, hostile behaviour, stress, machine learning, predictive algorithm.

Research topic description, including problem statement:
Problem statement – How can we leverage (now and in the future) machine learning AI to detect and predict hostile national security threats? To what extent could machine learning AI be utilized for assisting in detection of behavioural indicators for national security threats, such as insider risk and hostile reconnaissance. Can AI offer a reliable technical capacity for accurate detection of behavioural indicators associated with these threats?

Description – Protective security –
As the UK's technical authority for personnel and physical security, NPSA develops security guidance to assist organisations designing, building, operating and managing the critical national infrastructure (CNI). Part of this includes guidance on how to detect behaviour that indicates a potential national security threat, including insiders acting within an organisation, or a hostile actor attempting to conduct an attack externally.

AI could offer the potential to provide technological assistance in behavioural detection relevant to national security threats, alongside human analysis. However, its capacity, efficacy, and limitations to do so remains unclear. To what extend could AI be relied upon as a tool for detection and risk management?

In scope:

- Machine learning – what is the capacity of machine learning AI systems to identify behaviour patterns or indicators in large data sets? What types of human behaviours can these systems detect without explicit programming of what indicators and patterns to look for? What are the limitations for these systems in detecting human behaviours? Could the data include analysis of video/visual information to identify visual patterns or indicators of hostile behaviour?
- Prediction algorithm in machine learning: What is the current capacity for prediction algorithms in machine learning to identify future risk? Could these systems be used to predict unrepeatable, low-frequency events? How much data and what quality of data would be required for reliable outcomes if applied to threat types such as detecting insider risk or hostile reconnaissance?

Aspects that could be investigated include:

- The capacity of AI to detect threat behaviours in organisational data (IT usage/access patters, and text content (HR records))
- The capacity of AI to reliably detect behavioural indicators from CCTV footage (e.g., signs of stress and anxiety, or behaviours that are outside of the 'baseline' for a specific environment')

Example approaches:

- Literature review of current research on AI capacity for behavioural detection
- Primary research testing multiple AI systems capacity for detection of behavioural indicators in relevant datasets (text, IT systems access, or CCTV footage of hostile/threat actors).

Topic 19 - Barriers to bystander behaviour in high trust work environments

Key words:
Bystander behaviour, upstander behaviour, concerning behaviours, reporting concerning behaviour, help-seeking.

Research topic description, including problem statement:
Problem statement – Teams that rely on each other for protection against physical threats (armed forces, frontline police, emergency responders etc.) often have a high degree of inter-personal trust and loyalty. This can make it difficult to seek external help when team members are struggling. In some cases, individuals who are struggling may go on to engage in maladaptive behaviours that can pose a risk of harm to themselves, their team, their organisation, and wider national security (insiders etc.). How can organisations encourage staff to report behaviours of concern that they observe in their colleagues and obtain the support their colleagues need, without damaging essential trust and loyalty within the workplace?

Description – NPSA's research and work with organisations has frequently highlighted the issue of under-reporting or a lack of intervention when counter-productive or unusual workplace behaviours are observed by employees. Such behaviours have often been seen to be pre-cursors to insider activity or welfare issues.

We are looking to understand how best to adapt our current guidance (for example, the It's Okay to Say campaign) for high trust teams and organisations, such as the Armed forces, emergency responders, and police forces, to overcome barriers to reporting concerning behaviours in teams that have intense bonds of inter-peer trust and loyalty.

Aspects that could be investigated include:
- Barriers to reporting concerns about colleagues' behaviour in suitable cohort occupations.
- Key demographic groups at highest risk from barriers to help-seeking within suitable cohort occupations.

Example approaches:

- Literature reviews on barriers to help-seeking behaviours on behalf of others in suitable cohort occupations with analysis of key themes.
- Surveys or interviews with key cohort groups to identify barriers to help-seeking on behalf of colleagues, and what factors would help to overcome these, with analysis of key themes.
- Literature review on barriers for an individual to seek help within suitable cohort occupations, and which demographic groups are least likely to seek-help, and analysis of key themes.

Topic 20 - The future of insider risk – evolving threats

Key words:
Insider risk, future threat, workforce management, hybrid working, technology, international politics.

Research topic description, including problem statement:
Problem statement – What are the key factors that will drive insider threat in the next 5-10 years? How can organisations prepare to mitigate this threat to national security?

Description – Understanding and countering insider threats is an ongoing effort for NPSA. Part of this effort is attempting to predict how insider threats might evolve in the near to distant future, to inform guidance that helps target harden the UK against these changes. We wish to further explore how insider threat might evolve in the future given societal changes that have emerged in recent years, such as changes to working practices since the emergence of COVID-19, economic trends and differences in impacts across generations, and growing awareness of climate change.

There are several broader trends in society, such as changing ways of working, rising extremism, and employment culture that will impact how insider threat manifests and must be detected. Further research is required to assess how these trends impact Insider Threat both now and into the future, and how NPSA can adapt its guidance to help prepare for changes in how these threats may manifest in the near future.

We are looking to explore current and future trends and themes across a variety of industries and thematics. This research will provide NPSA with a refreshed knowledge base, building on the NPSA 2013 Insider Data Collection study. The breadth of this research is essential to elicit themes impacting insider threat that we do not currently have an awareness of. Our intention is that this research will highlight some key areas to inform future research programmes.

Aspects that could be investigated include:

- Analysis of current trends and themes impacting Insider Threat. What is it that we should be caring about? What should our advice look like for the future workforce? Themes that could be included: working patters (working from home, hybrid working etc.), international conflict and politics (ideological motivations and identity), environmental change (wider societal changes and challenges), where are the risks where it comes to different generations?

- Analysis of future challenges for addressing Insider Threat. Will NPSA's IR guidance be fit for purpose for companies created in 10-20 years out? If not, what are the key changes we need to make to assist customers in preparing for future insider threats?

Example Approaches:

- Literature review exploring how socio-cultural trends impact on individual identity (international conflicts, politics, economic changes etc.)
- Primary research into key areas of staff concerns or disenchantment in the modern workplace in relevant cohort organisations (HMG)
- Historical analysis exploring how key themes such as political ideology and international conflict have impacted insider cases, comparing key time periods in modern history and undertaking longitudinal trends analysis (for example, comparing WWI to WW2, WWII to Cold War era, or Cold War to modern era).

Topic 21 - Integrating multimodality and context to automatic language analysis

Key words:
Linguistics, forensic linguistics, applied linguistics, computational linguistics.

Research topic description, including problem statement:
There are two main underlying problems with automatic approaches to language analysis: a lack of ability to account for context, and a lack of interpretability of language across different modalities (for example, audio, image, video, and text).

Human communication is exceedingly context dependent[1]. As a simplified example, if I state that *the table needs to be moved* a listener will automatically use context clues to indicate whether I mean an item of furniture, or an excel style table. These might be physical context clues, or indicators from the co-text. When people are talking about sensitive, taboo, or illegal topics, this reliance on context increases even more. Automatic language tools are improving at utilizing co-text to help improve the accuracy of work, but they are still limited in the range of context that can be considered.

A separate, but related challenge is that online communications are exceedingly important to the intelligence community, and increasingly multimodal. This might be a soundtrack which changes the intended meaning of a picture (for example a classic circus soundtrack over a social media video of me parking my car, indicating that I am not showcasing my excellent parking skills but encouraging ridicule), or an emoji pasted over the top of an image (for example a picture of snow, with a nose emoji, indicating that the post is about nasally inhaled drugs rather than snow). Cross-modal communication like this is now the norm in many groups and societies, and that is particularly the case when discussing taboo (or illegal) topics.

Dover (2022) highlights how significant the internet and electronic communications are to intelligence communities. Automated approaches to language analysis can enable the quick triage and handling of significant amounts of data, however where they struggle significantly is with bringing together meaning from across different modes. This means that a significant amount of the communicative content risks being lost before it reaches an analyst.

These changes in meaning provided by either the context or the different modalities might be instantly understandable to us as humans, but an automated approach that struggles to consider such aspects, will provide a severely limited output. The topic here is designed to seek ways to combat these two problems – to integrate a holistic understanding of language with automatic language approaches. The desire is that the outputs will therefore be grounded in applied

and sociolinguistics and able to address language and communication in a more accurate and reliable way, considering how language actually functions.

[1] Context is complicated but could include any significant information about how the text was created, for what purpose, under what conditions, created by whom and for which audience is it intended. This could include: the genre of the text (e.g. an email, social media message), the field of discussion (i.e. the topic area), external events or news (e.g. the broader socio-political context), the intended audience/interlocutors (e.g. public space versus private message between friends), the shared goals of the interlocutors (e.g. planning a crime), broader topics in the text (e.g. intertextuality in a discourse community), the previous interactions and other messages with that interlocutor (e.g. knowing that a meeting relates to an earlier discussion), and the cultural context (e.g. the metaphors and stories used may be interpreted differently in different cultural contexts). Within this work it may not be possible to study all those contextual influences on the message, but priority will be given to techniques that could be applicable across these different types of context.

Example approaches:

The exact approach will depend on the form of automatic language analyses that are being considered, though researchers will need to source their own data set(s) to show a proof of concept. An overarching example approach would be starting from a sociolinguistic or corpus linguistic perspective, and seeking to ensure that the understanding of how language works remains in the automated approaches. This is supported by the literature, most notably Grieve et al. (2024), who in their recent paper on the Sociolinguistic Foundations of Language Modeling conclude that "incorporating insights from sociolinguistics is crucial to the future of language modeling" (p17).

However the benefits of such integration has a much longer trail of evidence. For example, in a 2013 Native Language Identification challenge (sometimes called Other or Native Language Influence Detection), where participants seek to identify an author's first language (when they are writing in English), Bykh et al. (2013) achieved a higher classification accuracy that other participants through using linguistically-informed features in their classifier. This included features such as parts of speech, lemma realisations and use of derivational and inflectional suffixes. Further work on Other Language Influence Detection for forensic linguistic purposes by Kredens, Perkins, and Grant (2019) highlights how vital an explanatory rich approach (such as one grounded in sociolinguistic explanations and features) is to analysis of language in evidential and investigative situations.

Focusing on the concurrent analysis of both the verbal and visual aspects of Instagram posts at the same time, Caple (2018) shows that taking a corpus-assisted multimodal discourse analysis can reduce partiality and enable triangulation. Polli and Sindoni (2024) look at the multimodality in hateful memes, and that the interplay between non-hateful text and non-hateful images can be used to produce hateful messages. They note that multimodality is conceptualized differently across the domains of computer science and sociosemiotics, however they also show that AI driven models can benefit from sociosemiotic insights and incorporating a multimodal critical discourse analysis approach.

More specific focused example approaches might include:

- Given a set of political speeches or news reports that happen over time in a changing context (e.g. during a conflict), how could an understanding of context improve topic modelling, document summarisation, an understanding of the evolution of events, or other forms of automated analysis? This could include (for example) the change salience of different places or people during the conflict, or a need to show strength to an audience in reaction to provocation.
- Given a set of social media posts with associated images (e.g. memes), how could an understanding of meaning and mood be better extracted from the multi-media content? For example, memes such as Wojak and Pepe the frog are often adapted quickly to express emotion reactions and humour at a given situation – how could that data be analysed alongside the text to give a more nuanced understanding of messages. Another example would be when images are used to convey instant emotional impact – for example in Daesh propaganda, CGI from video games was used to make it seem like the Eiffel tower had been attacked, or during the 2011 London riots images were shown of the London Eye on fire. Images like this may have more impact than just text messages.

References:

- Bykh, S., Vajjala, S., Krivanek, J. and Meuers, D. (2013). Combining Shallow and Linguistically Motivated Features in Native Language Identication. In NAACL / HLT 2013 Proceedings of the Eighth Workshop on Innovative Use of NLP for Building Educational Applications, 197–206, Atlanta, Georgia: NAACL/HLT
- Caple, H. (2018). Analysing the multimodal text. In Corpus approaches to discourse (pp. 85-109). Routledge.
- Dover, R. (2022). *Hacker, Influencer, Faker, Spy*. Hurst Publishers.
- Grieve, Jack, Sara Bartl, Matteo Fuoli, Jason Grafmiller, Weihang Huang, Alejandro Jawerbaum, Akira Murakami, Marcus Perlman, Dana Roemling, and Bodo Winter. (2024) "The Sociolinguistic Foundations of Language Modeling." arXiv preprint arXiv:2407.09241.

- Kredens, K., Perkins, R., & Grant, T. (2020). Developing a framework for the explanation of interlingual features for native and other language infuence detection. *Language and Law/Linguagem e Direito*, *6*(2), 10-23.
- Polli, C., & Sindoni, M. G. (2024). Multimodal computation or interpretation? Automatic vs. critical understanding of text-image relations in racist memes in English. *Discourse, Context & Media*, *57*, 100755.

Topic 22 - Deepfake acoustic profiles

Key words:
Voice Forensics, Deepfakes.

Research topic description, including problem statement:
Some recent research ((Williams, et al., 2025) and (Schäfer, 2025)) has investigated looking at the acoustic/prosodic features of deepfakes and real audio and has identified several features that could be used to identify deepfakes. However, the data is used is not realistic/representative of potential casework. For example, utterances are short (less than ten seconds) and can be compared to clean controlled real samples etc.

Research should be undertaken to test the robustness of such methods under realistic and challenging conditions (longer samples, state-of-the-art generators, blind comparison) and to identify characteristics that makes real speakers look like deepfakes.

Example approaches:
The research results clearly indicate that there are several acoustic/prosodic features that can be used to identify deepfakes. For example, previous research has found the fundamental frequency (F0) to be a potential indicator of deepfakes. The researchers could start with this or many other acoustic features and assess their suitability to identify deepfakes.
An approach would be to implement in automated models to identify deepfakes and compare with traditional black box detectors and determine how this approach performs under more challenging and realistic deepfake scenarios.

The desired outcome is for the researchers to identify multiple acoustic features that can be used to identify deepfakes in a variety of realistic and challenging scenarios, noting differences based on recording environment, speaker characteristics etc.

References:
- Schäfer, K. (2025). AI Got Your Tongue? Analysing the Sounds of Audio Deepfake Generation Methods. International Conference on Multimedia Retrieval (pp. 2023-2027). Chicago: Association for Computing Machinery.
- Warren, K., Olszewski, D., Layton, S., Butler, K., Gates, C., & Traynor, P. (2025). Pitch Imperfect: Detecting Audio Deepfakes Through Acoustic Prosodic Analysis. arxiv.

- Williams, E. L., Jones, K. O., Robinson, C., Chandler-Crnigoj, S., Burrell, H., & McColl, S. (2025). How Frequency and Harmonic Profiling of a 'Voice' Can Inform Authentication of Deepfake Audio: An Efficiency Investigation. JAET.

Topic 23 - Programmable metasurface structures

Key words:
Metasurfaces, Radar, Communications, Electromagnetic Warfare, Space-Time Modulation, Electromagnetic Wave Manipulation.

Research topic description, including problem statement:
Metasurfaces are engineered surfaces composed of arrays of sub-wavelength elements that can dynamically and precisely manipulate electromagnetic wave properties such as phase, amplitude, and polarization. In the context of this research, their ability to shape and modulate electromagnetic waves across spatial, spectral, and temporal domains provides new opportunities for signal manipulation and control. For example, recent work has demonstrated the effectiveness of metasurface-based techniques in relation to electromagnetic warfare (EW) [1].

Zhang et al. [2] introduced space-time-coding digital metasurfaces that enable dynamic manipulation of electromagnetic waves by programming both spatial and temporal responses. This allows for real-time modulation and precise wavefront shaping. Building on this foundation, recent research [3] has applied machine learning to achieve multi-frequency synthesis, enabling metasurfaces to adaptively generate complex waveforms across a broad frequency range.

These advancements significantly enhance control over electromagnetic wave scattering, particularly in the spatial domain. By enabling angular distribution of scattered energy, the technology allows signals to be directed toward multiple receivers simultaneously. This spatial versatility has important implications for systems that rely on angular diversity—such as radar—where it can disrupt accurate target localization by introducing ambiguity across multiple detection angles.

There are many other potential applications of metasurfaces to modify electromagnetic waves, for example, enhancing or modifying signatures of signals reflected by targets towards radar or communications systems, perhaps including some limited data modulation to in effect create a one-way communications channel, etc.

Collectively, these studies establish a strong foundation for extending metasurface-based approaches. Building on this and others' work, the proposed research will investigate how programmable metasurfaces can be developed designed and developed for multiple uses and in as varied domains as possible (air, land, sea, space) and for as many platforms as possible (everything from land

vehicles to ships, aircraft, space satellites and even clothing worn by people). The research will develop metasurface designs with the ability to generate effects in both the temporal and spatial domains, the research will explore material and designs suitable for the environments and uses outlined above.

Problem Statement - Metasurfaces offer a unique opportunity, due to their ability to dynamically manipulate electromagnetic wavefronts across spatial, spectral, and temporal domains, enabling precise control over signal distortions. This research addresses novel and advanced designs of metasurfaces that could lead to their widespread adoption. For metasurfaces to become ubiquitous across domains and platforms, designs are require that have the potential to meet the usual constraints of any technology to be adopted widely: size; weight; power; cost; mechanical robustness; the ability to operate in as many environments (for example, temperature, humidity, etc.); simple to integrate into existing structures; all while having as broad a frequency coverage and instantaneous bandwidth as possible.

Example approaches:

The following example approaches illustrate how the proposed capability could be developed and evaluated through a combination of theoretical analysis and concept demonstration:

- Theoretical Modelling: Develop analytical models of advanced and novel designs of metamaterials to predict the performance they may achieve, taking into consideration the designs' suitability for real-world applications (for example, size, weight, power, cost, etc.).
- Concept Demonstration: Investigate methods to design and fabricate metasurface-based concept demonstrators capable of real-time adaptive signal modulation. This will be used to experimentally validate the most promising metasurface designs from the earlier modelling phase.

References:

[1] R. G. L. de Mello, "Metasurface-driven Electronic Warfare". Hoboken, NJ, USA: Wiley-IEEE Press, 2025.

[2] Zhang, L., Chen, X.Q., Liu, S. et al. "Space-time-coding digital metasurfaces". Nat Commun 9, 4334, 2018. https://doi.org/10.1038/s41467-018-06802-0

[3] M. Rossi, L. Zhang, X. Q. Chen, C. Liu, G. Castaldi, T. J. Cui, and V. Galdi, "Machine-learning-enabled multi-frequency synthesis of space-time-coding digital metasurfaces," *Adv. Funct. Mater.*, vol. 34, no. 40, p. 2403577, Oct. 2024, https://doi.org/10.1002/adfm.202403577.

Topic 24 - Enhancing interviewer memory

Key words:
Investigative interviewing, Memory.

Research topic description, including problem statement:
Decades of research has illustrated the fallible nature of human memory, exploring implications ranging from day-to-day contexts (e.g. Schachter, 1999) through to unreliable and suggestible eyewitness testimony (Loftus, 1996; Wright and Loftus, 2008; Zaragoza, Belli and Payment, 2013).

However, research exploring the accuracy of memory recall of interviewers in the field is limited. The aims of this research are to comprehensively examine tools and techniques from but not limited to, cognitive psychology and investigative interviewing research, that could support increasing the accuracy of memory recall of interviewers in the field. A range of techniques should be explored, from techniques the interviewer can do/use following an interview to techniques that could be applied as a team approach. Additionally, this research should take into consideration the factors that can impact upon interviewer memory. The research should also consider the practicality of applying techniques and tools within a real-world context and propose research methods that would provide ecological validity to any findings. For example, in some real-world applications there may not be the option to have technology in the interview.

Example approaches:
Research methods such as field studies, analysis of real-world data and laboratory studies have been used previously to explore how memory functions during interviewing, including what factors impact on accuracy of recall. Similar approaches could be used for this study with the focus on read-world use cases relevant to the IC and FVEY IC Partners.

Topic 25 - Advancing forensic DNA analysis using microhaplotypes: enhancing mixture deconvolution, and ancestry inference

Key words:
Forensics, DNA, Sequencing, Microhaplotypes, Mixture deconvolution, Ancestry inference.

Research topic description, including problem statement:
Traditional forensic DNA markers such as short tandem repeats (STRs) and single nucleotide polymorphisms (SNPs) have limitations when applied to degraded samples, complex mixtures, and ancestry inference. While STRs offer high discrimination power, they are prone to stutter and mutation, and SNPs, though stable, often lack sufficient allelic diversity. There is a growing need for alternative genetic markers that can overcome these challenges and enhance forensic capabilities.

Microhaplotypes are short DNA segments composed of multiple closely linked SNPs that are inherited together as a unit, forming distinct haplotypes. These markers can be reliably distinguished using modern sequencing technologies and offer several advantages over STRs and SNPs, including low mutation rates, high allelic diversity, and suitability for degraded DNA. Their combined inheritance makes them particularly promising for forensic applications such as human identification, mixture deconvolution, and prediction of biogeographical ancestry.

Initial studies have demonstrated the potential of microhaplotype-based models to infer the biogeographical ancestry of contributors in two person mixed DNA samples. However, for microhaplotypes to be adopted in routine forensic practice, several challenges must be addressed, these include:

- The availability of sufficiently large and diverse population databases.
- The design of a robust forensic microhaplotype panel.
- The development of advanced bioinformatic tools for haplotype phasing, interpretation, and mixture analysis.

Additionally, machine learning and statistical modelling are needed to enhance predictive accuracy and automate complex analyses.

Example approaches:

Microhaplotypes are increasingly recognised as a promising next-generation tool in forensic genetics, offering enhanced resolution for individual identification, mixture deconvolution, and ancestry inference. Their usefulness could be significantly improved through the integration of advanced bioinformatics, machine learning, and statistical modelling. Machine learning enables the detection of complex patterns in genetic data, supporting accurate interpretation of mixtures and ancestry classification. Bioinformatics tools are essential for processing sequencing data, phasing haplotypes, and ensuring reliable profile generation, including from degraded or low-template samples. Statistical modelling provides the quantitative framework for population genetics analysis, likelihood estimation, and method validation, ensuring robust and defensible forensic conclusions. Together, these disciplines will enhance the precision, scalability, and evidentiary value of microhaplotype-based forensic DNA analysis.

Examples of potential approaches:

- Identify microhaplotype panels for forensic relevance across diverse populations.
- Develop and validate protocols for microhaplotype-based mixture deconvolution using massively parallel sequencing.
- Assess the performance of microhaplotypes in ancestry inference compared to existing STR and SNP-based methods.
- Create tools and databases to support forensic laboratories in adopting microhaplotype analysis.

Topic 26 - Ocean acoustic modelling for superior environment intelligence

Key words:
Sonar, underwater acoustics, ocean, measurements, modelling, data, information, intelligence, surveillance, reconnaissance

Research topic description, including problem statement:
Next Generation and Generation After Next acoustic superiority (including sonar, acoustic communications and any other acoustic technology/operation) in the underwater battlespace will depend significantly on our understanding and exploitation of the ocean acoustic environment (both the propagation of sound and the inherent noise created by the environment). Understanding acoustic behaviour in the ocean environment, and acoustically-relevant properties of the environment, is highly complex depending on a wide range of factors that change both spatially and temporally across multiple scales – even on the calmest days, the ocean is constantly changing, under the influence of a wide range of complex and dynamic ocean-acoustic factors. Presently, only the simplest acoustically-relevant properties of the environment are well described by measurements and only the simplest ocean-acoustic factors are considered in modelling.

This research topic aims to combine several research challenges to produce a plenary ocean-acoustic model that can digest complex ocean-acoustic data and generate superior intelligence about the ocean-acoustic environment, reflecting a greater understanding of acoustically-relevant properties of the environment, which can be exploited for the purposes of
intelligence, surveillance, and reconnaissance, as well as commercial monitoring of the ocean. Research challenges include:

- mathematical descriptions of acoustically-relevant ocean properties, such as internal waves, eddies, and spice, covering multiple spatial and temporal scales;
- investigation of methods to provide the best self-consistent picture of the ocean acoustic environment via direct and indirect measurements (e.g. acoustic measurements);
- development of physics based, data driven, or hybrid acoustic models, including noise and propagation models, to describe acoustic behaviour in the presence of different acoustically-relevant ocean properties;
- sensitivity and uncertainty analysis and quantification, based on the quantity and quality of input environment data to ocean-acoustic models;
- investigate the computational efficiency and accuracy of different models, including different model configurations;

- development of schemes to generate, visualise, and exploit (understanding the required fidelity of) the best available description of the ocean acoustic environment;
- investigate ocean-acoustic models, and other methods, to monitor the health of, and changes to, the ocean environment.

Example approaches:

The research challenges can be approached using a mix of applied mathematics, programming, statistics, data analysis, and machine learning. Example approaches include:

- develop an underwater acoustics foundation model to understand and process ocean-acoustic data and to generate ocean-acoustic information for different applications; this could include the design and conduct of large scale data collection and preparation activities and other data collection to enable fine tuning for specific applications;
- develop new analytical and numerical models to understand and predict acoustic behaviour in a variety of different environment conditions; this could include the development of methods to synthesise a variety of acoustically-relevant properties of the environment and to represent these properties in the acoustic models;
- develop an efficient framework or architecture for combining different ocean models and acoustic models; this could include the design and development of intelligent hybrid models that optimise the combinations of models based, for example, on uncertainty or computational efficiency.

Topic 27 - Improving synthetic aperture radar image formation through inverse modelling and Bayesian inference

Key words:
Synthetic Aperture Radar, Volumetric SAR, Position Navigation and Timing, Inverse Problem, Bayesian inference, SAR Interference, Urban Sensing.

Research topic description, including problem statement:
Intelligence, Surveillance, and Reconnaissance (ISR) systems rely on high-quality Synthetic Aperture Radar (SAR) imaging to deliver situational awareness. However, standard SAR imaging methods depend on simplifying assumptions that are often invalid in complex operational environments.

This research goal is to enhance SAR image quality and tactical interpretability by formulating SAR image formation as an inverse problem with a bespoke, selectable forward model. The research will focus on developing and demonstrating novel algorithms that improve performance under realistic and challenging conditions, such as:

- Interference from additional radio frequency sources, including distributed low-power noise.
- Artifacts caused by urban structures, complex wave scattering, or layover.
- Dynamic scenes, involving moving targets or structural vibrations.
- Time and positional errors during data collection.

Applicants are encouraged to address one or more of these problem areas through proof-of-concept algorithm design and demonstration. Research should incorporate Bayesian inference methods to design and evaluate inverse solvers, considering both linear and non-linear aspects and exploring dimensionality reduction or computational feasibility techniques.

Image quality should be evaluated using standard SAR performance metrics (e.g., resolution, noise-equivalent sigma-zero, sidelobe ratio) alongside subjective interpretability.

Example approaches:
https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9160976
In this article, the solutions for several inverse problems encountered in SAR imaging are considered, using the ARFL (Air Force Research Lab) Gotcha dataset, among others, to exemplify.

https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=10548437

This example describes a nonlinear SAR modelling capability, which is used alongside Umbra SAR data using manual trial and error to arrive at a likely structure observed within a given scene.

https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9497317

In this paper, several regularization methods are explored aiming to mitigate against the effects of interference in the SAR imagery. The problem is posed as a signal separation problem, and real data is used to demonstrate the results.

Topic 28 - Tracing the invisible: novel magnetic resonance isotope analysis for forensic footprints

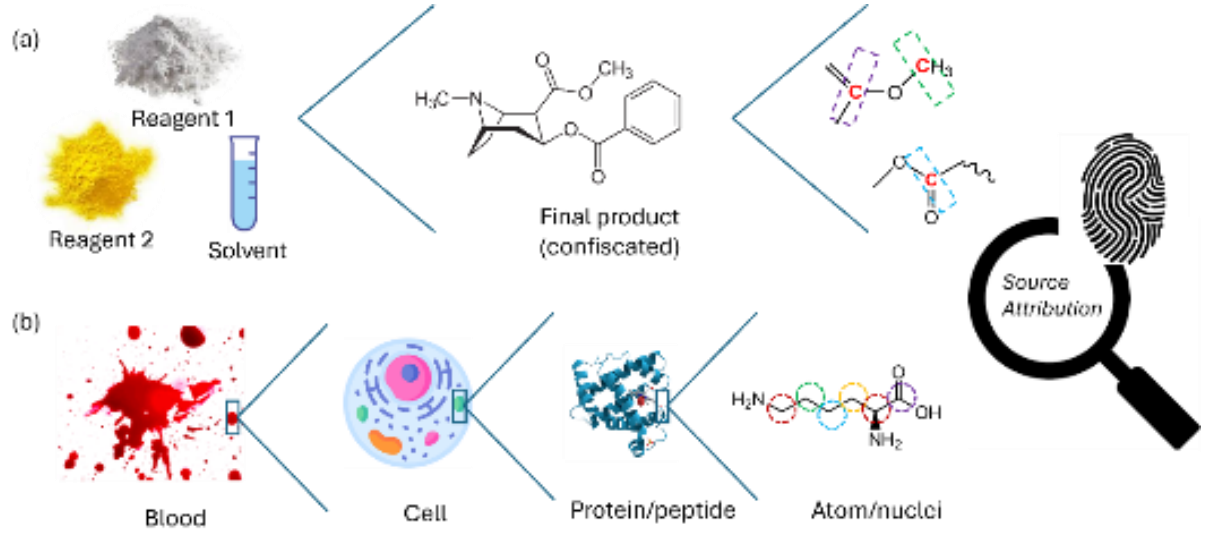
Key words:
Forensics, Trace Analysis, Fingerprints, Route Attribution, Origin, Material properties, Isotopic ratios, Nuclear Magnetic Resonance (NMR) and Imaging (MRI); Bio/Chemical Agents.

Research topic description, including problem statement:
The use of isotopic composition as a forensic and analytical tool has become a well-established discipline across environmental science, food authentication, counterfeiting, and pharmaceutical quality control.[1] Traditional bulk isotope ratio techniques (e.g. IRMS) provide valuable insights into origin and transformation processes, but they lack the resolution to distinguish isotopic variation at specific atomic sites within a molecule.[2] By harnessing the power of Nuclear Magnetic Resonance- NMR's atomic level precision, Position-Specific Isotopic Analysis (PSIA) offers a transformative approach, enabling the direct measurement of isotope ratios at individual molecular positions, thereby unlocking a new dimension of chemical origin and process attribution.

Recent studies have demonstrated that PSIA can reveal subtle isotopic fingerprints linked to synthetic pathways, metabolic transformations, and environmental conditions.[3,4, 5, 6] However, for complex attribution studies such as tracing the movement of a compound through multiple production stages (e.g. Chem/Bio agent synthesis) or environmental compartments the molecular isotopic landscape (e.g. blood samples, DNAs) becomes increasingly intricate. The proposed research of position-specificity will provide unprecedented insight into origin, transformation, or contamination of samples interests to wide of intelligence services including police, national security and defence.

More specifically, this research will advance the understanding of key isotopic attributes (e.g. site-specific ^{13}C, ^{2}H, ^{15}N ratios) that offer maximum insight into molecular provenance and transformation history. Furthermore, it will assess the impact of localized anthropogenic influences such as industrial solvents, synthetic reagents, or environmental pollutants that may alter or obscure isotopic signatures, either enhancing or confounding interpretive value.

Figure 1: Illustration of the proposed research's applications in two scenarios leading to source attribution of (a) confiscated drugs and (b) samples collected from a crime scene.



NMR is a supremely powerful technology with a wide range of applications, spanning from drug discoveries to disease diagnosis, most notably in the form of MRI. Its strength lies in its ability to accurately determine molecular structure from completely unknown substances in a non-destructive and non-invasive manner. The proposed research is well-positioned to fully exploit these advantages, advancing NMR toward frontline applications in a host of intelligence scenarios.
The expected outcome of this research to include- (a) A validated suite of NMR-based PSIA protocols for intelligence community; (b) A curated database of position-specific isotope signatures for key compounds e.g. novel illicit drugs, bio/chemical agents; (c) Demonstrated applications in forensic attribution, quality control, and environmental tracing; (d) Peer-reviewed publications with open-access analytical and software tools for wider applications.

Example approaches:
This research builds on a rich foundation of laboratory-based and field-informed approaches that have proven effective across disciplines such as geo-forensics, pharmaceutical sciences, food authentication, counterfeit detection, and environmental provenance research. By combining multi-analytical strategies with emerging technologies, the research goal will be to extend these methods into the molecular realm using position-specific isotopic analysis by NMR (PSIA-NMR).

PSIA-NMR offers a uniquely powerful tool for probing isotopic variation at the atomic level. When integrated with existing forensic, environmental, and biochemical frameworks, it can significantly enhance our ability to trace origins, verify authenticity, and understand transformation pathways. Unlike bulk isotope techniques, PSIA-NMR reveals subtle, site-specific signatures that often hold the key to unravelling complex histories.

The molecular targets in this research may include novel pharmaceuticals, synthetic intermediates, environmental metabolites, and even bio/chemical warfare agents. Each of these compounds carries a distinct isotopic fingerprint, one that reflects its source, method of synthesis, and environmental exposure. By analysing these fingerprints at specific atomic positions, the research will uncover layers of information that are otherwise inaccessible. The insights gained will be broadly applicable across sectors, from drug regulation and environmental monitoring to food safety and biomedical research, ultimately helping us better understand where things come from, how they change, and what stories they carry.

References:

- [1] P.H. Abelson, T.C. Hoering (1961), Proc Natl Acad Sci USA 47:623–632;
- [2] A.H. Lynch *et* al., (2011), Rapid Commun Mass Spectrom 25:2981–2988;
- [3] S. Guyader *et* al., (2019), Flavour Fragrance J 34:133–144;
- [4] D.W. Hoffman, C. Rasmussen (2019), Anal Chem 91:15661–15669;
- [5] T. Jezequel *et* al., (2017), Magn Reson Chem 55:77–90;
- [6] E. Tenailleau *et* al., (2004), Anal Chem 76:3818–3825.

Topic 29 - Multi-vector approaches to deanonymising privacy coins

Key words:
Privacy coins; Digital Data Threat; Investigation; Analysis.

Research topic description, including problem statement:
The threat posed by serious organised crime, rival states, and state-sponsored proxies is amplified by the digital data threats associated with privacy-focused cryptocurrencies, a form of decentralised finance. Open-source assessments suggest that some high-end law-enforcement and intelligence agencies may have developed methods to de-anonymise traceable ledgers, which sit on more open ledgers. The techniques for de-anonymising privacy coins are far more challenging. Open-source reviews of anti-money-laundering cases and crypto suspicious activity reports indicate significant blind spots in current intelligence practices.

Training from private vendors often emphasises heuristics designed for transparent chains (e.g., Bitcoin, Litecoin, Ethereum) and tactics like coin-dusting—approaches that adversaries can easily defeat and that do not transfer well to privacy-by-design systems. Where de-anonymisation of privacy coins by private entities is reported in the open source data it is said to have relied upon combining multiple investigative vectors—such as through investigation on the dark-web, examining the timing and sequencing of transactions, on examining network metadata and other data such as “know your customer” information rather than on any single analytic technique, as might be more common with transparent chains.

In terms of dedicated consultancy activity, CipherTrace (2021) claimed some ability to deanonymise a privacy coin called Monero, but researchers have remained sceptical. Shi et al 2024, have suggested a possible vulnerability with privacy coins that shows possible routes to revealing the identity of beneficial owners. *Chainanalysis* and *Elliptic* have introduced some private sector support to investigators mixing user analytics with platform telemetry, but these remain limited.

Unanswered questions in this area include:

- What technical, procedural, and organisational vectors have been used in successful deanonymisations of privacy coins to date?
- Which combinations of vectors maximise probability of attribution under real-world constraints (legal, resource, time)?
- How do ecosystem features create choke points that investigators can exploit?

- What are the governance, ethical, and oversight implications of scaling such methods?

Example approaches:

Design and empirically ground an optimised, management-oriented framework for targeting privacy-oriented coins and tokens that improves the IC's investigations in these digital data threats.

This could be achieved by:

- Cataloguing and analysing all known cases of successful or partial deanonymisation of privacy coins and tokens.
- Identifying and testing high-yield combinations of exploit vectors (technical, procedural, organisational).
- Producing an operational playbook that is – through focus groups, interviews and crowdsourcing - co-designed with practitioners and which foregrounds the opportunity and risks of these approaches.
- Mapping the privacy-crypto ecosystem—the features of these protocols, user and chain custodian attributes, user dynamics, linkages to dark-web users, forums, platforms—and to provide quality visual analytics.

Topic 30 - Bayesian calibration and inference for agent-based models of cybercrime ecosystems

Key words:
Agent-Based Modelling (ABM), Bayesian inference, simulation-based calibration, cybercrime, complex systems, likelihood-free inference, neural density estimation, uncertainty quantification.

Research topic description, including problem statement:
Cybercrime represents a complex adaptive ecosystem composed of heterogeneous actors -offenders, defenders, intermediaries, and infrastructures - interacting across digital, economic, and social domains. These interactions generate emergent systemic behaviours such as ransomware market evolution, botnet coordination, and adaptive defender responses.

Agent-Based Modelling (ABM) offers a powerful framework for representing these interactions by simulating thousands of adaptive agents, which then generate emergent criminal dynamics. However, despite ABMs' potential for strategic foresight, their adoption in criminology and cybersecurity remains limited by a **key mathematical challenge**: **how to rigorously calibrate and infer model parameters from sparse and noisy empirical data**.

Recent breakthroughs in **Bayesian simulation-based inference (SBI)** - particularly **black-box and neural approximate Bayesian computation** developed by Farmer et al. (2024) -provide a new path forward. These methods use **neural posterior estimation** and **density ratio estimation** to infer posterior distributions directly from simulated data, enabling fast and accurate calibration of models even when likelihoods are intractable.

Each agent subsystem operates on different temporal and spatial scales, requiring scalable architectures capable of running millions of interdependent agents with asynchronous events and stochastic decision rules. Designing and implementing such a simulation demands effective application of advanced computational and data engineering methods. The challenge lies not only in building a computationally tractable model, but also in ensuring that it remains interpretable, reproducible, and adaptable as new intelligence and threat data become available.

Applying these methods to cybercrime ABMs represents a novel mathematical and computational frontier. It will require developing **Bayesian frameworks** capable of handling multi-level uncertainty (behavioural, structural, and observational) and defining **summary statistics** that capture emergent cyber

ecosystem properties (e.g., attack frequency distributions, market turnover, trust network resilience).

Problem Statement - How can advanced Bayesian inference methods be applied to calibrate agent-based models of cybercrime ecosystems, allowing quantitative validation, uncertainty quantification, and improved predictive capacity for complex, adaptive cyber-criminal systems?

Example approaches:

This project may include the following methodological innovations:

- **Bayesian neural posterior estimation for cybercrime ABMs**: Implement neural density estimation to infer posterior distributions of behavioural and structural parameters from synthetic and real-world cyber incident data.
- **Likelihood-free model calibration**: Extend Doyne Farmer's "black-box Bayesian inference" approach to criminological ABMs with heterogeneous, boundedly rational agents and discrete event dynamics.
- **Cybercrime Ecosystem Modelling**: Extend the agent-based model completed by Huang *et. Al.* to fully encapsulate the cybercrime economy and apply codified behaviours and dynamics to the agents.
- **Hierarchical Bayesian frameworks:** Integrate multi-level data sources (case intelligence, dark web markets, attack telemetry) within a unified probabilistic model to reconcile micro-level agent behaviour with macro-level emergent outcomes.
- **Uncertainty and sensitivity analysis**: Quantify how uncertainty in behavioural rules or data propagates to emergent system dynamics and predictive performance.
- **Validation through synthetic data experiments:** Compare model forecasts with historical cybercrime market evolutions (e.g., ransomware economies) to assess out-of-sample predictive validity.

References:

- Agent-Based Modeling in Criminology, Annu. Rev. Criminol. 2025. 8:75–95, Birks, D; Groff, E; Malleson, N.
- Agent-based modeling in economics and finance: Past, present, and future, *Journal of Economic Literature,* 2025, Axtell, RL; Farmer, D.
- Forecasting Macroeconomic Dynamics using a Calibrated Data-Driven Agent-based Model, M Pangallo, F Lafond, JD Farmer, S Wiese – 2024
- A survey of agent-based modeling for cybersecurity. *Human Factors in Cybersecurity*. 2024. Vestad A, Yang B.
- Systematically understanding the cyber attack business: A survey. 2018. *ACM Computing Surveys (CSUR)*, *51*(4), pp.1-36, Huang, K., Siegel, M. and Madnick, S.

Topic 31 - Machine learning-based restoration of degraded speaker audio

Key words:
Speech enhancement, audio source separation, speech synthesis, intelligence, surveillance, data science, machine learning.

Research topic description, including problem statement:
Many teams working across intelligence and law enforcement encounter 'unclean' audio in which the speech of interest is very difficult to discern and transcribe, resulting in sparser intelligence, frustrated operations and under-exploited data.

While current machine learning-based methods for removing noise from unclean recordings of speech [1][2] perform well in scenarios where the sound of a single speaker is masked to some extent by environmental noise, they often fail in cases where the speaker of interest is faint and/or distorted. Such tasks become additionally complicated when multiple speakers are talking simultaneously, requiring additional processing [3] that risks further degrading the speech of interest. Existing open-source, synthesis-based approaches to the restoration of degraded speaker audio [4][5] show promise but do not yet restore the speech to the extent that it is reliably intelligible. These shortcomings exist in spite of an abundance of open-source clean and correlated noisy speech data [6].

A research project on this topic would aim to:

- Thoroughly assess the current technological landscape for speech enhancement and restoration.
- Determine and implement necessary improvements and adaptations to the above described approaches such that they more reliably result in coherent speaker audio. This stage would likely include re-training and fine-tuning existing models on bespoke data, and making modifications to existing machine learning architectures.
- Design, engineer and test new components to replace existing underperforming ones. These would target tasks like audio source separation, noise removal and speech synthesis.
- Consolidate the resulting models, architectures and components into a suite of tools for speech audio restoration.

Example approaches:

- Undertaking a comprehensive review of the current state of the art approaches to speech enhancement and restoration, including real-time approaches.
- Testing any approaches not already known to the advising agency on real-world data.
- Devising novel strategies for simulating degradations of audio
- Creating new datasets that more accurately reflect the speakers and degradations commonly found in the targeted scenarios (for example, artificially degrading an existing clean speech corpus [6] and combining it with bespoke noise data).
- Retraining and fine-tuning models in [1], [3], [4], [5] and other approaches found during the review, on speech and noise audio more closely correlated to the target use-cases.
- Design and implementation of novel approaches to speech audio enhancement and restoration; devising novel strategies for quality testing.
- Building new pipelines combining these new datasets, models and components.

References:

- [1] Defossez, A. et al, 'Real Time Speech Enhancement in the Waveform Domain', Interspeech 2020 paper and Python library. https://doi.org/10.48550/arXiv.2006.12847.
- [2] Sainsburg, T. et al, 'Noisereduce: Domain General Noise Reduction for Time Series Signals', Python library. https://doi.org/10.48550/arXiv.2412.17851.
- [3] Nachmani, E. et al, 'Voice Separation with an Unknown Number of Multiple Speakers', ICML 2020 paper and Python library. https://doi.org/10.48550/arXiv.2003.01531.
- [4] Liu, H. et al, 'VoiceFixer: Toward General Speech Restoration with Neural Vocoder', Python library. https://doi.org/10.48550/arXiv.2109.13731.
- [5] Kirdey, S., 'VoiceRestore: Flow-Matching Transformers for Speech Recording Quality Restoration', Python library. https://doi.org/10.48550/arXiv.2501.00794.
- [6] Dubey, H. et al, 'ICASSP 2023 Deep Noise Suppression Challenge', dataset. https://github.com/microsoft/DNS-Challenge.

Topic 32 - Bio-inspired molecular sensors for adaptive computing and environmental intelligence

Key words:
Molecular Sensing, Synthetic Biology, Biomolecular Computing, DNA/RNA Logic, Chemical Reaction Networks, Adaptive Systems, Biosensor Interfaces, Low-Power Computing.

Research topic description, including problem statement:
Biological systems have evolved remarkable capabilities for sensing, processing and responding to complex environmental signals. From molecular recognition by nucleic acids to the self-regulating feedback of metabolic networks, biology offers rich examples of computation without silicon. Advances in molecular biology, synthetic chemistry and bioengineering now make it feasible to design molecular sensors that also compute; systems able to detect signals, process information and trigger responses autonomously.

We invite proposals to investigate bio-inspired molecular sensors, integrating sensing and computation at the molecular or cellular scale. The goal is to explore how these systems can enable adaptive, low-power intelligence in settings where traditional electronics cannot easily function, such as inside living systems, in extreme environments or in highly miniaturised platforms.

Of particular interest are systems that:

- Exploit DNA, RNA or protein logic circuits to perform computation on environmental or biological inputs.
- Combine molecular sensing and decision-making, enabling autonomous activation or suppression of downstream responses.
- Operate in challenging or resource-limited environments, where conventional sensors are unsuitable.
- Provide new routes to biological-electronic interfaces, allowing molecular information to be captured and acted upon in real time.

Example approaches:
Proposals may take experimental, simulation-based or hybrid approaches. Possible directions include:

- **Molecular Logic and Computation:** Design and characterise molecular circuits using DNA strand displacement, riboswitches, enzymatic networks or similar mechanisms, which perform logic or classification tasks in response to chemical stimuli.

- **Chemical Reaction Network Modelling:** Use CRN frameworks to model molecular computation and assess the robustness, scalability and energy efficiency of different network topologies.
- **Biohybrid Sensor Interfaces:** Integrate molecular sensors with electronic, optical or microfluidic platforms to achieve reliable signal transduction and data readout.
- **Synthetic Biology for Sensing:** Engineer living or cell-free systems to detect multiple analytes and perform programmable responses. Explore how gene circuits or metabolic pathways can implement logic gates, memory or feedback control.
- **Assurance and Verification:** Develop methods to verify, calibrate and stabilise molecular sensing systems, ensuring repeatability, robustness and security in operational environments.
- **Synthetic Cells and Partitions**: Investigating physical partitions in a functional network that require transport control mechanisms that manage/coordinate system behaviour.

Topic 33 - Mapping the transnational child sexual offending ecosystem

Key words:
National Crime Agency (NCA)
Child Sexual Abuse and Exploitation (CSAE)
Transnational Child Sex Offender (TCSO)
Online Child Sexual Exploitation (OCSE)
Contact Child Sexual Abuse (CCSA)
Child Sexual Abuse Material (CSAM)
Sexual Exploitation of Children Travel and Tourism (SECTT)

Research topic description, including problem statement:

Please be aware that this is a sensitive topic involving discussions related to child sexual abuse, which may be distressing for some individuals; therefore, careful consideration should be given before engaging with this topic. We will ensure that appropriate support is identified and made available before proceeding with any related work.

A global study on sexual exploitation of children in the context of travel and tourism (SECTT) concluded that increased global tourism and greater information / mobile technology access have escalated risk in every country (expat.org.uk). The same report emphasises that transnational child sex offenders exploit situational vulnerabilities such as weak child protection in destination countries, inadequate detection, and mobility of offenders. Another report notes that the scale of transnational child sexual abuse is poorly known, but conservative estimates place the number of under 18 victims at 1–2 million per year in transnational offending contexts (Crimes without borders, 2024). The number of undetected / unreported offending is likely very large, given limits of international information sharing, victim under-reporting, corruption in destination countries, and a lack of standardised data collection. These figures support the assertion that transnational child sexual offending is a major global risk.

Transnational child sex offenders (TCSOs) present a profound and persistent threat to the safety and well-being of children worldwide. These offenders exploit the increasing ease of global travel, international connectively and the disparities in child protection frameworks across jurisdictions. Their offending often crosses borders, not just physically but digitally and legally, making detection and prosecution highly challenging. As a result, this area of offending remains significantly under-researched and poorly understood compared to domestic forms of child sexual abuse.

This research proposal seeks to address critical gaps in the academic and policy understanding of transnational child sex offenders (TCSOs), through mapping and understanding of offender typologies, contextual risk factors, and systematic weaknesses, with the aim of supporting a more coherent global response. Ultimately this will inform global efforts to identify, disrupt, and prevent the sexual exploitation and abuse of children by transnational child sex offenders (TCSOs), ensuring the vulnerable receive stronger protection and offenders face consistent accountability across borders.

The opportunities for exploration and research are fluid, to promote the incorporation of researcher skills and experience. We are open to innovative approaches and ideas which may support the national and wider foreign law enforcement community in further understanding of this threat area.

Example approaches:

- Review differences in national legislation to identify best practices and gaps in international cooperation and coordination.
- Combining international multi-disciplinary understanding to generate a holistic understanding of the threat.
- Development of a risk assessment that considers areas such as socio-economics, cultural, and governance to identify high risk regions or travel patterns of offenders.
- Review of how international organisations, law enforcement, NGOs, and the private sector collaborate, or fail to collaborate in addressing the TCSO risk.

Topic 34 - The psychology of influence: effective persuasion in the cybercrime ecosystem

Key words:
Offensive cyber; online behaviour; persuasion psychology; social psychology; online influence.

Research topic description, including problem statement:
There is a growing literature supporting the efficacy of influence strategies in the online environment (Costello *et al*., 2024; Simchon *et al.*, 2024). More recently, academic interest has centred on how large-scale personalised persuasion can be achieved based on psychological and environmental factors (Hackenberg *et al*., 2025; Matz *et al*., 2024). The proposed project draws on this evidence base connecting the psychology of persuasion with advances in large language models (LLMs) to address the problem statement, "What evidence-based persuasion and influence techniques are effective to shape behaviour in a cybercrime ecosystem?" Combining this knowledge, this project aims to proactively influence and achieve behaviour change within the cybercrime ecosystem. This is a shift from traditional cybercrime strategies that prioritise defensive systems. Rather the proposal seeks to develop and optimise scalable offensive approaches to provide disruption opportunities, shape disengagement and proactively discourage cybercrime.

Example approaches:
- Developing and testing models using persuasive dialogue interventions powered by LLMs.
- Explore the efficacy of using Artificial Intelligence (AI) to generate persuasive content based on psychological and linguistic understandings of a cybercrime environment.
- Develop a framework to test and examine the efficacy of persuasion strategies in the cybercrime ecosystem through linguistic and psychological insights.
- Apply knowledge of hacker communities (or malicious cyber actors) to understand narrative discourse to inform behaviour change.
- Optimise the scale, speed and personalisation of proactive online influence strategies.
- Identify cybercrime populations most vulnerable to behaviour change and influence to then develop targeted interventions for disengagement.

References:

- Costello, T. H., Pennycook, G., & Rand, D. G. (2024). Durably reducing conspiracy beliefs through dialogues with AI. *Science*, *385*(6714), eadq1814. DOI: 10.1126/science.adq1814
- Hackenburg, K., Ibrahim, L., Tappin, B. M., & Tsakiris, M. (2025). Comparing the persuasiveness of role-playing large language models and human experts on polarized US political issues. *AI & SOCIETY*, 1-11. https://doi.org/10.1007/s00146-025-02464-x
- Matz, S. C., Teeny, J. D., Vaid, S. S., Peters, H., Harari, G. M., & Cerf, M. (2024). The potential of generative AI for personalized persuasion at scale. *Scientific Reports*, *14*(1), 4692. https://doi.org/10.1038/s41598-024-53755-0
- Simchon, A., Edwards, M., & Lewandowsky, S. (2024). The persuasive effects of political microtargeting in the age of generative artificial intelligence. *PNAS nexus*, *3*(2), pgae035. https://doi.org/10.1093/pnasnexus/pgae035.

Topic 35 - The impact of artificial intelligence and machine learning on chemical and biological counter-measures

Key words:
Artificial intelligence, drug design, pharmacology, machine learning, neural networks, algorithm, MegaSyn, BioNavi, Chemistry42, proteomics, computational biology, synthetic biology, chemical weapons, biological weapons.

Research topic description, including problem statement:
Artificial intelligence (AI) enabled tools are expanding the scope of chemical and biological sciences.

Previously unknown molecules and organisms are now being discovered and previously unreachable molecules are becoming more accessible. AI enabled tools are being deployed in the pharmaceutical industry, biotechnology and genetic engineering, consumer product manufacturing (cosmetics, avoidance of animal testing and to reduce environmental impacts), and in agriculture (biodegradation and reducing toxicity to non-target species). This broad-ranging scientific trend may also be used to design or produce new chemical and biological structures similar or superior to known chemical and biological warfare (CBW) agents. The potential capacity for rapid growth of available CBW threats with enhanced or comparable lethality to presently known toxic agents could potentially overwhelm international arms controls and countermeasure capability and will require the proactive development of new surveillance methods and novel detection, identification and mitigation systems.
Applicants should approach the topic with intent of undertaking a literature review and feasibility analysis of predictive AI algorithm applications and trends with respect to potential impacts on chemical and biological warfare controls.

Example approaches:
Research proposals could approach this issue from a variety of disciplines, or as a cross-disciplinary effort. The problem touches on aspects of chemistry, biotechnology, synthetic biology, computer/software engineering, neural networks and machine learning (ML), applied science, innovation policy, and pharmacology. Proposals may consider ways to monitor and mitigate threats of generatively designed agents using:

- machine learning models that use publicly available datasets and open-source generative software
- additional machine learning tools to model parameters such as environmental and metabolic stability
- retrosynthesis tools (commercially available or open-source)
- identification of suitable “chemistry/biology starting points”.

References:

- de Lima RC, Sinclair L, Megger R, Maciel MAG, Vasconcelos PFDC, Quaresma JAS. Artificial intelligence challenges in the face of biological threats: emerging catastrophic risks for public health. Front Artif Intell. 2024 May 10;7:1382356. https://doi.org/10.3389/frai.2024.1382356.

Topic 36 - Atomic nuclear and optical clock integration

Key Words:
Quantum Sensor; Integrated Photonics, Atomic Sensors; Ion; Nuclear/Atomic Clock, Optical Clock.

Research Topic Description, including Problem Statement:
Optical clocks can outperform traditional microwave clocks by factors of 100 – 1000 in stability and have become some of the most precise measurement devices ever built. However, current precision optical clocks are mostly laboratory-sized. While recent work by multiple groups around the world attempts to reduce the size of fieldable systems, the concepts being pursued are still trailer or full-instrument rack in scale, at best. Significant miniaturization is necessary to achieve scalable, portable devices needed for these applications. Recent demonstrations have shown that ion optical clocks are particularly well suited to an integrated platform. Recent advances in research and development of nuclear based timekeeping devices have also sparked interest in new applications of these types of clocks. Work related to this new technology is encouraged.

Example Approaches:
Research for this topic may include a variety of methods to demonstrate a path to a fully integrated clock.

Topic 37 - Quantum engineering for quantum sensors

Key Words:
Quantum, Quantum Engineering, Quantum Sensors, Atomic Sensors, Machine Learning, Control Theory, Quantum Control, Signal Processing, Enabling Technology for Quantum Sensors, Magnetometer, Gyroscope, Accelerometer, Gravimeter, Atomic Clock, Atom Interferometer, NV Diamond.

Research topic description, including problem statement:
This topic is about using quantum engineering to make quantum sensors easier to build and operate, both in the laboratory and in the field. Quantum sensors are devices that encode a physical quantity into a few quantum states of the system- for example, atomic magnetometers, atom interferometer gravimeters, atomic clocks, NVD magnetometers, and so on.

Quantum sensors may optionally utilize non-classical states to increase their performance. As quantum sensors become more sensitive and accurate, a key remaining challenge is to make them more practical outside of the laboratory. They need to be easy to operate, fast to turn on, robust against vibration and thermal changes, small and low power. The emerging field of quantum engineering can address these problems by applying standard and new engineering techniques to quantum devices.

Example approaches:
Example approaches will depend on the maturity of the quantum sensor and its intended application environment.

Some interesting directions include (but are not limited to) using machine learning techniques to simplify the user experience, using quantum and/or classical control techniques to increase robustness against noise, employing digital signal processing algorithms to increase sensor speed or improve accuracy, and applying advanced packaging techniques to reduce sensor size. These techniques may also be used to improve the performance of enabling technologies for the quantum sensor, such as lasers, photonic integrated circuits (PICs) or photon detectors, but the proposal should then include the use of these enabling technologies in an actual quantum sensor. Proposals may include work on theory, modelling or algorithms, but must apply these to a quantum sensor in the lab during the first year of the effort.