Research topics 2023

Topic 1	**The psychology of intuition the implications of creativity and cognitive bias for the security community**
Topic 2	**Protect individuals and our workspaces from acoustic compromise, through the identification of threats and countermeasures**
Topic 3	**Practical applications for private information retrieval with big data**
Topic 4	**Secure hardware assurance through modelling and machine learning**
Topic 5	**To what extent can the RF signature of a city be detected and modelled?**
Topic 6	**Flapping wing Micro Aerial Vehicles (MAVs) for remote sensing**
Topic 7	**Sensor counter-deception**
Topic 8	**Methods for high-throughput energetic characterisation**
Topic 9	**Towards Antifragility**
Topic 10	**Finding agency in sensory data**
Topic 11	**Innovative antennas for space platforms**
Topic 12	**People counting in secure environments**
Topic 13	**Protocol-agnostic device identification and authentication in smart cities**
Topic 14	**Development of techniques to assess data aggregation**
Topic 15	**Review of advanced sensor technologies**
Topic 16	**Enhance Raman microscopy identification of biological and chemical materials on solid samples**
Topic 17	**Non-canonical protein translation and expression processes, synthetic biology and biosecurity**
Topic 18	**Modelling of chemical plumes in urban environments**
Topic 19	**Effect of aerosol particle morphology on reaction dynamics**
Topic 20	**Emerging application for superconducting electronics**
Topic 21	**Enabling components of human augmentation**

Topic 1
The psychology of intuition the implications of creativity and cognitive bias for the security community

Unclassified key words: game theory, search bias, improving decision making, human factors and security.

Unclassified research topic description, including problem statement:
Creative and innovative thinkers provide huge benefit to the security sector and these characteristics are highly beneficial to analysts, engineers and scientists. These individuals can identify alternative solutions to reoccurring problems and adapt to new novel situations, giving an organization huge advantages. Furthermore these individuals have a heightened sense of intuition compared to others. However, over a period of time, this creative, novel thinking can be affected by organizational cultures and group think behaviour.

Degradation of novel thinking or indeed cognitive bias that may occur from conducting repetitive tasks and this is of particular risk to those who conduct routine searches and inspections to certify an environment is secure and safe. Currently end users have some technology to assist with certifying an environment is safe, but do end users become biased over time in the manner in which they use/ do not use the technology provided correctly. To some degree an element of intuition can often lead highly skilled individuals to try something new, whereas others do not demonstrate this flare for creativity. In the latter example, this can lead to both false positives and false negatives. In other words their decision making becomes biased over time, leading to risks for the organization.

Due to the repetitive nature of the tasks do these individuals become lose their edge due to task fatigue or peripheral biases that render them unable to apply novel thinking. Are some individuals prone to search bias than others, if so why? Could the application of game theory provide any insight into this? Is it possible to develop a psychometric tool that could assist with the nurturing of creativity?

How can differences between trained individuals be measured and what technologies could be used to prompt, focus, or even train more use of intuition/ creativity to solve a problem. The relationship between eye movements and eye tracking can demonstrate bias in an independent way. The use of augmented reality may be beneficial both during training and on task to provide prompts for the end user. How could technology improve the decision-making during searches and prevent biased thinking.

This topic will require a proposal that is a combination of applied psychology, together with some form of engineering innovation. It will also need to present new innovative approaches that have not already been explored by research for the benefit of those who conduct searches and inspections.

Unclassified example approaches:

Eye movement research is a field of psychology that has shown how eye movements and tracking eye movements, directly influenced our attention and understanding of the word around us.

Various psychological theories have shown how task fatigue can lead to a degradation in performance.

Technologies such as augmented reality and immersive reality have been shown to be beneficial for commercial pilots to learn in a simulated environment, how to make critical decisions when faced with a real-world event.

Topic 2
Protect individuals and our workspaces from acoustic compromise, through the identification of threats and countermeasures

Unclassified key words: acoustics, ultrasound, infrasound, directional speakers, acoustic disruption, 'MSVE', metamaterials.

Unclassified research topic description, including problem statement:
There are three areas of acoustic compromise that we wish to explore. The first is related to speech, the second is related to the field of infrasound disruption, and the third is related to ultrasound egress.

With regards to speech, there are three key elements of interest. The first is to assure privacy of speech between individuals. The second is ensuring speech can be safely contained in a given space. The third is ensuring that you can protect an eavesdropping attack through egress of audio on other carriers. Each of these elements are important for the individual, the information content, and the organization in which they work.

With regards to infrasound, developing detection and countermeasures to radiated harmful effects. For ultrasound, certain levels can also be harmful to occupants, but they can also provide intelligence egress utilizing third party methods such as mobile phone signals or other methods etc.

We would like to explore the science of acoustics and if there are any opportunities or insights that can identify threats, provide closer attention for future work; or immediate opportunities to develop bespoke counter measures to protect UK assets.

In addition, we would like to understand and protect remote workers; offer best practice for protection of speech and any innovation that we could develop further. For example, particular interest is to examine the acoustic integrity of headsets that are routinely worn both at home and in office environments, which have now become commonplace during the pandemic during online meetings. Another measure is to examine how spaces could be better protected to ensure that speech is safely contained in an area (MSVE), either a designated purpose-built environment; a rapid deployment of a structure; or other practical counter measures. Similarly, protection from ultrasound and infrasound.

The identification of particular security problems and proposed countermeasures is of primary interest for both individuals and workspaces.

An ideal deliverable would be the ability to acoustically model 'a design' of environments with differing materials, prior to construction. The model would determine and guide material or design choices to achieve attenuation necessary to provide a MSVE requirement at an early stage.

Metamaterials as an emerging technology in production methodology, could these be engineered to offer retrospective installation into a building fabric for a cost-effective audio suppression or directional control over acoustical waves?

We appreciate that this is a broad topic covering many aspects of acoustic research, therefore, we would welcome any expressions of interest in all or part of the above.

Unclassified example approaches:

- Commercial company (USA) Holosonics produce directional speakers that could have a security use.
- Government sponsors have used disruptive technologies in the acoustic ranges, specifically sub aural, potential news articles report these being used, plus examples of use in crowd control. Directional speakers.

Glossary:

MSVE – Minimum Safe Vocal Effort. A level of speech (dB) in an environment that cannot be overheard (by third parties).

Topic 3
Practical applications for private information retrieval with big data

Unclassified key words: encryption, data security, big data, information, cryptography.

Unclassified research topic description, including problem statement:
The use of big data is emerging in almost every sector; allowing commercial organisations greater insight into their customers buying habits, health organisations improved understandings of patients and drug use (e.g., antibiotic resistance) and Governments using big data in wide ranging application from vehicle traffic flow to biometrics at borders.

Data is often held by in servers by potentially untrusted sources. For privacy reasons, cryptographic techniques are typically used to protect the contents of the data from the owners/operators of the data storage systems, and in accessing the data a key or selector needs to be provided which has to identify the contents of the data being accessed.

This causes issues to the IC when Lawful Intercept has been granted by a legal warrant when investigating criminal activity for example, that the specific data required to be accessed is inadvertently revealed to both the data owner and the operator of the data storage systems.

One very way simple way to for the IC to achieve anonymity of data being investigated is to take the entire contents of the database, that way the owner of the data cannot determine which is of interest. This is technically quite straightforward and will likely be considered by a court to be necessary and proportionate for small datasets, but within large datasets this becomes impractical and raises questions about proportionality of the approach and collateral intrusion, whereby a court may refuse a legal warrant.

The focus of this research topic is to gain knowledge and develop methodologies to efficiently probe big datasets, identify and acquire the specific data of interest without inadvertently notifying the data owner and the operator of the data storage systems.

Unclassified example approaches:

Private Information Retrieval (PIR) allows a client to download an element (e.g., movie, friend record) from a database held by an untrusted server (e.g., streaming service, social network) without revealing to the server which element was downloaded. While powerful, PIR is very expensive—and unfortunately this expense is fundamental: PIR schemes force the server to operate on all elements in the database to answer a single query. This methodology may inspire new techniques that are less expensive.

Information theoretic approaches such as distributing the database between multiple servers can help solve this problem however a challenge remains to ensure non collusion between these databases which could reveal which items were accessed.

Topic 4
Secure hardware assurance through modelling and machine learning

Unclassified key words: machine learning, artificial intelligence, modelling, component recognition, electronics, hardware assurance, printed circuit board, automation, automated testing.

Unclassified research topic description, including problem statement:
With the global diversity of electronic components and printed circuit board (PCB) manufacture and assembly supply chains, there is limited confidence that delivered assembled PCBs have been manufactured and assembled as designed without error. PCB testing is therefore required after manufacturing to verify the PCB functions as required and does not have component(s) missing, wrong component(s) added, component(s) that have failed or will likely fail or components that are counterfeit. In the current climate of a shortage of semiconductor die, the potential of counterfeit components appearing in critical PCBs is increasing. Testing is a trade-off of how extensively to test the product versus time and cost to perform the testing. Depending on the final PCB application the effort to assure the hardware in both secure and insecure environments can be considerable.

Assuring a PCB with components in place is a difficult and manually time-consuming task to perform that does not scale with increasing PCB complexity. Even when original design data or a golden reference PCB are available, generating in-circuit tests and interpreting the results is currently a manually intensive task that relies on engineering best practices and experience to undertake and optimize.

By utilizing parallel world developments in Machine Learning, or other modelling approaches, complex PCBs can be assured against and compared to their specifications. This topic focuses on Machine Learning and modelling methodologies as it is believed this will be key to automating assurance, prior knowledge of PCB development/manufacture is not essential.

Unclassified example approaches:
Possible approach:

- Using high resolution images of PCBs, coupled with component recognition technology and Machine Learning to automate modelling of complex PCBs and their characteristics.
- Model PCBs with components to characterise the resultant measurement values when individual components are interconnected with different values and configurations. Equivalent to measuring the resultant resistance/capacitance/inductance of a PCB net with multiple components attached.
- Use modelling to infer the reverse, decomposing a resultant measurement value into individual component values.
- Develop a model of a PCB optimise the number of measurements required to fully test cover a PCB.
- Develop and build a prediction model to give confidence in assurance level of the PCB.

Topic 5
To what extent can the RF signature of a city be detected and modelled?

Unclassified key words: smart city, RF, modelling, monitoring.

Unclassified research topic description, including problem statement:
Problem statement: as smart devices and vehicles increase within large urban environments; the overall RF signature of a city increases. Signals can originate from the ground, within buildings or from rooftops. With the related rise of smart cities and digital twins, to what extent can the RF signature of a city be detected, modelled, and incorporated into existing smart city models? Can a live service be created to anonymously monitor RF signatures in real-time?

Description: “Big data” is growing and is increasingly used by more industries. With the wealth of open-source and commercial-off-the-shelf (COTS) hardware, software, and database systems, how can we best use the available systems that detect RF signatures to model hotspots, dark spots, anomalies or faults within cities? Such data can be of use by autonomous vehicle manufacturers to improve their modelling, such as capability to handle dark spots in a built-up environment, or to predict where there may be more accidents caused by lack of constant contact to an online server or car-to-car communication.

If there is no existing method of detecting RF in such a manner, can one be created? How would such a system look? What would be the necessary technical and ethical considerations when collecting such data? How could it be stored, labelled or included within existing smart city datasets?

Unclassified example approaches:
- Literature/existing system review
- Functionality review
- Gaps
- Suggested improvements
- Link in with existing smart city models
- Anomaly/fault detection
- Development of an RF detection system.

Topic 6
Flapping wing Micro Aerial Vehicles (MAVs) for remote sensing

Unclassified key words: soft robotics, aerospace engineering, flapping wing vehicles, nano uncrewed aerial system, micro aerial vehicle.

Unclassified research topic description, including problem statement:
Flapping wing Micro Aerial Vehicles (MAVs) – uncrewed aerial vehicles inspired by birds, bats or insects that use flapping propulsion – have not yet reached their potential as remote sensing platforms. They have potential to be as small as insects, enter confined or covered spaces, perch and loiter, display high manoeuvrability and stealth, achieve better energy efficiency, mimic insects with much greater fidelity, be carried by people or other aerial vehicles, safely fly overhead in public spaces, and provide sufficient payload capacity for multiple miniaturised sensors. This research topic aims to combine several basic research challenges to move towards production of insect-sized, flapping-wing MAVs capable of efficient, sustained, controlled and untethered flight outdoors. Challenges include:

- designs inspired by insect dynamics and morphology
- development of soft, flexible artificial muscles that are more responsive, compact and lightweight than traditional actuators
- computational modelling of fluid-structure interaction and stimuli-responsive materials
- test, validation and calibration of modelling using 3D-printed prototypes
- integration of miniaturised batteries, electronics, control, communications and sensors.

Unclassified example approaches:
Example approaches include those that seek to:

- produce designs that draw on inspiration from the dynamics and morphology of insects using motion tracking environments and facilities for high-resolution imaging
- develop controllable, soft actuators using material characterisation and computational modelling expertise and facilities
- test, validate and calibrate modelling using 3D printing facilities, prototyping and testing facilities
- integrate state-of-the-art miniaturised components using electrical, mechanical and aerospace engineering expertise and facilities.

Topic 7
Sensor counter-deception

Unclassified key words: intelligence, surveillance and reconnaissance (ISR), sensing, situational awareness, deception, strategy, game theory, Bayesian inference.

Unclassified research topic description, including problem statement:
Military sensing is often complicated by the fact that an adversary's objective is in direct conflict with one's own. Adversaries will work hard to obscure their state and their intent, for example by hiding, manipulating their signature, or deploying decoys and countermeasures. This complicates inference and means any useful ISR picture compilation method must be robust to such tricksiness. Behaviour like this is not confined to a single domain or single sensor modality and techniques found in certain scenarios have analogues in others (e.g., radar jamming/optical dazzle). The IC is looking for methods of both quantifying the effect of deceptive behaviour on the ISR picture, and where possible acting to mitigate such an effect.

Unclassified example approaches:
Deception of sensing can take many forms and occur in many situations. We are interested in general aspects of the problem space such that we may draw conclusions and provide mitigations in multiple domains. We want research to build toward a mathematical description of how to counter types of behaviour designed to deceive sensors. This may begin from general-purpose human-centric theories of deception and specialise them toward sensing and inference, or it may build from models of sensors and target intent. Whichever way it goes, the research must develop a general mathematical framework characterising multiple and varying types of deception. These may encompass hiding, dazzling, decoying, mimicking, inventing real and fake targets, among many other examples. Solutions to single and overly specified problems are not of interest here.

We will not be overly prescriptive as regard solutions; all techniques are welcome. We are, however, looking for methods which can be engineered within future ISR and autonomous systems and will eventually deliver benefit to the intelligence community. Preference will therefore be given to research which shows strong potential for exploitation in this direction. Cross-disciplinary research is encouraged.

Current component methods of sensor counter deception research cover modelling of intent, efficient optimization, game theory, Bayesian inference, scalable inference on graphs, high-dimensional sampling methods. This list is neither complete nor prescriptive.

Topic 8
Methods for high-throughput energetic characterisation

Unclassified key words: energetic materials, analytical chemistry, automation, robotics, high-throughput screening, materials science, chemistry.

Unclassified research topic description, including problem statement:
Characterisation of energetic material stability, reactivity and energy content is often a slow process that requires relatively large quantities of material and meticulous manual preparation. Tests rely heavily on human skill and dexterity during the data acquisition stage, leaving them open to systematic, batch-to-batch and error-driven variation. They are also difficult to automate directly since these tests have been designed around humans, maximising simplicity, and safety for the user. In a future that utilises automated discovery and high throughput testing of functional materials, this would provide a bottleneck for rapid screening of new candidates. Therefore, new methods are sought that would accelerate this vital stage in the materials development pipeline. Human-led test methods would then be reserved for full characterisation of only those candidates of the highest potential to enable greater scrutiny and assurance of their characteristics.

Unclassified example approaches:
Development of new or enhanced analytical methods capable of linking molecular or material structure to stability, reactivity, or energetic material performance. These methods should be amenable to inline or higher-throughput analysis that would be suited to screening candidate functional materials.

Development of an automated system that incorporates existing technologies or processes in a more streamlined overall process that combines rapid characterization of potential energetic materials with their synthesis. This process should be compatible with greater automation and high-throughput analysis of candidate materials.

Topic 9
Towards Antifragility

Unclassified key words: antifragility, cyber security, resilience, self-healing systems.

Unclassified research topic description, including problem statement:
Cyber defence is currently based on resilience: matching known attacks with proven defences. Adaptation and improvement are only possible using human intervention to inject innovation after the fact.

The concept of Antifragility was suggested by Taleb (2012) [1]. This creates the possibility of using machine learning to create self-healing systems within a cycle of continual improvement. Antifragile cyber systems are therefore systems that are sufficiently resilient to survive preliminary attack, can learn from this experience, and can self-improve. In other words, antifragile systems gain in resilience the more that they are attacked. The technology for achieving this does not yet exist, however, recent encouraging developments in robotics could be used to make progress.

The main challenge is establishing an AI that has sufficient self-awareness to interpret the attack experience and innovate improved defensive measures to itself. Specifically, the AI will need:

- A model of self (potentially using machine theory of mind) to discriminate the effects of exogenous events from the effects of self-action
- Perception of malicious agency (ie the resolving the attacker as an exploiting/harmful agent using percepts gained through interpretation of sensory data)
- Formulation of attack defences (solving the correspondence problem [2]: transforming actions in the domain of the attacker to responses in the domain of the defender)
- Deploying effective defences that do not compromise system function or performance unduly
- Resisting deceptive and/or coercive attacking agents.

Detailed challenges include:

- Machine perception of behaviour – achieving high accuracy in noisy streaming sensory data
- Characterisation – representing the nature of cyberattack in a form that is machine actionable
- Machine innovation – this combines expert knowledge for attack analysis, intimate understanding of the system being defended, and the ability to predict the effect (and side-effects) of remedies before deployment
- Whole system perspective – self-remedies are not innovated in isolation; the system must be able to model effects beyond its own limits and avoid unintended consequences
- Demonstrate the antifragile property in a real system.

References:

[1] Nassim Nicholas Taleb (Author), *Antifragile: Things that Gain from Disorder*, Random House; Illustrated edition (27 Nov. 2012), ISBN-13: 978-1400067824.

[2] Nehaniv, C.L. & Dautenhahn, K., The Correspondence Problem in Social Learning:--What Does it Mean for Behaviors to Match Anyway, 2002, Procs of Perspectives on Imitation: from Cognitive Neuroscience to Social Science, http://hdl.handle.net/2299/1790.

Topic 10
Finding agency in sensory data

Unclassified key words: agency, agent-based systems, bio-inspired systems, complex systems, non-linear systems.

Unclassified research topic description, including problem statement:
The present-day era of cybersecurity is largely defined by defence from hostile code interventions (such as ransomware and viruses) and hostile intrusion through weak access controls. We believe that many present-day cyber-physical systems will evolve towards large scale, highly interdependent, collectives of agents having emergent properties. We therefore expect future cybersecurity challenges to evolve to include defence from malicious agency.

We believe that emergence is a consequence of interaction/interdependency between agents (cyber-physical components), and that the properties, although absent in the individuals, exists in the collective. These are complex systems.
The nature of emergence drives us towards the use of models of agency for the cybersecurity of collectives because of the symmetrical relationship between attacker and defender – we assert that future cyber conflict will partly lie in the emergent space of complex systems. Complex systems are nonlinear, emergent, with diverse internal components, use feedback mechanisms, are autonomous in behaviour, adaptive, and capable of learning. They use intensive internal communications to balance system cohesion with the forces of adaptability, and to work as a collective towards a common goal. They are unstable and may alternate unpredictably between seemingly random and stable patterns of behaviour.
This makes complex cyber-physical systems vulnerable to cyberattack in new ways, but we think the emergent properties are also a potential asset in responding to this threat - malicious agency could be countered by benevolent agency.

Unclassified example approaches:
Biology provides the following inspiration:

- Life-as-a-system inspires the engineering of technological systems – life has emergent properties and is increasingly being understood in terms of systems theory
- Classification of life systems (cladistics) inspires the characterisation of agency as traits (apomorphies) – this may be transferrable to machine learning applied to sensory data sets
- Life systems demonstrate complexity, and therefore provide worked examples suitable for informing engineering.

Possible approaches:

- Analysis of non-parsimonious decision trees using phylogenetic tree analysis techniques from evolutionary biology (cladistics) – does the digital shadow left by agency in sensory data correspond meaningfully to apomorphies and/or synapomorphies?
- Modelling the behaviour of cyber-physical systems as simple cybernetic regulatory systems – using systems theory to determine irregular behaviour indicative of malicious agency. Examples from nature are given by Camazine & Deneubourg (2003) [2]
- Modelling the behaviour of complex adaptive systems – perhaps with the "Revealed Dynamics Markov Model" (Bramson, 2019 [1] pp79-128).

Principal challenges:

- The appropriateness of techniques from evolutionary biology – determining when there is sufficient lack of parsimony for the required degrees of freedom and, when so, to extract meaningful characterisations of behaviour (apomorphies) from noisy data using techniques from biology
- Characterising behaviour and agency in systems – creating agent-based models that are similar to malicious agency so that detection in sensory data from the digital shadow can be demonstrated.
- Comparing evidence from digital shadows with putative behaviour models – bridging the gap between a sensory representation and a behavioural one. We also need to decide when a correspondence between a hypothesised agency and our model of that agency has occurred.
- Defining maliciousness – At some point, we will need to define what we mean by a "malicious agency". Karnouskos (2015) [3] discusses this in terms of the exploitation of one agent by another (this could be seen as the perversion or obstruction of the victim agent's mission goal by an attacking agent).

References:

[1] Ted Carmichael (Editor), Andrew J. Collins (Editor), Mirsad Hadžikadić (Editor), *Complex Adaptive Systems: Views from the Physical, Natural, and Social Sciences* (Understanding Complex Systems), Springer; 1st ed. 2019 edition (27 Jun. 2019), ISBN-13: 978-3030203078

[2] Scott Camazine (Author), Jean-Louis Deneubourg (Author), Nigel R. Franks (Author), *Self-Organization in Biological Systems: 38 (Princeton Studies in Complexity), Princeton University Press* (17 Sept. 2003), ISBN-13: 978-0691116242

[3] Stamatis Karnouskos, Chapter 6 - Industrial Agents Cybersecurity, Editor(s): Paulo Leitão, Stamatis Karnouskos, Industrial Agents, Morgan Kaufmann, 2015, Pages 109-120, ISBN 9780128003411, https://doi.org/10.1016/B978-0-12-800341-1.00006-1. (https://www.sciencedirect.com/science/article/pii/B9780128003411000061)

Topic 11
Innovative antennas for space platforms

Unclassified key words: antennas, cube satellites, direction-dependent modulation, inflatable antennas, plasma antenna, reconfigurable antennas.

Unclassified research topic description, including problem statement:
Space is an increasingly important domain for the UK as has been highlighted in the Integrated Review and the importance endorsed by publication of the UK Space Strategy. The Space sector is also changing rapidly with much more activity in the sector focusing on smaller platforms (CubeSats) that are cheaper to develop and launch through innovations such as rideshare arrangements. Although the CubeSat platform and associated electronic systems have developed rapidly and have been to a large extent commoditised one area that has not seen the same level of progress is CubeSat antenna technology.

User requirements often call for high gain, wide bandwidth and directionality but these are difficult to achieve when the host platform is relatively small and constrained, this is especially true in the <1GHz region, where the antenna size/weight is appreciable compared to the spacecraft platform itself. Similarly launch requirements often mean that the antenna must be stowed and compacted to fit into the available volume.

This research topic is to progress the state of the art of satellite antennas for small CubeSat applications. The goals will be to maximise gain and bandwidth by advanced materials and/or novel mechanical geometries. It is acknowledged that it is unlikely a single configuration will cover a very broad frequency range therefore the research topic may wish to focus on one or more of the sub frequency bands 100MHz to 1GHz, 1GHz to 3GHz, 3GHz to 6GHz, 6GHz to 18GHz where it is accepted that the potential solution may be different for each sub band.

Challenges include:

- Simultaneous constraints on electromagnetic, thermal and mechanical design goals, such as:
  - Limited choice of materials that will survive in Space.
  - Optimising RF performance operating near the link budget limit and the need for circular polarisation
  - Constrained spacecraft payload weight
  - Constrained spacecraft launch size
- Mutually exclusive design goals, such as:
  - Mechanical complexity of designs versus the reliability of deployment in the space environment
  - Antenna size/weight versus spacecraft stability (asymmetry of mass).

Assumptions that can be made:

- Deployment on a small CubeSat e.g., 3U or 6U spacecraft having stabilised attitude.
- The coexistence of other antennas (such as S or X band command and control)
- RF antennas operating in the 1 to 5 GHz spectrum with TX power of no more than +33dBm, but with scope for high gain in the ground station.

Unclassified example approaches:

The following potential approaches are suggested (but should not be taken as prerequisites or constraints):

- Direction-dependent modulation schemes and other novel superpositioning techniques
- Reconfigurable/tunable antenna designs
- Low loss lens antennas (artificial dielectrics, Fresnel/Zoned material lens, lightweight Luneburg lens)
- Low loss ceramic/dielectric resonator antenna designs, such as
  - Substrate Integrated Waveguide (SIW) antennas (planar waveguide antenna)
  - Polyrod arrays
- Novel use of smart materials, laminar materials and composites
- Solid-state plasma antennas (eg plasma silicon)
- Novel inflatable (precision reflector) designs for sub 2 GHz
- Origami and flexible substrate antenna designs for sub 2 GHz.

Topic 12
People counting in secure environments

Unclassified key words: building use, data fusion, distributed sensors, privacy-preserving counting.

Unclassified research topic description, including problem statement:
As the diversity and scope of Government premises increases, especially for unclassified work, there is an increasing need to understand the popularity and patterns of use of facilities without compromising the identity of the individuals using them. This is in addition to GDPR. Aims include increasing value for money in existing building operations (including energy management), targeting investment in facilities for best impact, improving physical security, making reasonable adjustments for the disabled, efficient improvement of lighting, ventilation, and other working conditions affecting wellbeing and effectiveness.

A distributed sensor array that detects the scale, intensity and distribution of human activity in a building is envisaged. The cost per sensor must be low.

Challenges include the sensor positioning problem (ie eliminating blind spots and achieving adequate coverage area).

Challenges include the sensor positioning problem (ie eliminating blind spots and achieving adequate coverage area).

Unclassified example approaches:
The following people counting techniques are suggested:

- Passive RADAR (e.g., using ambient Wi-Fi signals to resolve the number of individuals).
- Optical Flow imaging (i.e., motion only), possibly with ToF laser ranging.
- Low resolution far-IR thermal imaging (e.g., 8x8 thermopile array).
- Passive IR sensor arrays (for motion detection).
- IR/laser beam breaking at pinch-points, corridors, doorways, openings, etc.
- Under floor pressure mats.
- Carpet pile shading/markings imaging (i.e., transient imprint of footprints).
- Electrostatic field disturbance/coupling (deflection of a generated ES field because of people in proximity).
- Passive ultrasound sensing with direction finding (assumes movement of people's clothing as a source of ultrasound).
- Active ultrasound imaging (eg real time room-scale tomography at 40kHz).
- Infrasound analysis (determination of activity from infrasound production from doors, lifts, etc.).

Compound sensing using fusion techniques may improve accuracy and reliability.

Topic 13
Protocol-agnostic device identification and authentication in smart cities

Unclassified key words: complex systems, architecture, device discovery, smart cities, IoT, IIoT, cyber security, data verification, authentication, identification.

Unclassified research topic description, including problem statement:
Smart cities are physically distributed and typically uncontrolled environments within which a wide range of devices are deployed. To ensure the security of their environments, system integrators and maintainers of smart cities need to have comprehensive awareness of devices within their smart city networks, and confidence that those devices are not being impersonated. While some of this functionality may be provided by network protocols used in a smart city, the heterogeneity of current smart city networks does not present a clear mechanism for system-wide device identification and authentication.

This project would be expected to:
- Determine classes of devices and associated communications protocols likely to be used in a smart city. Explicate existing methods for device identification and authentication applicable to these device classes and protocols.
- Review both current and conceptual future flaws in the secure authentication of smart city devices. This would include techniques that allow for the impersonation of devices at the time of provisioning or at a later date due to a practical physical or online attack.
- Devise a device and communications protocol-independent architecture which facilitates the identification and secure authentication of all devices connected in a smart city environment.
- Deploy the architecture, using a variety of case study devices deployed in representative networks, within a laboratory environment to validate its effectiveness against the identified flaws.

Unclassified example approaches:
Suggested approaches would include:
- Literature review, vendor documentation analysis and open-source intelligence scan to determine:
  - The types of devices and communications protocols commonly used in smart cities.
  - Current methods for smart city device and network identification and authentication.
  - Current flaws in the secure authentication of smart city devices.
- Analysis and laboratory research to determine:
  - The validity of any published flaws and potential attacks on the identification and authentication of smart city devices.
  - A device and communications protocol-independent architecture which facilitates smart city device identification and secure authentication.
  - The validity of the architecture against identified attacks and flaws using a variety of case study devices deployed in representative networks.

Topic 14
Development of techniques to assess data aggregation

Unclassified key words: data aggregation, re-identification, de-anonymization.

Unclassified research topic description, including problem statement:
Problem statement: development of a methodology to enable identification and repeatable assessment of risks arising from the aggregation of data sets.

It is recognized that data aggregation arising from combinations of data sets can result in revealing or allowing the inference of information that is not contained in the aggregated data. For data that may be linked to an individual or groups of individuals, it is difficult to measure re-identification or de-anonymization risks that may arise in ways that are both general and meaningful. For data relating to physical assets it can be difficult to assess what can be inferred about the criticality or sensitivity of the assets and their associated infrastructure.

There have been several publicized examples of anonymized data being de-anonymized enabling the identification or re-identification of individuals and locations. At present there is no published guidance defining how to assess the potential consequences of data aggregation, nor are tools available that allow testing or formal evaluation of combined data sets prior to their publication or disclosure.

While there is some understanding of the issue in respect of personal and travel data, the concept is poorly understood with regards to asset data, particularly relating to infrastructure assets, where factors such proximity, interconnection, interdependence can create criticalities which may be of benefit to parties conducting hostile reconnaissance. A complicating factor with infrastructure data is the need to understand not only the geospatial relationships but also the significance of facilitating the disclosure or inference of links between sensitive or potentially sensitive physical assets/sites and the infrastructure that supports them.

Unclassified example approaches:
Examples of potential data aggregation threats include:

- Identity disclosure – associating individuals with specific records and/or locations which may arise from insufficient de-identification, re-identification by linking data from two or more sets, or from pseudonym reversal.
- Attribute disclosure – identifying an attribute in a dataset held by a specific individual, group of individuals, or by asset(s) with high probability, even if the data associated with the targeted entities are not identified.
- Inferential disclosure - making an inference about an individual, group of individuals, location(s) or asset(s) with high probability, even if the targeted entities were not in the dataset prior to de-identification/anonymization.

References:

https://doi.org/10.6028/NIST.SP.800-188.3pd

The latest draft of NIST SP 800-188 (3pd) - *De-Identifying Government Data Set* - provides some background to the issue and an extensive list of references. The proposed research would build upon this to develop methods and where practical tools to assist users to identify and address potential aggregation issues.

Topic 15
Review of advanced sensor technologies

Unclassified key words: sensors, emerging technologies.

Unclassified research topic description, including problem statement:
Problem statement: Scientific and engineering advances in areas such as quantum, photonics, machine learning and artificial intelligence are creating opportunities for the development of new types of sensors which may create as yet unquantified threats and opportunities for the security and intelligence communities.

Some of the advances referred to will arise from our greater understanding and application of new and emerging technologies, Others will arise from novel applications of known technologies particularly as a consequence of technical advance in say manufacturing techniques which allow minaturisation, improve reliability and or yields of specialist components or fabrications.

The proposed research should consider the technologies and innovations from two perspectives:

- Threat - Would the availability of a capability provided by the technology enable a hostile or malicious actor to bypass or undermine existing security measures?

And

- Opportunity - How might the capability be employed by the security and intelligence community to address limitations in existing measures or anebale the adoption of new/novel techniques.

Unclassified example approaches:
Use of quantum gravimetric sensing can enable the detection of buried concealed objects. From a counter terrorism perspective, the development of techniques based on this technology could be beneficial in the detection of improvised explosive devices, but this approach is also applicable to the detection of buried infrastructure (e.g. pipes, tunnels, underground buildings, etc.). It therefore might be used in a protective capacity to detect attempts to defeat physical security measures though underground or underwater activity. Unlike ground penetrating radar, the use of gravimetrics is a passive technology and thus a potentially interesting countermeasure.

Topic 16
Enhance Raman microscopy identification of biological and chemical materials on solid samples

Unclassified key words: raman microscopy, forensics, chemicals, biological materials.

Unclassified research topic description, including problem statement:
Methods for the non-destructive identification, characterization, and localization of biological and chemical materials on solid samples is lacking for forensic applications. While there are many methods available for the identification of biological and chemical substances on the surface of forensic samples, these methods typically destroy or leave a visible indication that the surface has been modified for analysis. This project involves expansion of current Raman microscopy methods used for the non-destructive identification of biological and chemical materials on the surface of forensics samples. A variety of laser sources will be utilized to identify and localize different types of biological materials, including proteins, nucleic acids and lipids, as well as chemical substances such as petroleum products, powder residues and other relevant materials on the surface of samples. The capability for the non-destructive analysis solid samples has wide applications in forensics.

Unclassified example approaches:
This position is to develop processes for Raman microscopy. Imaging of solid object prior to biological or chemical analysis allows focused analysis of high value items prior to any destructive analysis.

Raman microscopy systems have advanced in recent years and could be implemented in a variety of facilities.

Topic 17
Non-canonical protein translation and expression processes, synthetic biology and biosecurity

Unclassified key words: frameshift slippage, leaky translation, alternative splicing, entangled proteins, biosecurity, structure-to-function, protein expression.

Unclassified research topic description, including problem statement:
Viruses have provided the template for numerous natural non-canonical protein expression modalities to include alternative splicing, frameshift slippage, and overlapping genes. Current estimates indicate that more than 50% of viral genomes contain one or more overlapping genes. Recent discoveries have shown similar overlapping genes do exist in humans and eukaryotes but at a much lower occurrence, roughly between 1% to 26%. While viral genomes are smaller by multiple orders of magnitude compared to most living organisms, limiting the total length of potential nucleotides for encoding proteins, other facets related to protein structure, function, and expression are at play ranging from evolutionary driven replication efficiencies and community survival, all of which likely play a role in which organisms have adapted noncanonical protein translation.

Recent research has led to the development of computational tools and laboratory techniques for the rational engineering and expression of 'entangled proteins' in bacterial systems. This research has successfully demonstrated expression of overlapped genes and provided multiple examples of the biosecurity implications, especially from an evolutionary escape perspective, of such engineering practices. While successful, the current published approaches focused predominately on sequence alignment and gene overlap. The algorithms have focused on substitution and alignment approaches with minimal optimization to capture secondary interactions and disruptions to protein expression. While novel, additional research is necessary to continue informing towards improving our understanding and control over non-canonical expression modalities.

The Intelligence Community Postdoc program seeks post-doctoral level research proposals focused on improving our understanding of non-canonical expression systems and methods for rational design of entangled or otherwise engineered proteins. This can include research to enhance the understanding of the design of entangled or otherwise non-canonically expressed proteins, that improve the ability to predict the function of entangled proteins, and/or pushing the boundaries of what is possible with regards to expression and encoding non-canonically expressed proteins that align with improving biosecurity capabilities.

Unclassified example approaches:

The intelligence community is interested in fundamental capabilities aligning towards characterizing protein expression, function, and associated biosecurity concerns. The recently completed IARPA Fun GCAT program, focused on threat detection of short DNA fragments. The papers referenced below include concerns from the screening community regarding the impact of non-canonical protein expression.

References:

https://www.science.org/doi/10.1126/science.aav5477
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8924478/
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8665328/
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8528312/
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8490965/
https://www.nature.com/articles/s41586-021-03511-5
https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8294169/

Topic 18
Modelling of chemical plumes in urban environments

Unclassified key words: plume modelling, environmental modelling, chemistry, chemical attacks, CBRNE, large eddy simulations, computational fluid dynamics, atmospheric modelling, aerosols, aerosol science.

Unclassified research topic description, including problem statement:
From an atmospheric modelling perspective, urban environments are exceedingly complex. The movement of materials is driven by multiple non-linear processes with nearly infinite dimensionality. Current models are forced to balance using high order approximations to reduce computing time with loss of accuracy and reproducibility. When all of this is combined with the need for rapid responses to potentially hazardous chemical plumes (chemical attacks, industrial toxins, etc.), the current models fall far short of what is needed.

This solicitation seeks to find an approach for characterizing the key variables and information needed to accurately model plumes in urban environments.

Accurate and rapid modelling of chemical plumes is critical for providing local, national, and global leaders with the information necessary to protect civilians and military personnel from hazardous areas.

Unclassified example approaches:
The focus of this effort is on reducing computational time without sacrificing accuracy of computational models. Approaches can be compared to available experimental data for validation.

Relevant data and techniques include computer vision, AI/ML, weather modelling/prediction, traditional plume modelling variables as well as new information streams.

References:
Lateb, M., et al. “On the use of numerical modelling for near-field pollutant dispersion in urban environments – a review”, Environmental Pollution 208 (2016) 271-283. Robinson, M., et al. “Variability and Time of Day Dependence on Ozone Photochemistry in Western Wildlife Plumes” Environ. Sci. Technol. 2021, 55, 15.

Topic 19
Effect of aerosol particle morphology on reaction dynamics

Unclassified key words: aerosols, environmental science, chemistry, physical chemistry, physics, kinetics, thermodynamics, microphysics.

Unclassified research topic description, including problem statement:
The properties and dynamics of mixed aerosol particles depend on their phase, chemical composition, and morphology. The rates of reactions strongly depend on whether the condensed phase reacting substances are available on the particle surface or obscured by non-reactive substances, or fully encapsulated by a protective shell. In particular, the chemical and physical processes associated with secondary organic aerosol (SOAs) formation are complex and varied with several knowledge gaps remaining. SOAs account for a significant fraction of ambient aerosols and so an understanding of their formation, properties, and dynamics is needed to address both climate change and human health.

Additionally, accurate identification of aerosols in complex environments is vital to national security as many chemical threats are, or could be, delivered as aerosols. Understanding the role of particle morphology in the properties and dynamics of aerosols is critical to assessing threats in a timely manner.

This solicitation seeks an approach for characterizing the morphology of aerosol particles to study how that affects chemical reaction dynamics and physical changes.

Unclassified example approaches:
The focus of this effort is on developing an understanding of the role morphology plays in reaction dynamics of particle mixtures. Approaches may include experimental methods and/or computational approaches (compared to available experimental data for validation wherever possible). Relevant data and techniques may include aerosol mass spectrometry, electron resonance spectroscopy, photochemical aging processes, or other approaches. Variables to be considered include chemical composition, temperature variation, humidity levels, and particle formation methods.

Topic 20
Emerging application for superconducting electronics

Unclassified key words: superconductivity, microelectronics, computer architecture, digital signal processing, neuromorphic computing.

Unclassified research topic description, including problem statement:
With the end of Dennard scaling and now Moore's law, future advances in computing will increasingly come from novel approaches to microelectronics. Superconducting electronics (SCE) offers the possibility of energy-efficient computing and/or high clock speeds, bypassing the power dissipation and signal distribution limitations of high-density chips.

However, present-day SCE have low circuit densities, especially for memory, making the implementation of conventional CPU architectures in SCE difficult.

This topic aims to identify emerging computing problems that can utilize the unique advantages of SCE and for which the lack of dense superconducting memory is not a fundamental impediment.

Unclassified example approaches:
- Superconducting hardware accelerators: customized hardware for performing specific computational tasks extremely fast and/or efficiently.
- Design of novel processing-unit architectures that leverage low-dispersion superconducting interconnects to better utilize off-chip low-density memory, possibly utilizing chip stacking.
- Digital signal/image processing of data streams generated by cold sensors: radar/communications receivers, transition edge sensors, superconducting analogue-to-digital converters.
- Neuromorphic and stochastic computing implemented with superconducting technology.
- Novel interfaces between SCE and cold CMOS to enable the use of dense CMOS memory in SCE architectures.

Topic 21
Enabling components of human augmentation

Unclassified key words: human augmentation, cognitive augmentation, bioelectronics, neural interface, human-machine teaming, human machine interface, bioengineering, biomaterials, sensors, electronic skin, artificial neural networks, brain computer interface, cognitive enhancement, human-in-the-loop.

Unclassified research topic description, including problem statement:
Devices for detecting a variety of inputs including motion, pressure, and electrical activity are necessary for many human-augmentation technologies. However, development in human augmentation is incremental and derives from advances in technologies that fill a need. More recently, researchers have begun to realize the possibilities of these technologies in advancing human capabilities, and projects have developed with the aim of extending a person's abilities. Sensors that enable human augmentation, for example, can include implants, biotechnologies, and information technologies. The aim of this topic is to develop a fundamental understanding of enhanced capabilities, augmented intelligence, and more rapid, structured, voluminous data exchanged between human and machine.

Unclassified example approaches:
A brain-machine interface requires sensors to input information from brain function to a machine, or vice versa. Human augmentation has great potential through bioengineering to achieve significant advances in enhancement and control process of human capabilities beyond their normal range. There are different ways to approach this research; versatility is encouraged. For example:

- One approach could investigate enabling components which would allow a brain-machine interface to control a swarm constellation or receive multiple intelligence feeds from different platforms, taking a systems of systems integration approach.
- A different approach could focus on investigating advanced software using machine learning and big data to augment the potential for a human-machine interface to be used in support of intelligence collection or analysis. Whether information technology augments human intelligence via brain interfaces or via advanced wearables, software will need to determine the information, intelligence, or other input that would increase human cognitive capacity.
- Another approach could explore a human-machines interface's potential for augmenting human capabilities, such as boosting human reaction time or altering human behaviours, while investigating how different sensors or implants could improve these abilities.