ROYAL ACADEMY OF ENGINEERING

Government Office for Science

Research topics 2020

Ref	Topic Title
2020-01	Determining the impact and use of synthetic biology methods to create existing, modified or new pathogens
2020-02	Near-field explosive properties, understanding the effect of short duration, high intensity environments on adjacent material
2020-03	Detecting needles in haystacks - how can quantum sensors help improving security screening?
2020-04	Measuring deterrence success of public assistance measures
2020-05	Generation of novel sensors for chemical detection
2020-06	Pattern detection (structural) within large complex network graphs
2020-07	Agile manufacturing of multi-constituent metamaterial inspired electromagnetic devices
2020-08	An investigation of 5G technology and the threats it presents for the security community and identification of countermeasure opportunities
2020-09	Research into future millimetre wave wireless systems propagation in modern built and secure environments
2020-10	Smart cities, multimedia mesh networking
2020-11	Automated component recognition for hardware assurance
2020-12	Improving energy storage and energy harvesting in IoT wireless sensor nodes
2020-13	Modelling the effects of mechanical stress for batteries in wearable applications
2020-14	Propagation-resistant safe battery packs without compromising on high energy densities
2020-15	Robust physical layer security for wireless communications
2020-16	Improving quantum and optical sensors using machine learning techniques
2020-17	Reconfigurable broadband RF metamaterials
2020-18	Reasoning for autonomous domain specific robots
2020-19	Cyber influence on behaviour change: Prevalence, predictors, progress and prevention
2020-20	Explainable and trustworthy artificial intelligence

Topic 2020-01

Determining the impact and use of synthetic biology methods to create existing, modified or new pathogens

Key Words: pathogen; synthetic biology; genetic engineering; molecular biology; gene editing; detection; virus

Problem Statement:

Genetic engineering technologies are rapidly developing, rendering the manipulation of genetic material increasingly simple, efficient and convenient. This has numerous applications, including the generation of existing naturally occurring pathogens or novel synthetic pathogens de novo from genome assembly techniques, as well as the genetic editing of naturally occurring pathogens to produce synthetic variants. As synthetic biology techniques and methods for manipulating genetic material continue to evolve, it is likely that the technical barrier to genetic engineering will decrease, rendering this approach more accessible to those with less technical expertise or reduced capability.

Malicious use of genetic engineering could be used to modulate a range of pathogen characteristics, so as to enhance pathogenicity, onset and severity of symptoms and environmental persistence. Furthermore, it may be challenging to determine when genetic engineering has been employed, for example when a naturally occurring pathogen is generated de novo in a laboratory setting and used as a bioweapon. As these synthetic pathogens may mimic to an extent the symptoms of wild-type variants, it is plausible that their presence may go unnoticed. The purpose of this research topic is to more greatly understand how existing and emerging genetic engineering technologies may be used to create or modify pathogens and determine what biomarkers may be identified to facilitate the detection of their use.

Example Approaches:

A possible approach may include:

- Collation and analysis of existing, emerging and future genetic engineering methods and technologies, and their potential applications to the production of existing, novel or modified pathogens.
- Determining how pathogen characteristics could be selectively modulated by genetic engineering techniques.
- Determining how the use of synthetic biology techniques to produce existing pathogens may be detected, both pre- and post-release e.g. presence of biomarkers.
- Determining how the use of synthetic biology techniques and resulting modified organisms may hinder available detection methods.
- Determining whether a new pathogen is the product of synthetic biology techniques.

Topic 2020-02

Near-field explosive properties, understanding the effect of short duration, high intensity environments on adjacent material

Key Words: explosives temperature; energetic modelling; near field

Problem Statement:

When an explosive reacts, either through detonation or deflagration, a complex series of chemical reactions occur rapidly generating an explosive shock wave coupled with intense thermal effects in very short (microsecond) timescales. The effects of combined thermal and shock exposure to materials in contact with the explosive charge, including reactive chemicals, biological materials or mitigation materials, is not well understood.

We seek research proposals that will increase our understanding of the near field behaviour, including thermal and shock. This understanding gained through this research should be of sufficient accuracy to allow its application to assessments of novel devices. The electromagnetic emission spectrum of explosions is also not well characterised. Improved methods of measuring this behaviour, either through modelling, experimentation or both, would improve our capability for remote detection.

Example Approaches:

- It is envisaged that this project would include both computational and experimental aspects. Computational and theoretical approaches will be developed to predict the near field behaviour of different energetic materials, including conventional, commercial and improvised. This could include a combination of thermochemical calculations, ab initio molecular modelling and hydrodynamic simulations and may integrate existing models.
- The modelling data would be complimented using precision experiments to measure the near field behaviour, including the intensity and duration of the thermal output in the near field region.
- Synergistic effects between the shock / blast wave and the thermal effects would be assessed.
- An experimental method for reproducing thermal environment of an explosion in laboratory-based experiments could be developed.

Topic 2020-03

Detecting needles in haystacks – how can quantum sensors help improve security screening?

Key Words: detection of explosives; weapons; contraband; security screening of vehicles; containers; cargo; deliveries; pallets; security screening of crowds

Problem Statement:

Whilst there is a wide variety of proven technologies for screening people and items for the presence of explosives and weapons threats and other contraband, deployment of these established technologies can become impractical from the perspective of efficiency as the requirement scales. For example, while baggage X-ray machines can screen hundreds of items an hour, larger, purpose-built machines can typically only screen a few tens of vehicles or containers per hour. Similarly, airport-style screening of people and their possessions cannot easily be scaled to work at major sports stadia and concert venues where peak flows of people are much greater.

Globally, governments, industry and academia expend considerable effort identifying and commercializing innovative improvements to established technologies such as X-ray, metal detection, passive millimetre-wave, radar, explosives trace detection. How might innovations in quantum technologies – especially quantum sensors – be harnessed to offer alternative approaches? In particular, how might quantum techniques offer new, more efficient and / or effective ways of detecting threat items that are several to many orders of magnitude smaller than the volume being screened – the proverbial problem of "finding a needle in a haystack"?

Example Approaches:

Potential applications / problems include:

- Screening vehicles (cars, vans, lorries, buses, coaches, etc.) for explosives and weapons threats and other contraband.
- Screening shipping containers, pallets and other bulk cargo / freight / delivery items for explosives and weapons threats and other contraband.
- Screening individuals and their possessions for very small contraband / threat items (e.g. sim cards, USB sticks, razor blades).
- Screening groups – or even crowds – of people collectively (rather than individually) for the presence of explosives and weapons threats.

Topic 2020-04
Measuring deterrence success of public assistance measures

Key Words: detecting; behavioural; outcome of campaign analysis; deterrence; prevention; methods of measurement

Problem Statement:
There have recently been several initiatives to increase public awareness around actions to take if they observe suspicious behaviour. The end goal is to inspire and empower the public, create a more security-conscious society and deter those with malicious and criminal intent. Improving public vigilance of potential suspicious activity has resulted in an increased volume of reports requiring investigation. When the public report their concerns of suspicious behaviour, this is relayed to several different stakeholders, for example local police, British Transport Police or security teams within venues.

The initial message from the public passes through a chain of communication which results in action taken by the necessary stakeholder. There are many different communication nodes that the message must pass through efficiently before an action is taken. Improving the effectiveness of the reporting system is an area of interest, which could be achieved by novel processes or technologies.

There are currently some methods of measuring the effectiveness of the message propagating through the system, however innovative means to assess and evaluate this mechanism are required.

Further, to measure the effectiveness of individual initiatives, it is essential to have a robust definition of success and measures of outputs and impacts. There are some means by which deterrence is measured, however, novel means to assess initiatives, especially those that can gather results quickly in dynamic environments would be beneficial. This extends to the predictive measures of success of future initiatives. This will improve the development of future initiatives, enabling new deterrence ideas to be deployed more quickly to help the public.

Example Approaches:
- Analysis of current reporting systems to determine where efficiencies could be made.
- Development of methods and techniques to assess the lifecycle of the chain of communication from when public reports are received to when action is taken.
- Determination of an efficient but effective reporting system for all stakeholders.
- Generation of models that assess and predict the effectiveness of current and future reporting structures.

- Approaches to reduce false alarms as the result of deterrence initiatives.
- Development of methods and techniques to assess deterrence/prevention of an activity.
- Analysis of initiatives to determine novel measures of success.
- Generation of models that measure, test and predict the effectiveness of future public awareness initiatives.
- Creation of qualitative metrics for analysis of reporting structures.

Topic 2020-05
Generation of novel sensors for chemical detection and identification

Key Words: detection; sensors; chemical detection

Problem Statement:
First responders (e.g. fire and rescue service, specialist policing teams) require fast detection and identification of hazardous or toxic chemicals (including, but not limited to, explosives, drugs and other contraband) when there has been an incident or industrial spillage. Current processes can detect and identify chemicals with a high level of certainty, however there are often high numbers of false 'alarms' or indeterminate results. This is due to the interferents which exist in the environments where sensors are deployed and which can contaminate the sampling process, and complicate analysis.

Within a sample there can be many different particulate matters present, all of which need to be identified with a high level of certainty. First responders carry a range of different sensing equipment, as not all capabilities are able to address all samples. Novel chemical sensors that can detect a wider range of chemicals, with a higher specificity and selectively, whilst reducing the false alarm rate would be greatly beneficial to first responders.

Beyond the fundamental ability to detect and identify chemicals, there is an enduring desire to limit the risk to first responders when collecting samples. While this can be addressed through Personal Protective Equipment, another approach is to increase the distance at which first responders can sample and analyse unknown substances. Therefore, approaches which enable standoff detection and identification are of particular interest.

Example Approaches:
- Adaption or improvement of existing sensors to reduce the false positive rate in 'real-world' environments.
- Generation of new technologies to create a sensor that can identify multiple compounds with a high level of certainty.
- Multiple sensors used in tandem or integrated to create a standoff chemical detection system that has low false positive rates. Standoff chemical detection could be from a short (cm) to long (m) distance away, using a variety of mediums to hold the sensor, such as a fixed location or unmanned aerial vehicle (UAV).
- While most standoff detection methods would use some form of laser-based spectrometry, novel approaches that use ion-mobility or mass spectrometry techniques would be of interest. In addition, the community is interested in approaches that can be adapted for liquid, solid or power samples, in either bulk or trace volumes.

Topic 2020-06
Pattern detection (structural) within large complex network graphs

Key Words: large complex networks; scalable; pattern detection; graph theory

Problem Statement:
Social networks, Internet of Things, software development and vulnerability assessments are examples of areas that can all be modelled and understood using graph theory and complex network analysis. Graph theory allows a variety of scenarios across a range of areas to be represented as networks and analysed to identify structures and behaviours.

The structure of the network is key to its function and the discovery of repeating structural patterns across a single large complex network is of particular interest. Currently, pattern discovery within a scenario of interest can only be undertaken manually. This is very time consuming due to the size of both the network and the patterns. The scale and breadth of network structures are increasing rapidly, whilst some are expanding into temporal and dynamic datasets (e.g. Internet of Things). This impacts the viability of manual pattern detection.

To date, within UK HMG limited research has been undertaken to identify ways of overcoming this problem. There are no known algorithms available to discover large (~50-100nodes) patterns within a single large complex network, although progress is being made through the use of novel approaches e.g. motif detection and graph neural networks.

Although open source complex network datasets are available, none have been found to contain sufficient repeating patterns for training and testing or exploration. Open source datasets of complex networks that are available and potentially adaptable, include, but are not limited to:
- https://www.cnn.group.cam.ac.uk/Resources
- https://github.com/gephi/gephi/wiki/Datasets
- http://www.ee.cityu.edu.hk/~gchen/ComplexNetworks/SoftwareDatabases.htm

Example Approaches:
A scalable method for discovery of large repeating patterns within a single large complex network is required. The key requirement for this project is to research, identify and develop algorithms or produce innovative solutions that could identify repeating patterns across a single large complex network.

Current focus of research is the discovery of exact matching large patterns (~50-100nodes) within a static complex network. Future work may include extending the research to discover

patterns within a temporal and dynamic complex network dataset. Proposals that consider a methodology which can be extended are sought, as there is potential to extend this work for a 3rd year.

Research proposals should include:

- Research into available algorithms and assessment of suitability for adaption or extension. Proposed methods will be assessed against:
  - Scalability
  - Ability to cope with hierarchical pattern discovery
  - Potential for node categories to be considered
  - Discovery of exact matching patterns
  - Discovery of similar patterns
- Development of one or more methods for assessing against open source data.
- Improvement of method dependent on test results.
- Potential to adapt deliverable for pattern discovery on a temporal or dynamic dataset.

Technical partnering will be provided. Throughout the project regular delivery of working scripts is required to enable inhouse testing on data. Where possible following internal testing, feedback on performance will be provided.

Topic 2020-07

Agile manufacturing of multi-constituent metamaterial inspired electromagnetic devices

Key Words: metamaterials; functional materials; microwave; optical; additive manufacturing; 3D printing; 4D printing

Problem Statement:

Maximising and optimizing the performance of devices and components within extreme size and form factor design constraints is bounded by fundamental theoretical limits and available routes to manufacturing; where the latter further limits the internal geometries of devices and components and the palette of materials available to present manufacturing processes.

The emerging field of metamaterials is demonstrating how complex multi-scale topology, symmetry and order in the arrangement of dissimilar materials (like conductors, insulators and other electromagnetically functional materials) can deliver novel device concepts. These concepts offer game changing extensions to the engineering trade-offs, that have been long accepted between performance, size and form factor. This approach provides a design paradigm to engineer devices with performance characteristics substantially closer to the theoretical limit.

Further advanced manufacturing processes, like 3D and 4D printing, are required to enable the manufacturing of more complex items with topologies not realizable by conventional means like top down lithographies. However, fundamental progress is required to extend these processes to work with the required combinations of materials. Additionally, radical new 'self- or directed-assembly' approaches like synthetic biology may ultimately also become competitive as fabrication pathways in this respect.

A fellowship in this area would realise machine specifications or methodologies to combine diverse materials in complex topologies over relevant length scales to enable access to such engineering capability and application outcomes. By demonstrating application relevant proofs of concept, investment for industrialization would be stimulated.

Example Approaches:

- Simple proof of concept studies and test items have been produced, but access to complex multi-scale topologies created from multiple materials remains the research challenge and goal. Examples include a flat microwave Luneberg lens equivalent by casting graded layers of tailored refractive index materials (Mateo-Segura, Carolina; Dyke, Amy; Dyke, Hazel; et al. Flat Luneburg Lens via Transformation Optics for Directive Antenna Applications, IEEE TRANSACTIONS ON ANTENNAS AND PROPAGATION, 62(4), p1945-1953, 2014); casting

layers of tailored magneto-dielectric layers to improve electrically small antennas (Wang, YQ; Edwards, E; Hooper, I; Clow, N; Grant, PS. Scalable polymer-based ferrite composites with matching permeability and permittivity for high-frequency applications, APPLIED PHYSICS A-MATERIALS SCIENCE & PROCESSING, 120(2), p609-614, 2015), as well as using similar materials and fabrication methods to demonstrate novel ground planes for low profile antennas (Dstl in collaboration with University of Oxford).

- Current PhD studies supported by Dstl at Universities of Exeter (relating to magnetically coupled helices) and Nottingham (relating to additive manufacture of graded metal-ceramic structures, and separately optical band moth-eye anti-reflection structures) provide examples and confidence that this fellowship would be timely. They further highlight the interdisciplinary nature of the topic and the relevance of a Fellowship to provide focus and drive.

Topic 2020-08

An investigation of 5G technology and the threats it presents for the security community and identification of countermeasure opportunities

Key Words: 5G; millimetre wave; radio physics; technical security; wireless sensing; pattern recognition; countermeasures

Problem Statement:

Modern and future wireless technologies, such as fifth generation (5G), are utilizing increasingly higher frequencies extending into the millimetre wave and beyond with their associated ability to support higher information bandwidths. The commercialization of this technology is leading to the availability of low-cost RF sub systems and components at these higher frequencies. This will increase the likelihood of technical threats utilising these technologies and frequencies. We need to understand if the existing threat models are challenged by this new technology and devise appropriate and effective countermeasures.

The aim of the research is to:

- Explore how these frequencies and waveforms interact with electronic systems at a fundamental level.
- Adapt 5G technology sub systems to demonstrate:
    - The technical surveillance vulnerabilities posed by these
    - Their application to detective countermeasures
    - Provide advice and guidance to protect the public, businesses and national infrastructure and enhance security screening at airports/ border checkpoints

Example Approaches:

There is a growing area of research that examines security and privacy concerns, identifying attack methods and identifying countermeasures to offer greater protection from such attacks. For example, there has been research to discover how audio from loudspeakers may potentially be recovered from soundproof buildings due to the subtle disturbances they cause to RF transmitters such as widely available such as Wi-Fi. The research identifies the risk and then describes how to protect against this potential attack method. (Reference: "Acoustic Eavesdropping through Wireless Vibrometry" Teng Weiy, Shu Wangy, Anfu Zhou and Xinyu Zhangy University of Wisconsin - Madison, Institute of Computing Technology, Chinese Academy of Sciences)

Topic 2020-09

Research into future millimetre wave wireless systems propagation in modern built and secure environments

Key Words: millimetre wave; propagation; radio physics; radio propagation; built environments; technical security

Problem Statement:

Modern and future wireless technologies, such as fifth generation (5G), are utilizing increasingly higher frequencies into the millimetre wave and beyond with their associated ability to support higher information bandwidths. The increased path loss at these higher frequencies means that the density of wireless access points is also increasing resulting in a closer proximity to secure systems and raising associated electromagnetic security concerns. Understanding the radio physics of radio propagation of high bandwidth signals at millimetre wave within, into and through buildings and the associated wider built environment is necessary for modelling the electromagnetic security threat posed by these new and emerging systems. The approach is to produce a field portable system and undertake radio propagation measurements of high bandwidth millimetre wave links in representative (including overseas) built environments and develop a representative propagation model.

Example Approaches:

- Although existing radio propagation models exist for millimetre wave propagation, there has been little work in recent years that takes into account the modern building materials and techniques used in modern building and the built environment, in particular the differences in these across the world.
- Current recommendations of the International Telecommunications Union, ITU, provide two separate recommendations for building entry loss and for clutter loss. Recommendation ITUR P. 2109 predicts building entry loss for two types of buildings classified as thermally efficient and traditional buildings assuming a direct path which is not typical for base station mountings. Recommendation ITU-R P. 2108 predicts the loss due to clutter which includes buildings and other obstacles. Currently there is no model that combines clutter loss and building entry loss for typical base station deployments.
- Understanding millimetre wave propagation in and around the constructions of secure working environments is considerably lacking.

Topic 2020-10
Smart cities: multimedia mesh networking

Key Words: smart cities; multimedia mesh networking

Problem Statement:
Many networks in Smart City applications are wireless based, however, spectrum is limited because of limited capacity and operating restrictions on pre-authorised licence bands, and limited availability of formal allocations. Other transmission media are required in order to expand capacity, increase the opportunity for node deployment in hostile environments, and exploit serendipitous paths in forming mesh networks.

This topic is to explore and identify realistic and tangible communications media for reliable mesh networking at bandwidths appropriate for the edge of the network. This will involve considering transmission at the physical layer using non-traditional techniques. It is anticipated that only one medium will be exploited per transmission path. It is assumed that identified media will be bidirectional in most cases, but need not be exclusively so.

The topic is about innovating the method of communication for network nodes in order to alleviate bandwidth limitations, avoid communications conflicts, increase ubiquity in the real-world environment, and create opportunities for improving cybersecurity of network traffic at the physical layer. This will require the identification of communication media with properties suitable for practical implementation. Key issues include:

- physical size, weight, heat, power budget
- impact of media conversion (challenges of multimedia routing in ad. hoc. media channels)
- impact of multimedia on protocols and user throughput
- impact on multimedia on user/application/node authentication
- tractability of overall network performance modelling
- tractability of overall network security/threat modelling

A critical output are the design methodologies, the key design limitations, and the "how to design" know-how in order to engineer a multimedia mesh network to a desired design objective (such as throughput or security).

Example Approaches:
Example media that have been considered or are being pursued include: Non-Zenneck electromagnetic surface wave on passive conductors; light (both visible and non-visible); acoustic (including within fluids); mains borne signalling; wide area chemical signalling using airborne volatiles (scent); modulated ionising radiation.

Topic 2020-11
Automated component recognition for hardware assurance

Key Words: machine learning; computer vision; printed circuit board; PCB; hardware assurance; integrated circuits; IC; electronics; component recognition

Problem Statement:
Printed Circuit Board (PCB) fabrication and assembly generally follow market forces and are undertaken in areas where costs are lowest. It is common for a PCB to be designed in one location, fabricated in a second location, then assembled in a third location prior to shipping to its final destination where these supply chains and shipping routes are outside the control of the initial designer and the end consumer. Full verification of the supply chain to authenticate each individual step and component in the process is presumed to be prohibitively difficult, time consuming and expensive. It is therefore an accepted risk that the supply chain is vulnerable to outside influence and potential attack.

A recent WIRED article ("Planting Tiny Spy Chips in Hardware" Andy Greenberg 2019-10-10) details a relatively cheap and simple proof of concept attack whereby a security researcher added a small integrated circuit (IC) onto a PCB to successfully attack and gain access to the security administration configuration code running on the board thus gaining full control of the running software. The additional IC was chosen to be of a small enough size that it would be hidden in plain sight among the forest of components on the board making it very difficult to all but the most determined and technically capable end user to find. While this is a proof of concept attack, a more capable and better resourced attacker could further refine this method, further increasing the difficulty of identifying any potential attack. One method to mitigate against this type of attack is examination of the electronic components and their locations on the PCB and comparing the components to known good samples and their position to that specified in the design data. Comparing both the components to a known good reference and comparing the layout to the design data is currently a slow manual process that does not scale with increasing demands for PCB and supply chain verification.

The aim of this topic is to create a process to automatically identify, categorize and determine component packages and record their centroid location information. This automated process would greatly reduce the manual effort required and speed up the process of hardware assurance, helping to mitigate against hardware attacks on critical and secure high value systems. Though the aim is simple to write, and automated component recognition has been researched as a proof of concept on contrived PCB examples, the wide variety of IC package types available and idiosyncratic PCB layouts make it a hard problem to generalize component recognition outside contrived examples. The array of high value end user equipment

purchased that would benefit from enhanced hardware assurance means a more generalized and efficient approach to automated component recognition is a necessity.

Example Approaches:

- Literature review of published knowledge on PCB component recognition
  - Identify common processes and compare their strengths and weaknesses
  - Identify possible solutions and algorithms
- Generate and acquire a PCB image dataset encompassing variations of PCB designs and components
  - Evaluate the optimal approach to imaging PCBs and components for machine learning, e.g. 2D/3D/hyperspectral images
- Use the dataset to optimize machine learning algorithm to recognize components, their locations on the PCB and label them
- Test and verify machine learning algorithm
- Create a Windows PC application to automate component recognition, generate a labelled output and specify a hardware setup optimized for component recognition

Topic 2020-12
Improving energy storage and energy harvesting in IoT wireless sensor nodes

Key Words: Internet of Things (IoT); wireless sensor nodes; WSN; battery; batteries; Li-ion; lithium polymer; solid state; energy harvesting; electrodynamic; piezoelectric; photovoltaic; solar; thermoelectric; triboelectric; power electronics; low power

Problem Statement:
The Internet of Things (IoT) is a growing market with predicted worldwide spending in this field to exceed $1.2T by 2022. This topic is focused on wireless sensor node (WSN) hardware which are designed to be cheap and easy to install without the need to integrate into existing infrastructure. Examples are smart electricity metering to ensure accurate monitoring of the National Grid load, smart home features e.g. internet connected thermostat lighting and security intruder detection and crop monitoring ensuring farmers can obtain real time data on soil quality and moisture content to improve yields. However, use of WSNs are currently limited by a number of factors including; the energy density of small form factor power sources, sensor performance vs power consumption, device/maintenance overhead (e.g. battery change), efficiency of existing energy harvesting systems and more generally size, weight and costs.

The aim of this topic is to address shortcomings in the way WSNs are powered, with the broader goal of increasing the duration of the device. Proposals are welcomed that tackle this goal from a variety of different routes. Proposals should look to build upon or surpass the current academic/industrial start of the art, some examples below:

- Small form factor energy storage: there are commercialized wearable medical trackers to measure body temperature when a fever is developing. They can be worn as an unobtrusive and conformable patch with Bluetooth connectivity to a Smart phone, however they only have a 48-hour lifetime.
- Energy harvesters: there are commercialized thermoelectric generators (TEGs) and there has been a significant amount of academic publications. TEGs can provide 'free' power from a temperature differential, but typically this differential is difficult to maintain, or the device is restricted to conditions where heating and cooling is readily available (i.e. a radiator pipe). This can often result in intermittent and unreliable power.
- Low power sensors: there has been development of 'intelligent tags' that off reduced power levels down to nanowatts to greatly increase the lifetime of a typical Lithium coin cell, but this comes with the limitation on the complexity of data that can be obtained.

Example Approaches:
The following examples highlight several strategies to improve the shortcoming in WSN power noted above. However, all proposals that address the aim will be considered.

- Using novel materials or assembly approaches to develop efficient energy harvesters that can function over a wider range of ambient conditions. This should aim to push forward the current technology which often provides insufficient or unreliable power.
- Develop an energy harvesting system that provides continuous and reliable power enabling WSNs to be battery free.
- Develop miniaturised primary or secondary battery technology in the order of mm3, but maintaining state of the art energy densities typically seen in larger packages (i.e. greater than 300 Wh/L)
- Increase the efficiency of power electronics used to covert harvested energy into useful power. For example, the conversion of nanoamps of current at several kilovolts typically seen with piezoelectric harvesters to power WSNs currently results in significant power losses.

Topic 2020-13
Modelling the effects of mechanical stress for batteries in wearable applications

Key Words: battery; batteries; electrochemical cells; Li-ion; lithium polymer; modelling; mechanical stress; wearables; wearable applications; composite structures; failure modes; conductive textiles

Problem Statement:
Wearable technologies are becoming an increasingly large industry. As of 2017 the global wearables market was worth ~$38 Billion by revenue and is forecasted to reach ~$85 Billion by 2022 (IDTechEx Wearable Technology 2017-2027). As a breakdown of the markets, this industry is dominated by smartwatches, fitness trackers and medical devices. Some of the leading players and products are well-known, such as the Apple Watch, Fitbit and the various hearing aids available. There is also significant growth expected in the e-textile market, from an almost non-existent market in 2016 to ~$2 Billion [USD] by 2022 (IDTechEx E-Textiles 2017-2027). This has been driven by the miniaturization and reduction in power consumption of electronics, advances in the maturity of printed electronics and the developments in weaving conductive threads. To further battery technology in these sectors, it is anticipated that batteries will be embedded directly into garments. The impact of the natural movement of a human and their garment on the mechanical stresses that develop within a lithium polymer cell is not well understood. As such embedded batteries in a wearable device are typically limited to a coin cell or a lithium ion cell which is encased in a relatively rigid outer packaging. Utilizing lithium polymer cells which are not rigidly encased and are instead in mechanically conformable devices will increase consumer appeal and could enable advanced power systems for wearables and e-textiles products.

The aim of this topic is to better understand the mechanical and electrical degradation of lithium polymer cells when under a variety of mechanical stresses typical to wearable applications. It is noted that there is some open source information on the biomechanical movements and the muscular and joint forces of the shoulder region (Ambrosio, J., et al., Symposium on Human Body Dynamics 2011) and the lower body during exercise (Thompson, W., K., et al. NASA/TM-2015-218852 2015). There are also several e-textile and wearable porotypes that have been evaluated in the literature (Stoppa, M. and Chiolerio, A., Sensors 2014), where serpentine printed structures or woven conductors are used to aid strain relief during natural garment movement. These studies suggest that the number of mechanical variables that wearable electronics, specifically lithium polymer cells in this scenario, may undergo is vast. For example, the bending radii, number of bending cycles, twisting angle, effect of 'scrunching', the dimensions and aspect ratio of the lithium

polymer cell, and the effect of the substrate or material supporting the lithium polymer cell (for example, fabric, polymer, rigid leather backing). Due to the numerous variables outlined, it is impractical to test all scenarios.

Computer modelling could dramatically reduce the amount of testing required. There have been models that have identified mechanical degradation in lithium ion cells during cycling (Laresgoiti, I., et al., J. Power Sources 2015) and have simulated lithium ion cells under abuse (Ali, M. Y.; et al., J. Power Sources 2015), but to our knowledge there are limited open source publications modelling the effects of mechanical degradation on lithium polymer cells during realistic flexing scenarios.

A successful model may incorporate the following:

- Experimental observations as a basis to understand and then model particle to particle mechanical interactions in typical lithium polymer components, such as metal foils, coated electrodes and separators.
- Simulate the effect of the mechanical stresses that occur within a multiple layered lithium polymer cell during typical flexing in a wearable garment.
- Alter certain flexing variables (such as bending radii etc.) to understand the effect of a variety of mechanical stresses on a lithium polymer cell.
- Consider the elastic properties of the substrate or material supporting the lithium polymer cell.
- Consider the elastic properties of the substrate or material supporting the lithium polymer cell.
- Identify likely failure modes of a lithium polymer cell and when they may occur.
- Increase understandings of how the mechanical degradation effects the electrical response of a lithium polymer cell.
- Include the effect of stresses from flexing on interconnects and woven conductive fibres.
- It is noted that modelling human biomechanical movements is out of scope of this project.

Example Approaches:

The unmounted soldier has an ever-increasing need for man portable power, leading to an increasingly heavy burden. It is desirable that equipment is powered by light-weight lithium polymer batteries that are body-borne, garment embedded, conformal, not impacting movement, and distributed evenly across a soldier. However, a barrier to utilizing such a system is the unknown effect of the mechanical stress on the lithium polymer cells, and subsequent impact on safety and the electrical performance fatigue. For example, if a lithium polymer cell is embedded within the soldier's garment, what are the effects of the mechanical stresses that the lithium polymer cell may undergo when the soldier is running?

Topic 2020-14

Propagation-resistant safe battery packs without compromising on high energy densities

Key Words: batteries; battery packs; lithium; li-ion; safety; propagation resistant; passive; energy densities

Problem Statement:

Li-ion batteries have become indispensable in modern life and have enabled a plethora of portable devices such as mobile phones and drones due to their high energy density. Li-ion batteries are poised to revolutionize the transportation sector with major auto makers announcing a complete switch from internal combustion engines to battery electric vehicles (BEV), as such the BEV market share is projected to be about 20 % of all new car sales globally by 2030.

Due to the increased run-time or reduction in size/weight, the military and IC community have also become reliant on high energy Li-ion batteries to power their equipment. However, there is a safety drawback with Li-ion batteries. The energetic lithiated anode and the highly flammable organic electrolyte typically present in Li-ion batteries have resulted in several safety incidents, such as BEV fires reported to occur spontaneously, overheating of the Boeing 787 Dreamliner auxiliary power unit battery and a battery fire within the Navy's Advanced SEAL Delivery Vehicle (ASDS).

Due to the requirement to increase safety of large battery packs with multiple cells in series and parallel, typical battery packs in BEVs may exhibit energy densities of only ~120 Wh/kg and ~200Wh/L, whereas cell level energy densities can exhibit up to ~250 Wh/kg and ~650 Wh/L. The large reductions in energy densities are in part a result of increasing safety. However, an individual cell can still fail in an unsafe manner, this has to be managed to prevent propagation throughout an entire battery pack. Notable work to develop propagation-resistant batteries was done by NASA. It was found that in 18650 cells there was a high propensity to side wall ruptures.

To prevent propagation of failure, a pack design included increased cell spacing, interstitial heat sinks, individual cell fusing and flame arresting vent ports, all of which impacts size and weight. The aim of this topic is to develop fundamental understanding of the materials and cell parameters that impact a passive propagation-resistant battery pack in order to realise energy densities close to the cell level but retain the safety features shown in the NASA propagation-resistant battery pack.

Example Approaches:

The following examples can improve our understandings before undertaking development of a propagation resistant battery pack:

- Investigate the limitations of building block cells at close proximity. For example, is it safer to use 20Ah cell vs. a 2Ah building-block cell for a kWh battery?
- Further understandings of resistance to propagation vs. building-block cell design (e.g. high power vs. high energy cell)
- Model pack energy density as a function of parameters such as cell energy density, cell spacing, cell construction (prismatic vs. cylindrical), phase change materials, etc.
- Validate models using small representative battery packs

Topic 2020-15
Robust physical layer security for wireless communications

Key Words: wireless communications; physical layer security; cybersecurity; antenna arrays; OAM; direction dependent modulation

Problem Statement:
Current networks need to send large amounts of data efficiently and securely between multiple different points. Many methods for implementing physical layer security are inefficient, have difficulty in the presence of multipath and fading channels and/or lack the ability to be implemented for multiple users having simultaneous access. Conventional cryptographic protection is not always realizable in systems with low computational resources and low entropy. An additional downside is that the key exchange that is necessitated in most systems can be recorded and analysis performed to determine cryptographic weaknesses.

Topic Description:
This topic is to explore and characterize the performance of physical layer security techniques, especially in the presence of multipath and fading channels. Another aspect of key interest is to achieve a practical working range, which could be in excess of 100 meters (far field). The goal is to design an efficient modern communications system that can incorporate physical security techniques to increase the cost to eavesdroppers to intercept the signal. Characterization of the physical layer security should include evaluating for the efficiency of the system as well as probability of detection and probability of interception both with and without a prior knowledge. For any physical layer security technique, practical implementation should be considered including the impact of antenna element choice, array design, protocols, and data rates on error rates, mutual information and multi-user support. The report should also address the trade-offs for power and system complexity versus the security achieved by the link.

Example Approaches:
- Security-oriented beamforming; artificial noise injection; directional modulation; orbital angular momentum (generates the illusion of higher order rotation in the EM field by superimposing phased contributions from an array of antenna elements)
- Secure Antenna Polarization Modulation (SAPM) (dual polarized antennas are used to create data distortion with an element of randomness at all transmission angles except the intended ones)
- Modelling the security based on the inter-symbol interference (rather than simple Signal to Noise Ratio (SNR)

Topic 2020-16
Improving quantum and optical sensors using machine learning techniques

Key Words: machine learning; artificial neural networks; atomic sensor; quantum sensor; optical sensor; atomic magnetometer; atom interferometer; atomic clock; NV centre; Rydberg atom; optical frequency comb; optical fibre sensors; noise suppression; sensor calibration.

Problem Statement:
Quantum sensors (e.g. atomic magnetometers, NV centres in diamond, atom interferometers, atomic clocks, Rydberg atom electric field sensors) and novel optical sensors (e.g. optical frequency combs, fibre sensors) can show great sensitivity in the laboratory and in some cases have been demonstrated outside of a laboratory environment. However, barriers to more widespread use include the complexity of operating many of these sensors and the instability of the sensors in a relatively uncontrolled environment. For example, some quantum magnetometers require the ambient magnetic field and any field gradients to be carefully tuned, and some sensors with thermal sensitivities require some feed-forward process to correct for temperature fluctuations.

The process of nulling ambient fields or measuring thermal response characteristics can be time-consuming and frustrating, because often the sensor systems have complex and nonlinear behaviours that cannot be modelled well. Fortunately, algorithms used in machine learning are often highly suitable for problems such as these. While machine learning is more typically used to analyse data that has already been acquired, this topic is about using these algorithms to improve the performance of the sensor itself. A working quantum or novel optical sensor should be used to quantitatively improve a sensor when using machine learning algorithms as part of the sensor system, where improvement is along performance parameters such as accuracy, speed, robustness to noise and environmental fluctuations, or along system parameters such as size or complexity.

Example Approaches:
To date only a few examples of machine learning algorithms applied to quantum systems or traditional sensors have been published. Some examples include using artificial neural networks along with co-sensor data to increase the accuracy of the thermal calibration of a sensor, using a sequential Monte Carlo algorithm to optimize the Ramsey pulses driving an NV centre in diamond in the presence of environmental noise, using Bayesian optimization to find efficient procedures for generating a BEC, and using a conditional variable auto-encoder to decrease the measurement time of a current map of a quantum dot device. Because this is a relatively new approach to improving sensor performance, this topic is not at all limited to the sensors and algorithms described in this topic or in the literature. However, this topic

does not include using machine learning algorithms to process data already acquired by a sensor, or to devise new algorithms without testing them on a real sensor, or modelling sensor performance without demonstrating the algorithms on a real sensor.

Topic 2020-17
Reconfigurable broadband RF metamaterials

Key Words: radio frequency, microwave, metamaterials, reconfigurable, tuneable, broadband

Problem Statement:
Despite several advances in development of metamaterials operating in the radio frequency range, devices are still limited in bandwidth and have limited reconfigurable performance. Metamaterials provide unprecedented capability to control electromagnetic radiation. However, there has been limited development in radio frequency metamaterials exhibiting truly broadband operation, as well highly reconfigurable performance. Novel materials and metamaterial design platforms that would enable fully reconfigurable optical devices are desired.

Example Approaches:
Improve bandwidth and reconfigurable performance of radio frequency metamaterials: metamaterials, varactors, phase change materials, optically-driven control, electrically-driven control. One approach could be to design new RF antennas with phase change materials incorporated into the device, providing reconfigurability across a broad bandwidth.

Topic 2020-18
Reasoning for autonomous domain specific robots

Key Words: mission planning; autonomy; cognition; planning; artificial intelligence

Problem Statement:
This research topic addresses the challenge in developing reasoning for autonomous robots. Reasoning robots would require agents that perform deliberative planning. The goal of planner agents is to generate a set of synchronized high-level commands that once executed will achieve mission goals. In robotics the planner/deliberator is the locus of time-consuming computations. Usually this means such things as planning and other exponential search-based algorithms but also includes polynomial-time algorithms with large constants such as, but not limited to, certain vision processing algorithms in the face of limited computational resources. Techniques and methods for the development of autonomous goal/mission management and planning agents are of need.

Example Approaches:
Two categories of planners are "hierarchical task network (HTN) planners" and "planner/schedulers" (Kortenkamp and Simmons, 2016; Georgievski and Aiello, 2015). An example software packages that supports automated planning is CASPER (Continuous Activity Scheduling Planning Execution and Re-planning).

Topic 2020-19

Cyber influence on behaviour change: prevalence, predictors, progress and prevention

Key Words: social influence, persuasion, coercion, social cyber security, narratives, behaviour change, cyber-medicated changes

Problem Statement:

The aim of this project is to understand and forecast the impact of cyberspace on changes in human behaviour which has implications for social and political outcomes. Social cyber security has been identified as a key area where social behavioural science (SBS) can exchange knowledge and contribute to issues and challenges for the IC (US Decadal survey, 2019). How cyber may mediate behaviour change and the boundary conditions to such influence ('when and for whom') are core research areas for the SBS. There are recently developed models of social influence that draw, in particular, on group-level identity processes tied to common interests, belonging and shared norms. A key step forward would be to investigate the applicability of these models to cyber and their implications for actual behaviour change in the 'real-world'. Key questions are whether 1) existing models of social influence translate straightforwardly to the cyber environment and if not, how to redefine them accordingly and 2) cyber influence does have a direct relationship to behaviour and when this is most likely to occur. This research area is of broad scope and interest with potential to form a much larger research enterprise.

Example Approaches:

Proposals could consider the following approaches or perspectives:

- Investigate the personal and social characteristics of users (strengths and vulnerabilities) that are most and least likely to be cyber influenced
- Identify and demonstrate through experimental studies key factors that facilitate and disrupt cyber influence on users' behaviour
- Understand the factors that escalate the success of cyber influence to widespread behaviour
- Explore methods that can prepare and inoculate users to cyber influence tactics and assess their success
- Examine the underlying personal and social motivations that underpin certain areas of cyber influence including extremism and promoting actions that present security threats

Topic 2020-20
Explainable and trustworthy artificial intelligence

Key Words: artificial intelligence; trust in technology; automation; uncertainty; explainable AI; trusted analytics

Problem Statement:
Artificial intelligence (AI) capabilities must be adopted if analytical insights into big data are to reach their full potential. A key barrier to adoption appears to be user trust in 'black-box' algorithms, especially under uncertainty and when dealing with high-stakes consequences. A thorough understanding of user trust, interpretability of AI techniques and design methodologies for assistant uptake and trust in these systems is imperative if these technological advantages are to be adopted in order to achieve required analytical outcomes.

The issue of explainable AI remains a major obstacle to the broader application of AI-powered products and services due to issues of transparency and accountability. In addition to public debate around the need for transparency and accountability to be built into AI applications, this issue remains an obstacle for governments developing regulatory frameworks and legislative changes to govern the use of AI technologies. Many engineers and data scientists have questioned whether meaningful explainability, to the degree required, is technically possible, particularly as approaches such a neural networks and deep learning are becoming increasingly ubiquitous and complex.

Example Approaches:
- Research proposals could approach this from a variety of disciplines, or as a cross-disciplinary effort. The problem touches on aspects of data science, engineering, psychology, human-centred computing, systems and design thinking, software development and UX and UI design, with links into social sciences.
- Proposals could consider:
    - Explainable AI and approaches for increasing the transparency and reasoning behind more complex deep learning methods
    - Understanding the antecedents to trust and propensities user have to trust new technological capabilities
    - Understanding barriers to user trust and how to regain trust once lost
    - How the measured consideration of design of systems could influence trust and how system features may be manipulated to mitigate loss of trust
    - How human-machine interfaces can be better designed to enable a symbiotic working relationship between the human and computer