Royal Academy of Engineering

Government Office for Science

UK Intelligence Community Postdoctoral Research Fellowships 2022

Applicant guidance notes

Deadline 26 April 2022

Royal Academy of Engineering
UK Intelligence Community Postdoctoral Research Fellowships 2022

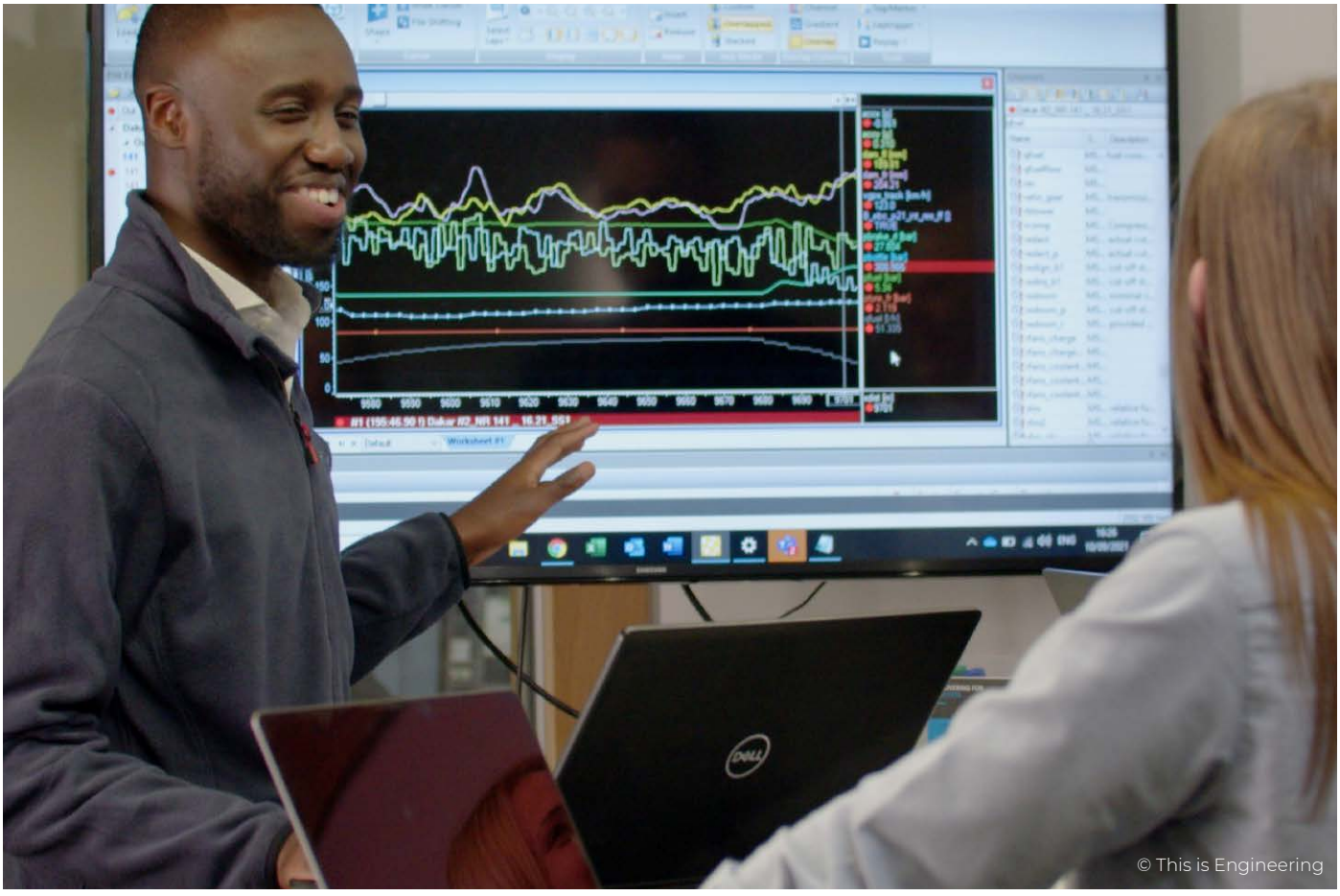
Contents

Click on a section below

Introduction

The Government Office for Science offers UK Intelligence Community (IC) Postdoctoral Research Fellowships to outstanding early career science or engineering researchers. These Research Fellowships are designed to promote unclassified basic research in areas of interest to the intelligence, security, and defence communities. The Centre for Protection of National Infrastructure, Department for Transport, Defence Science and Technology Laboratory, Home Office, and the National Cyber Security Centre are among the organisations represented in the UK Intelligence Community for the Postdoctoral Research Fellowships.

Members of the IC identify research topics and the Research Fellows work locally with University Research Advisors to develop and submit research proposals that align with the topics. The research is conducted by the Research Fellows while working in partnership with the University Research Advisor and collaborating with an advisor from the Intelligence Community (IC Advisor). The Research Fellowships are aimed at early career researchers from all branches of science and engineering who have up to five years postdoctoral experience. Each application for the UK IC Postdoctoral Research Fellowships is capped at a maximum grant of £200,000 over a 2-year period.



Diversity and inclusion

The Royal Academy of Engineering is committed to diversity and inclusion and welcomes applications from all underrepresented groups across engineering. It is the Academy's policy to ensure that no applicant is disadvantaged or receives less favourable treatment because of age, disability, gender reassignment, marriage and civil partnership, pregnancy and maternity, race, religion or belief, sex, or sexual orientation.

Access Mentoring support

The Academy aims to provide additional support to applicants from groups that are persistently underrepresented within UK engineering through the grant application process. This positive action will contribute to improving diversity in the talent pipeline and widening the diversity of applicants and awardees within the Academy's research grant schemes.

To be eligible for Access Mentoring, applicants must be either **women or from a Black, Asian or minority ethnic** background. Access Mentoring is a resource limited opportunity. Mentors will be assigned on a first come first served basis. For more information on Access Mentoring please refer to the guidance.

Part-time and flexible working

The Academy wants to support applicants to achieve a balance between their personal and work demands and is happy to discuss individual requirements and consider part time and other flexible working arrangements.

UK IC Postdoctoral Research Fellowships can be held part-time, but **must be the only source of employment.** The request for a part-time Research Fellowship (at no less than 50% of full-time equivalent) must be made clear within the application. Alternatively, the Research Fellowship can be converted from full time to part time, or from part time to full time, during the fellowship, assuming the host institution's HR department supports the request.

Research Fellows are entitled to maternity, paternity and adoption leave under the host institution's normal conditions of employment. The Academy will extend the duration of the Research Fellowship pro-rata to take into account such periods of leave and any conversions to part-time working. Research Fellows with caring responsibilities should liaise directly with the host institution if they wish to apply for part-time or flexible working.

Submission deadline

There is one application round each year. The online application system for the 2022 round will be open on 31 January 2022. The submission deadline for the 2022 round will be **4pm (UK local time)** on **Tuesday 26 April 2022**. Applicants will be informed of the result in July 2022.

Eligibility criteria

1. UK IC Postdoctoral Research Fellowships must be held at a UK higher education institution/university in a department that can show it is capable of fully supporting the research project and researcher.
2. It is the responsibility of the applicant to contact the host institution and gain formal approval from the relevant head of department or school before submitting an application.
3. The proposed research project must address one of the research topics outlined at the end of this document.
4. UK IC Postdoctoral Research Fellowships are aimed at early-career researchers. Applicants must have a PhD, which was awarded no more than **five years** before the submission deadline: **Tuesday 26 April 2022**. This time period includes applicants' work experience in academia or/and in industry. A margin of up to three months more than the five-year limit is acceptable. If applicants have had maternity/paternity leave or other extenuating circumstances, this will be taken into consideration if the relevant dates and details are provided in the application form.
5. PhD students are eligible to apply, but must have been awarded their PhD (or the PhD has been unconditionally approved) before **1 August 2022** or the offer will be withdrawn.
6. The applicant must not hold a permanent academic position before the start of the UK IC Postdoctoral Research Fellowship. Probationary or fixed-term lecturers are eligible to apply if the probationary or fixed-term status remains till the start of Research Fellowship.
7. UK IC Postdoctoral Research Fellowships must commence between **1 October 2022** and **1 December 2022.** The duration of a UK IC Postdoctoral Research Fellowship is two years full-time, calculated on a pro-rata basis for part-time awards. Requests for a shorter UK IC Postdoctoral Research Fellowship are not accepted.
8. UK IC Postdoctoral Research Fellows will be employed by the host institution and are required to devote all their working time to the Research Fellowship. The UK IC Postdoctoral Research Fellowship must be the Research Fellow's only source of employment.
9. There are no nationality and age restrictions for applicants. The host institution is responsible for securing all necessary work permits and related costs for the UK IC Postdoctoral Research Fellows.

10. Applicants who have applied to this scheme before and were unsuccessful are eligible to reapply. These applications will be considered as new applications.
11. No security vetting is required as part of the UK IC Postdoctoral Research Fellowship scheme, but by applying to this scheme the applicant is agreeing to be vetted if it becomes necessary during the Research Fellowship. Applicants are asked to declare any reasons why they might not be eligible to work in this area (see Statement of Support and Declaration in the application form). If security vetting is required and the Research Fellow does not meet the security vetting requirement, the UK IC Postdoctoral Research Fellowship award will be withdrawn.
12. Any applications that are incomplete or do not adhere to the guidance will be rejected.
13. Once submitted the application form cannot be edited and updated.

Mentoring and monitoring

The scheme's programme manager will work with each UK IC Postdoctoral Research Fellow to identify an Academy Fellow to be their mentor. The mentor will support and provide independent expert advice throughout the Research Fellowship about research and career development. In addition, UK IC Postdoctoral Research Fellows will be supplied with an Intelligence Community Advisor (IC Advisor), who will advise the awardee and the University Research Advisor on the research project.

UK IC Postdoctoral Research Fellows must submit a progress report every three months throughout the duration of the fellowship as well as an annual report at the end of each year. The reports summarise the research accomplishments during the UK IC Postdoctoral Research Fellowship, including publications, papers presented, conference participation, and other aspects of the research outcomes. A template will be provided for the report. The release of payments is dependent upon the receipt of reports by the Royal Academy of Engineering. In addition, the Research Fellow, Academy representative and mentor will meet annually to discuss the annual report, identify progress being made and make plans. The Research Fellows are responsible for arranging the annual review meetings with their mentors.

The UK IC Postdoctoral Research Fellow will be invited to attend the US Annual IC Academic Research Symposium during the period of the Research Fellowship.

Duration

UK IC Postdoctoral Research Fellowships are for a two-year period with an evaluation after the first year. If the project warrants a third year of research and the Research Fellow, University Research Advisor, and IC Advisor concur, the Research Fellow is required to submit a supplementary research proposal. The proposal should not exceed three pages and must be emailed to the Royal Academy of Engineering no later than 1 January of the second year of research. This submission does not replace the annual reporting requirement. The third-year extensions will be based on the quality of the research proposed and the availability of funding.

How to apply

All applications must be submitted via the Academy's Grants Management System (GMS) https://grants.raeng.org.uk.

All applicants must first register and provide some basic log-in details to create a profile. Before completing the application form, applicants are asked to complete **a Diversity Monitoring Form** to help the Academy monitor and assess its equality, diversity and inclusion policy. The information will be treated as strictly confidential, non-attributable and only reported when collated. It is gathered, stored, and used in compliance with the Academy's Privacy Notice in line with the General Data Protection Regulations 2018. The information will only be used for statistical purposes with access restricted to staff involved in processing and monitoring the data. It will not be seen by anyone involved in any selection processes. No information will be published or used in any way that identifies individuals. The Academy will retain personal information for six years.

The application form has six sections and should take approximately one hour to complete, assuming you have answered the questions offline and merely need to enter the information, rather than compose it. To compose the application in its entirety will take significantly longer.

A summary of the guidance notes is imbedded within GMS. However, the guidance given below is more detailed and recommended.

Many of the questions have prescribed word limits, which are designed to keep answers focused and give applicants an indication of the level of detail required. In such cases the number of words used will be displayed beneath the question and updated in real time.

Applicants can download a pdf of their application after submission, which is recommend for reference. There is only one application stage and those meeting the eligibility criteria will enter the assessment stage.

Completing the application form

After logging in and selecting 'UK IC Postdoctoral Research Fellowships', you should be presented with the 'Instructions' window. Here you will see some general instructions on how to use the system as well as the following sections of the application form:

1. Applicant and institution details
2. Applicant profile
3. Project details
4. Resources requested
5. Statement of support and declaration
6. Marketing

At any stage in the application process you can save your work and return to it later. You can answer the questions in any order you like, so you can freely skip some sections and return to them later. Please read the guidance provided in this document in detail, so you know exactly what is required in each section. You should also ensure that you have all the necessary documentation to complete the application, such as a copy of your CV and supporting letters.

1. Application and institution details

Please provide your name and preferred correspondence details. You should also provide the details of the host university, where the UK IC Postdoctoral Research Fellowship will be held and confirm that this is the 'lead' organisation.

2. Applicant profile

This section requests details as to your suitability and eligibility for the Research Fellowship. You will need to answer some general questions on your experience and upload your CV.

Q. What date was/will your PhD Certificate awarded?

Applicants must have a PhD, which was awarded **no more than five years** prior to the submission deadline **(26 April 2022)**. PhD students are eligible to apply, but must have been awarded their PhD (or their PhD has been unconditionally approved) before **1 August 2022**. Please enter the date your PhD Certificate was awarded or the date your PhD was unconditionally approved by the university. If you have not yet received your PhD, please provide an estimate of when it will be awarded or unconditionally approved.

Q. Extenuating circumstance (optional question)

Should your PhD Certificate have been awarded more than five years prior to the submission deadline (**26 April 2022**), please provide details of the circumstances. Please cover any periods of maternity/paternity leave, extended sick leave, national service, or other activity that you feel should be considered when assessing your eligibility for the UK IC Postdoctoral Research Fellowship. The Academy's decision on eligibility is final.

Q. Do you currently hold a permanent academic position?

Applicants must not hold a permanent academic position before the start of the Research Fellowship.

Q. Applicant's CV

The format and content of your CV is left to your discretion, but should include a list of publications. You may wish to indicate which publications you deem most significant and include a link to any that are open access. You do not need to include contact details as these are included earlier in the application form. **Please also avoid personal information (e.g. gender, date of birth and nationality) in the CV. The CV must be uploaded in a single PDF file, and the file size should be less than 5MB.**

Q. Applicant's most significant achievements

Please describe three to five of your most significant achievements in your research career. We would like to emphasise that all achievements and outputs are welcome and considered valuable to the Academy, not just peer-reviewed publications. Outputs also include, and are not limited to code, patents, spin-out companies, events, public engagement, and policy impact. Please briefly explain the significance of the achievement in a way that will explain it to a researcher from your discipline who may not be familiar with the latest work in the particular field.
500 words maximum

The Academy's research programmes are aligned with the principles of DORA. If research articles published in peer-reviewed journals are to be included in an application, we would therefore like to emphasise that the scientific content of a paper is much more important than publication metrics or the identity of the journal in which it was published.

Q. Impact of COVID-19 (optional question)

The Academy understands that the impact of the coronavirus pandemic on researchers and their work will be varied. If you wish, please provide a summary of how the pandemic has affected your research profile development that reviewers and panel members should consider. Reviewers and panel members will be advised to take into consideration the unequal impacts that COVID-19 related disruptions might have had on individuals.

The impact can include, but is not limited to, the following examples: pause on experiments/research plans, reduced ability to work due to additional caring responsibilities, delays in publishing/submitting a key paper(s) (please note pre-prints can be included in your publications list).
500 words maximum

3. Project details

Q. Research topic

Please select one of the research topics relevant to your application from the drop-down list.

Q. Project title

Enter a title for your research project. This will be used in communications should your application be successful. **Please use no more than ten words** and ensure that it is understandable to a non-specialist reader.

Q. Abstract

Describe the research in terms that can be understood by a non-specialist reader. What similar research is being/has been undertaken nationally and internationally, and how does your project differ.
300 words maximum

Q. Statement of problem

A brief outline of the basic facts of the problem, explain why the problem matters, and pinpoint a solution as quickly and directly as possible.
200 words maximum

Q. Background and relevance to previous work

Sufficient details should be given in this discussion (1) to make clear what the research problem is and exactly what has been accomplished; (2) to give evidence of your own competence in the field; and (3) to show why the previous work needs to be continued.
1000 words maximum

Q. General methodology

Please provide a detailed description of the exact work to be completed. Describe the programme of work, indicating the research to be undertaken and the milestones that can be used to measure progress. Detail the methodology to be used in pursuit of the research and justify this choice. What similar research is being/has been undertaken nationally and internationally, and how does your project differ?
1000 words maximum

Q. Explanation of new or unusual techniques

If you are using any techniques that are not standard in the area of the research proposed, please explain the technique and the rational for using it.
500 words maximum

Q. Expected results and their significance and application

Describe what you expect to get out of the research. It should join the data analysis and possible outcomes to the theory and questions that you have raised. Summarize the significance of the work and proposed applications.
1000 words maximum

Q. Academy's strategic goals (optional question)

How do you align with the Academy's strategic priorities? Note this is not an assessment criterion and is for staff use only. We want to understand the extent to which our programmes as a whole meet our strategic aims, but your answer will not influence the decision and applications are judged purely on merit. The strategic plan is available on our website here.

Select the answer that best describes the strategic aims your research will address:

- Sustainable society
- Inclusive economy
- Both
- Neither

Please give a short explanation for the answer you have selected.
100 words maximum

Q. Diversity and inclusion

The Academy strives to create cultures in which everyone can thrive, and we believe that diverse perspectives enrich our collective performance. What does diversity and inclusion mean to you and your research, and what are you and your team doing to address it? Consider your team, collaborators and universities, the implications on your research design and topic and the overall contribution this will have on your success.
250 words maximum

Q. Literature citations

List the reference material referred to in your proposal. Where possible include web-links to any open access articles, to help reviewers in locating the articles quickly. You may want to highlight the most relevant ones.
1000 words maximum

Q. Images and diagrams

Upload any images and/or diagrams related to your project that add value to your application. You should reference them in your response to the methodology and other questions. **You can upload a single pdf document only**, so collate pages if necessary and ensure you order them in the way you wish them to be viewed.

4. Resources requested

Please see the relevant research grants office at your host institution for assistance with the costs section. The below categories explain what costs should and should not be included in your application. You must be able to demonstrate that the resources requested in this application are justified and appropriate for delivering the proposed research.

Each application is capped at a maximum contribution from the Academy of £200,000 over the two-year period, at 80% of full economic costs.

4.1 Directly incurred costs

1) Staff

The UK IC Postdoctoral Research Fellowship's aim is to support researchers at an early stage of their research career. Salary should be at a level commensurate with skills, responsibilities, expertise, and experience. It is expected that requested salary will be comparable to postdoctoral researcher or early-stage lecturer salary scale points. The Academy reserves the right to provide support at a different level if it is considered appropriate.

The Research Fellow's salary can be requested for a period of two years full time equivalent. Salary increments over the period of the Research Fellowship should be considered in the costs, but possible future pay awards should not be anticipated. Please note that the Academy does not pay inflation and inflation should not be applied to the costs. In addition, the Academy is not able to cover the costs of the apprenticeship levy on research grants. Salary costs do not need to be justified in the 'Justification of costs' section, but are expected to be in line with the starting salaries of early-career researchers.

The UK IC Postdoctoral Research Fellowship may be held on a part-time basis (at no less than 50% of full-time equivalent) if the applicant is to be employed part time. Applicants wishing to hold the award on a part-time basis must state the % time in the 'Justification of costs' section and explain why part-time working is requested. The costs table should be completed as if it will be a two-year full-time research fellowship. This will be adjusted accordingly if the award is offered.

Please note:

- No other staff salaries can be requested as part of a UK IC Postdoctoral Research Fellowship.
- The UK IC Postdoctoral Research Fellowship must be the Research Fellow's only source of employment. The Research Fellows are encouraged to apply for other funding, but these grants should not include any components that require the Research Fellow to reduce their full-time working on the UK IC Postdoctoral Research Fellowship. The grants should not cause any delay and interruption to the completion of the UK IC Postdoctoral Research Fellowship.

2) Travel and subsistence

Travel and subsistence costs can be requested for the Research Fellow only and must be for activities directly related to the research project. Travel costs should be based on the most suitable and economical form of travel. Subsistence costs should reflect the normal rates that apply in the host institution.

Costs for attending national and international conferences (including two visits to the US Annual IC Academic Research Symposium) should also be included where such attendance will directly benefit the research project. Conferences should, as far as possible, be individually identified in the proposal with attendance costs and fees fully justified in the 'Justification of costs' section.

3) Other Costs

Other costs should be specified and justified in the 'Justification of costs' with details provided in terms of their requirement for the research project. Examples include purchase or hire of small items of equipment, computer software licences, laboratory consumables, purchase of specialist publications, publication/printing costs, professional membership subscription fees or

training costs. Unless the need for significant computing power can be justified, the costs requested from the Academy for the purchase of a computer should not exceed £2,000 (including VAT), and no more than one computer should be requested over the duration of the UK IC Postdoctoral Research Fellowship.

Please note: The cost of any single item of equipment, software, database subscription or upgrade to existing equipment, requested from the Academy should not exceed £3,000 (including VAT). Should any piece of equipment include multiple separate items that are purchased individually and then combined to make a single functioning system, the cost of the entire system requested from the Academy should not exceed £3,000 limit.

The Research Fellows are expected to make full use of any equipment, which is already available to them at the host institution and should therefore only request funding for equipment that is necessary and not currently available.

4.2 Directly allocated costs

1) Estates

The Research Fellows may apply for estates costs over the entire duration of the UK IC Postdoctoral Research Fellowship. Please consult with your proposed host institution for guidance as to these costs. Estates costs do not require justification in the 'Justification of costs' section. Where the Research Fellow will be away from the host institution for six months or more in total, estates costs should not be requested for that period. In such situations, this should be confirmed in the 'Justification of costs' section.

2) Other directly allocated

Other directly allocated costs can be requested, calculated on the basis of estimates and should be justified in the 'Justification of costs' section. Potential costs include research/technical staff whose time is shared across several projects and charge out costs for existing equipment, for example access to departmental SEMs and analytical facilities. You cannot request salary costs for specific technicians, but you can request pool technician time costs for the host institution's own facilities, equipment, and staff only.

Costs for major facilities not owned by the host institution, such as those supported by STFC, cannot be requested. If such facilities are required for the project, the applicant should contact the facility in question to determine access requirements. If access to a facility is essential to the research programme and hence the UK IC Postdoctoral Research Fellowship, both access to and external funding for the cost of the facility must be secured within one year of the proposed start date of the UK IC Postdoctoral Research Fellowship.

4.3 Indirect Costs

1) Indirect

Please consult with your host institution for guidance as to these costs. Research Fellows may apply for indirect costs over the entire duration of the UK IC Postdoctoral Research Fellowship. Indirect costs do not require justification in the 'Justification of costs' section. Please refer to the efficiency savings published by RCUK in March 2011 when submitting your figures for indirect costs. Your research office will be able to assist.

Q. Costs table

Applicants must consult the host institution's research grants office to provide advice on the cost elements that are required. The costs for UK IC Postdoctoral Research Fellowship applications must be calculated using the full economic costing model (fEC). **The Academy provides 80% of the fEC for each UK IC Postdoctoral Research Fellowship – up to a maximum of £200,000 for 2 years.** The host institution is expected to provide the remaining from its own funds or other grants. Please ensure that you allow plenty of time for your research office to prepare these costings.

Please note: Some of the cells are auto-calculated and all values submitted should be rounded up to the nearest pound.

Q. Justification of costs

Please provide a descriptive breakdown of the funding requested. Ensure you have adhered to the guidance provided for allowable costs as detailed in this document. The justifications should be a narrative description of what resources are being requested and why. It should include:

- all necessary justifications for costs included in the costs table
- to what extent the equipment requested will be used by other researchers and what equipment you are not requesting funding for (or for which you are requesting funding at a reduced rate) because suitable equipment is already available to you
- what costs will be covered by other sources, for example industry or existing grants, so are not being requested as part of the application
- if relevant, an explanation of why you wish to work part time and at what rate.

500 words maximum

5. Statement of support and declaration

This section seeks confirmation that the applicant has provided accurate information and will update the Academy of any material changes, which may affect the award. It should also confirm that the host institution will support the UK IC Postdoctoral Research Fellowship. You must upload all the additional documentation as per the details below and then tick the box confirming the information provided is correct.

Q. Research Advisor's statement of support

The University Research Advisor must complete a statement in support of the application. The statement should be a maximum of two pages and should confirm that they are willing to act as a Research Advisor for the duration of the UK IC Postdoctoral Research Fellowship.

Q. Research Advisor's CV

The CV must not exceed two pages, and should be submitted as a PDF.

Q. Host institution/university letter of support

The head of department or school, pro-vice-chancellor or dean at the host institution/university must provide a statement in support of the application. The statement should be on headed paper and signed. **The submission deadline will not be extended due to an individual's unavailability.**

The statement **should be a maximum of two pages** and address the following areas:

Suitability of the applicant

- Quality of the applicant's research track record
- Potential of the applicant to become a future leader in their chosen field
- Potential to act as an ambassador and advocate for the research

Support and commitment from the host university

- Alignment of the proposed research fellowship with university research strategy and priorities
- Details of mentoring and resources (e.g. laboratory equipment) that will be provided to the candidate, should the application be successful
- Other university activities (e.g. teaching, committees, etc.) the candidate will be expected to undertake
- Detail of the career development support that the applicant will be offered
- Details of how your institution adopts a proactive approach in encouraging researchers from underrepresented groups in engineering, especially women, to apply
- Evidence of your commitment to equality and diversity

Impact of COVID-19 on the host university's support

The host university can use this letter of support to highlight the impact of the coronavirus pandemic on their support for the UK IC Postdoctoral Research Fellowship if they wish. Reviewers and panel members will be advised to take into consideration the unequal impacts that COVID-19 related disruptions might have on the host university's support for the Research Fellowship.

The Academy and the Government Office for Science expect the host institutions to be committed to and provide support that aligns with principles set out in The Concordat to Support the Career Development of Researchers and The Concordat for Engaging the Public with Research, and DORA.

Q. Host institution/university declaration

The declaration from the applicant's host institution/university should be completed by an appropriate officer/position from the central research grants office or equivalent. The letter should be on headed paper and should carry the signatory's name and position and the institution/university's official stamp (if applicable). The purpose is to check that the university is in principle willing to host a Research Fellow, subject to contract. The letter must confirm the application has been approved by the institution/university and **must contain the exact wording given in the box below**, as well as any further remarks the university wishes to make. **The submission deadline will not be extended due to an individual's unavailability.**

On behalf of the institution/university I can confirm that I have read and accept the application guidance and other information regarding this award scheme, which is provided on the website of the Royal Academy of Engineering. I also confirm that:

- The costs submitted in the application are correct and sufficient to complete the project as envisaged. Any shortfall in funding discovered after the award has been made will be covered by the university, potentially through other grants.
- The applicant will be employed by the university for the duration of the award.
- If awarded, the applicant will be given full access to the facilities, equipment, personnel, and funding as required by the application.
- The applicant's teaching and administrative duties will be restricted to enable them to dedicate their time to research.
- We are aware that the UK IC Postdoctoral Research Fellowships scheme has non-standard intellectual property rights (IPR) conditions relating to or resulting from the proposed research. If proposal is recommended for funding, we will be ready to assess the IPR conditions in the offered award contract.
- I am authorised to approve the submission of applications for funding and this application has successfully met all our internal approval procedures.

Q. Other support letters (optional)

Other letters of support must:

- be on headed paper and clearly state who they are from
- be from external collaborators i.e., people and organisations NOT working at the host institution and its affiliates
- be signed
- confirm that the author knows the applicant
- explain why they are interested in the project
- provide details on what form the collaboration will take.
- clearly demonstrates the nature of the collaboration and how it will be beneficial to the applicant and the project
- **be no more than two pages.**

As reviewers are asked to assess these alongside your plans for collaboration, aim for quality over quantity and keep the letters short and concise to better enable the reviewer to identify the salient information. A bullet-point list of contributions is a highly effective method of making the reviewers' role easier.

Please ensure the letters of support are collated and submitted in a single PDF document.

Q. Applicant declaration Part 1

No security vetting is required as part of the UK IC Postdoctoral Research Fellowship scheme, but by applying to this scheme you are agreeing to be vetted if it becomes necessary during the Research Fellowship. Please declare any reasons why you might not be eligible to work in this area. If security vetting is required and the Research Fellow does not meet the security vetting requirement, the UK IC Postdoctoral Research Fellowship award will be withdrawn.

Q. Applicant declaration Part 2

Please complete with your full name and position once you have read and understood the declaration written in the application form.

6. Marketing

This section is optional, but helps the Academy to understand which of our marketing materials are most successful at reaching the academic community and helps us to improve our future communications work.

Once the entire application form is completed, a **'submit application'** button will become available. Please note that once submitted the application cannot be edited, but you may log-in to view it from your GMS account. You may also want to print a copy of the application for your record.

Assessment process and criteria

The scheme has one-stage assessment process. Applications will be assessed by a review panel consisting of the UK government intelligence, security, and defence community members (under the auspices of the Government Office for Science) and Academy Fellows. The panel will provide comments against each of the following assessment criteria, the overall quality of the application and make a recommendation on whether the applicant should be funded:

1. **Candidate**
   Quality of the applicant's research track record
2. **Research quality and vision**
   Quality of the applicant's research vision and novelty of the approach to the chosen research topic
3. **Impact**
   The potential contribution of the research to the UK government intelligence, security, and defence community
4. **Research environment**
   Quality and level of the host institution/university's support and commitment to the research fellow's research project and their career development

Declaration on Research Assessment (DORA)

The Academy's research programmes are aligned with DORA, which is a set of principles aiming to improve the ways in which the output of research is evaluated by funding agencies, academic institutions, and other parties. The outputs from research are many and varied, and as a funder of engineering research the Academy needs to assess the quality and impact of these outputs in order to make awards. It is imperative that research output is measured accurately and evaluated wisely.

In the assessment of research output, we would like to emphasise that all outputs are welcome and considered valuable to the Academy. Outputs can include open data sets, software, publications, commercial, entrepreneurial, or industrial products, clinical practice developments, educational products, policy publications, evidence synthesis pieces, and conference publications. With regard to research articles published in peer-reviewed journals, the scientific content of a paper is much more important than publication metrics or the identity of the journal in which it was published.

We value and appreciate the time and effort that reviewers give to support our research programmes. A good, helpful review for the Academy is one that assesses research on its own merits rather than by surrogate measures, such as on the basis of the journal in which research is published.

For all queries please contact the Royal Academy of Engineering's research programmes team at research@raeng.org.uk

Research topics 2022

Topic 1	**The Internet of Space Things using commercial grade radios**
Topic 2	**Nanotechnology implications for chemical and biological warfare safeguards**
Topic 3	**Prospects for machine learning to ascribe motivation**
Topic 4	**Machine led discovery of electrically functional materials for additively manufactured and printed electronics**
Topic 5	**Protect individuals and our workspaces from acoustic compromise through the identification of threats and countermeasures**
Topic 6	**Conceptualisation of swarm or team robots for autonomous tunnelling**
Topic 7	**Characterisation and source mapping of 3D printed materials through materials analysis**
Topic 8	**Uncovering insights into locations using geosocial data**
Topic 9	**Cloud data security – a dynamic forensic analysis**
Topic 10	**Threat model considerations in systems that use neural networks at the edge**
Topic 11	**Responsive access to low-Earth orbit**
Topic 12	**Characterising the impact and detection of microbiome/microbiota modifications**
Topic 13	**Characterising the impact and detection of synthetic monomers to product semi-synthetic biological products**
Topic 14	**Low shot training and testing of machine learning algorithms for detection of Items of concern**
Topic 15	**The cybersecurity of complex adaptive systems**
Topic 16	**Exploration and exploitation of artificial light: an opportunity or security risk?**
Topic 17	**Detecting anomalous small-scale seismic events**
Topic 18	**Data analysis for national security using artificial neural nets implemented on quantum annealing processors**

Topic 1
The Internet of Space Things using commercial grade radios

Key Words: cybersecurity, cubesat, LEO, IoT, IoST, waveform, coding

Research Topic Description, including Problem Statement:

Space is a new domain for the Internet of Things. Internet of Space Things systems integrate ground-based nodes with space-based infrastructure and terrestrial broadband backhaul. Several UK-based service providers are poised to launch services. However, the IC is interested in understanding the trade offs needed to design Internet of Space Things (IoST) systems for distributed ground sensors including command and control in circumstances where the very best performance can be achieved with the least commitment of power both on the ground and in orbit. At the same time, development and operating costs need to be kept to a minimum.

For this reason, the IC is interested in defining the design criteria for two-way LEO satellite communications using readily available radio chipsets where power, weight and size are all constrained.

Aspects to be taken into account include:

- On-air waveform efficiency and Ionospheric penetration (taking into account Total Electron Content (TEC) variations, angle of incidence, and space weather phenomena)
- Coding schemes for power efficiency, range and operation at extremely low SNR assuming maximum achievable bandwidth is always wanted
- Design implications for encryption schemes. Some work has been done in this topic and is in the public domain on the space-ground down link. This project will explore the ground-space up link, and also combine the paths two to show how efficient and effective two-way communications using short datagrams can be designed. Reciprocity over the paths is not assumed.

Key outcomes are:

- A parameter sensitivity analysis for waveform and coding schemes using suitable readily available radio chipsets that explores the compromise between link performance and power commitment.
- Link budget calculations and expected achievable bandwidths assuming a 500 - 2500km range to the satellite, maximum RF power levels <30dBm, and constrained antenna gains at both ends. A variety of ISM and allocated satellite bands should be included.
- Identification of performance limitations as a result of variations in Total Electron Content (TEC) in the Ionosphere, polarization effects, angle of incidence (elevation), and doppler constraints (assuming LEO satellites).
- Practical terrestrial experiments that confirm key aspects of theoretical modelling.

Example Approaches:

Long Range (LoRa) is a popular choice for the one-way space-ground link with several choices of parameters and waveforms in use by operators (tinygs.com). The LoRa signal is tolerant of the magnitude of doppler shift encountered in LEO satellites. It is possible to use the cyclic redundancy check (CRC) to plot a Receiver Operating Characteristic (ROC) curve for LoRa datagrams received on the ground. However, this may be misleading as it relies on a linear relationship between SNR and decode success – this is clearly not the case as the signal processing is non-linear. Also, the up link path (ground-space) is not taken into account, and there is no guarantee of reciprocity. So alternative performance criteria are needed.

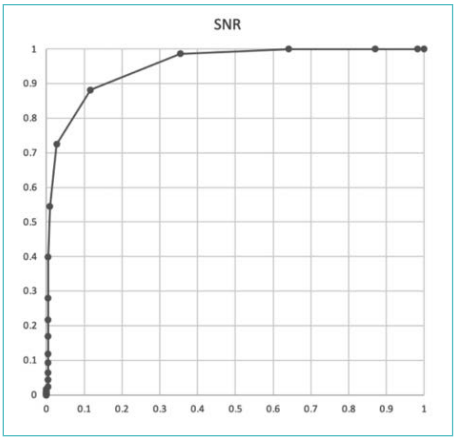


Figure 1:

ROC curve drawn for space-ground link for Norby satellite (LoRa SF=10, CR=5, BW=250kHz) on 436.703MHz

A variety of chipsets are available ranging from ultra-narrowband ultra-low data rate through to broadband burst transmissions. This repertoire needs to be systematically evaluated.

Topic 2
Nanotechnology implications for chemical and biological warfare safeguards

Key Words: chemical, biological, warfare, CBW, nanotechnology, emerging threats, nanoengineering, pharmacology, countermeasures, proliferation

Research Topic Description, including Problem Statement:

Nanotechnology involves the manipulation and engineering of nanoscale materials to exploit special properties and enable new applications. While such applications may be of benefit in delivering new solutions to global healthcare, agriculture, manufacturing, and environmental challenges, there is a possibility of nanotechnology also expanding the pool of biological and chemical agents of concern. Some applications of nanomaterials may generate new threat agents, improve agent delivery methods or increase the threat from known agents. These new or redesigned threats will require proactive development of new countermeasures and new detection, identification and monitoring systems.

Applicants should approach the topic with the intent of including literature review and analysis of nanotechnology applications and trends with respect to potential chemical or biological warfare impacts.

Example Approaches:

Research proposals could approach this issue from a variety of disciplines, or as a cross-disciplinary effort. The problem touches on aspects of chemistry, engineering, applied science, innovation policy, and pharmacology. Proposals could consider the both the potential utility of nanotechnology to enhance or change chemical warfare and biological warfare agents, and ways to monitor and mitigate nanomaterial enabled threats:

- themselves as highly toxic chemical and biological warfare agents;
- to enhance or change the delivery or effects of chemical and biological warfare agents;
- to enhance or reduce the effectiveness of detection, protection or medical countermeasures against chemical and biological warfare agents; and
- to encapsulate chemical agents in order to enhance their environmental persistence, facilitate transportation or to regulate their delivery or effects.

Other avenues of investigation include:

- alternative pathways to converge existing Chemical Biological Warfare threats with nanotechnology;
- the development and proliferation of tools with which to manipulate, utilise and produce nanotechnology;
- coverage of nanotechnology by current arms control treaties such as the Chemical Weapons Convention and the Biological Weapons Convention;
- deficiencies or potential gaps in current domestic and international policy surrounding nanotechnology in relation to research & development that could encroach on the CBW threat environment; and
- potential applications of nanotechnology in terms of detection, protection or medical countermeasures against chemical and biological warfare agents.

Topic 3
Prospects for machine learning to ascribe motivation

Key Words: literary studies, motivation, narrative constructs, machine learning, deceit detection

Research Topic Description, including Problem Statement:

Significant work has been done on machine learning (ML) for facial recognition to detect emotion. But can a ML system recognize emotional markers in text, particularly in order to distinguish sensational or provocative text from other styles of writing? Can types of language reliably indicate textual intensities such that ML systems can be developed to grasp the connotative effects of language?

What are the prospects for ML to use abductive methods (theorised by Charles Sanders Pierce, in AI contexts by Reza Negarestani) or extrapolated volition (e.g. Eliezer Yudkowsky's theories) to offer insights about persuasive narratives? Abduction is useful because it has the capacity to extend reasoning not only through deviations from norms, but also through deviations from expectations, e.g. a text may deviate from a truthful stylistic paradigm, but this in no way contradicts the expectation of that text, for instance, if we know it comes from a satirical website. Approaches to
detect deceit could potentially inform understanding and characterisation of motivations behind observed effects.

Example Approaches:

This project explores humanities fields, models and theories with respect to ML capabilities and potentials.

Possible approaches include:

- Consider textual markers of narrative crisis and whether ML can use values to explore factual or probable conclusions.
- A key ML research challenge is getting a system to learn what you mean rather than exactly to what you say. What are the prospects for ML systems to use abductive methods or emerging work on volition and alignment to offer insights about persuasive narratives?
- What disciplinary constellations might ML utilise to grasp motivation, for persuasive narrative or deceit detection?
- How might advances in alignment theory contribute to the way ML might discover expectations in texts?
- Is there a prospect for an approach that would enable ML to designate possible value systems informing text or texts, or linking texts or media?
- Could a motivation sensitive ML system detect actors in concert or recognise commonly motivated patterns?

Subsequent research might build and test potential ML applications based on the outcomes of this topic, i.e. ML development is not within scope of this topic.

Topic 4
Machine led discovery of electrically functional materials for additively manufactured and printed electronics

Key Words: electrically functional adhesives, electrically functional inks, electrically functional materials, machine learning, artificial intelligence, neural networks, AME, Additive manufactured electronics. PCBs, printed circuit boards, 3D electronics, printed electronics, roll to roll, adhesive, ink, electronic material, resistor, resistivity, capacitor, capacitance, semiconductor, inductance. Inductor, magnetic, ferroelectric, conductor, conductivity, piezoelectric, piezoelectricity, photovoltaic, solar, electromagnetic, thermoelectric, triboelectric, antennas, power harvesting, RFID, flexible electronics, wearable electronics

Research Topic Description, including Problem Statement:

Additively manufactured electronics, printed electronics, 3D electronics, flexible electronics and wearable electronics is a fast-growing market. It permits a move away from the wet chemistry processes which are energy intensive, labour intensive, plant equipment intensive, uses hazardous chemicals and produces significant waste streams with associated environmental disposal concerns.

This topic is focused on electrically functional materials which are required for fabricating a wide range of products cheaply and quickly with considerable geometrical complexity at low production quantities. These electrically functional materials are required in several forms such as printable adhesives, printable inks or as bulk printable material, and must be capable of being printed using commonly available commercial process equipment such as UV Objet, Dragonfly, aerosol jet and piezoelectric nozzles etc.

The current generation of printable electrically functional materials have several issues:

- Currently in the commercial market there are very few printable electrically conducting adhesives, conducting inks or dielectric inks that can match the electrical, thermal and mechanical performance of conventional metallurgical solders or bulk materials.
- Very few electrically functional inks can match the performance of or replace conventional surface mount passive components (such as resistors, capacitors and inductors) and be capable of being cured or sintered using typical processes such as UV lamps or IR heat sources commonly found on AM/AME printing equipment.

Thus it is challenging to move away from using wet chemistry-based PCB fabrication, SMD components and the associated common bonding processes such as solder reflow.

To investigate new adhesives, inks and materials would take too long using conventional materials sciences in terms of discovery, screening, time consuming & labour intensive. The materials science space is too large & difficult to navigate quickly and efficiently.

The aim of this research topic is to encourage proposal submissions that use machine learning, artificial intelligence, neural networks and any other computational technique(s) to rapidly accelerate the discovery of candidate adhesives, inks and materials. The promising materials would then need to be screened to produce a shortlist of viable electrically functional materials.

Example Approaches:

- Focus on the fundamentals of improving printable electrically functional materials such that their performance is nominally similar as that encountered in conventional assembled PCBs for a wide range of electrical, mechanical, thermal, and bonding properties.
- Focus on reducing the time and effort required to identify and screen potential candidate materials while keeping an eye on its compatibility with existing processes commonly found within AM & AME printers.
- The author is materials class agnostic, so it is acceptable to search for materials that are electrically conductive but are not metallurgical but have similar electrical properties to that of bulk copper, silver or gold for example but can be printed and cured/sintered using existing curing/sintering processes commonly found in AM & AME printers. Similarly, when looking for high dielectric constant materials, are there any others that are better than barium titanate, it does not need to be restricted to ceramics only.
- Develop a computational framework and materials dataset to aid future down selection of printable electrically functional materials.

Topic 5
Protect individuals and our workspaces from acoustic compromise through the identification of threats and countermeasures

Key Words: acoustics, ultrasound, infrasound, directional speakers, acoustic disruption, 'MSVE'

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 regard 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 regard 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 work spaces.

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.

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.

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.

Topic 6
Conceptualisation of swarm or team robots for autonomous tunnelling

Key Words: swarm, robotics, autonomy, tunneling, excavation, mining, AI, underground, subterranean, coordination, navigation, GPS denied, simulated robotics, small scale robotics, transport, task optimization.

Research Topic Description, including Problem Statement:

Subterranean excavation is a dangerous, labour intensive, and time-consuming task. We want to develop ways of mitigating these issues by replacing humans with a multi-unit system of robots that improves reliability and efficiency through redundancy. This system can be a swarm of identical robots, majority identical with several "leaders", or groups of task specific ones. The system may consist of a true swarm of autonomous agent robots or semi-autonomous agents that are directed by a few leaders or a centralized computer. At the end of this effort the post-doc will submit a report detailing one or more potential robotic excavation systems.

The study will need to address three primary phases of operation. The system will need to excavate soil, transport the soil down the length of the tunnel, and then install some structure to shore (strengthen with some rigid liner/structural element) to make the tunnel stable for use. This theoretical system should meet the following requirements with the assumption that the excavation will be only horizontal and in ideal soil with good stand-up:

- Capable of excavating >50 feet
- Autonomous or semi-autonomous operation with all user interface outside the tunnel
- Individual robots be portable (<50 pounds each)
- Robots able to maintain tunnel axis within 9" at 50'
- Minimal on-site servicing
- Excavate at least 1 foot per hour of smallest cross-sectional area achievable
- Simple and rugged controls
- Persistent power without umbilical's if possible

Several key challenges will need to be addressed. The robots will need sufficient bracing force to be able to dig into naturally compacted soil, though it does not need to account for solid rock, gravel, or flowing sand. The robots must remain portable but be capable of transiting the tunnel multiple times and/or excavate significant amounts of soil without stopping the excavation process via coordinated recharging, swappable batteries, or some other method. Their design should be simplified enough that non-expert users can affect repairs and maintenance.

Example Approaches:

The investigator may take one of three potential avenues:

- Utilize market surveys, subject matter expert input, and/or simulated robotic systems to conceptualize a swarm excavation system.
- Alternatively, robots (at scale or nominal size) could be constructed to empirically demonstrate a viable system. These robots need only demonstrate the mechanical functions, they could be manually controlled via wires – swarm communications are not required for an initial demonstration.
- Another method of the investigator's design that they believe will meet the needs of the proposal.

Topic 7
Characterisation and source mapping of 3D printed materials through materials analysis

Key Words: 3D printed materials, 3D printer, materials analysis, analytical chemistry, X-Ray Diffractometer (XRD), X-Ray Fluorescence (XRF), Scanning Electron Microscope (SEM), Gas Chromatograph Mass Selective Detector (GCMSD), Raman, FTIR, Nuclear Magnetic Resonance Spectroscopy (NMR), forensics

Research Topic Description, including Problem Statement:

As 3D printers and 3D printed materials become cheaper, the potential for illicit supplies created by 3D printers is increased. Items created by 3D printers are not traceable by law enforcement agencies and can be a cost-effective way to bypass security designed to prevent transport of illicit items. 3D printers have the potential to create firearms, firearm accessories, weapons, pharmaceuticals, physical keys to secure locations, lockpicking tools, false latent prints used to bypass biometric security, skimmer components, and counterfeit currency. As more materials become available for 3D printing, the potential for illicit use becomes greater.

There is a growing demand for forensic examination of 3D printers and 3D printed materials. Due to the recent availability of this technology to the general public, there is a lack of research and validated test procedure that can be used for forensic examination. The goal of research associated with this topic should focus on materials analysis of 3D printed materials to associate with a brand/manufacturer or even a specific 3D printer.

Example Approaches:

Analytical Chemistry techniques such as X-ray diffractometer (XRD), X-ray Fluorescence (XRF), Scanning Electron Microscope (SEM), Gas Chromatograph Mass Selective Detector (GCMSD), Raman, FTIR, and Nuclear Magnetic Resonance Spectroscopy (NMR) can provide great detail concerning primary and trace components used in manufacturing of a specific item. Additionally, classic forensic techniques such as tool marks could provide valuable information that can characterize 3D printed material.

Use cases for 3D printed materials for nefarious purposes are generally increasing. Developing forensic techniques to identify source of production, supply chains, and prosecute individuals engaged in criminal activity will greatly enhance investigations in the Secret Service, Intelligence Community, and Law Enforcement agencies.

Topic 8
Uncovering insights into locations using geosocial data

Key Words: data mining, LBSN (Location-Based Social Networks), geosocial patterns, NLP (Natural Language Processing), social media, geotagging, machine learning, artificial intelligence

Research Topic Description, including Problem Statement:

The fusion of GPS-equipped mobile devices with online social networking platforms has given rise to location-based social networks (LBSNs). These networks allow users to share their location, activities, and thoughts in real-time. This is a rich and largely untapped source of data that has several application domains with potential for solving a range of crucial problems. In particular, this data provides opportunities for research into three main aspects of human mobility: geographic movement (locations visited), temporal dynamics (periodicity of movement), and social networks (evolution of relationships).

An analysis of all these aspects may provide interesting societal patterns as well as insights into how spaces are used and evolve over time. The purpose of this research is to develop techniques to accurately label location usage and building types leveraging only geosocial data derived from LBSNs. Potential other areas of exploration include developing predictive methods of geographic movement by leveraging historical regional geosocial data.

Example Approaches:

The proposed research should seek to identify location usage and building types through the lens of geosocial data derived from LBSNs. Applicants are encouraged to explore diverse methodologies that draw upon different areas of data science and data mining including machine learning, natural language processing, and graph theory. The approach should allow for the incorporation of LBSN data from multiple platforms.

Topic 9
Cloud data security – a dynamic forensic analysis

Key Words: cloud, cloud computing, independent verification, security, data, assurance, confidentiality, integrity, authenticity, machine learning, artificial intelligence, forensics

Research Topic Description, including Problem Statement:

Cloud computing has become integral to everyday life, but there are also vulnerabilities of concern to the IC. Cloud technology is predicated on seamless re-use of resources – compute, memory, disk etc., which can lead to questions regarding what happens to data after you think it is deleted, who else can access your data when on/sent to Cloud resources, and what is accessible in memory from previous use of resources?

Cloud platform security is typically measured using industry standards at snapshots in time, but these are not always sufficient to answer: "How much do we trust Cloud providers with our data, today?".

This topic should aim to metricise trust in Cloud data security, dynamically and independently, on the major Cloud platforms including AWS, Azure and GCP. Current assessment tools provide assurance at a snapshot in time; what is required is a way of being able to continuously forensically analyse this facet of security.

Example Approaches:

- Developing a framework and associated tools to independently and dynamically assess security of data (Confidentiality, Integrity, Authenticity) on the major Cloud platforms (for example AWS, Azure and GCP), in order to create metrics around confidence level of data security.
- Create and deliver a tool/framework that can analyse data residue and accessibility on Cloud resources, at-rest and in-transit, together with relevant dashboards.
- Develop a metric system of trust in major Cloud platforms (potentially down to individual service level), together with a dashboard to present this historically.

Topic 10
Threat model considerations in systems that use neural networks at the edge

Key Words: cybersecurity, neural networks, edge, IoT, machine learning

Research Topic Description, including Problem Statement:

With machine learning advances in hardware and software being powered by strong commercial interest and consumer awareness of data security/privacy it is becoming more practical to deploy trained models to the edge of a system on low power devices to filter information, make decisions and provide context to data before it is aggregated on back-end systems.

Neural networks are benefiting from advances in core principles, software libraries and optimized hardware to run them making an eco-system that is moving quickly but still relatively immature in terms of its success deploying solutions to "production".

There is a major cyber security concern around neural networks, presenting the question, what are the cyber security risks of using neural networks at the edge of a system? I.e., Could a nefarious adversary affect a system that has a neural network as a component, either to defeat, deceive or coerce the system?

Other thoughts for steer are:

- What attack vectors could an adversary use in a neural network on an edge device?
- We consider "edge" devices to be low power sensors to small servers with a preference for the sensor end, potentially with specific hardware optimised for running neural networks (TPUs, GPUs, FPGAs, Neuromorphic chips).
- Consider what information may change an adversary's approach, e.g., if they knew the hardware, firmware, software, model deployed, training dataset, validation dataset etc.

Example Approaches:

One approach could be to consider the neural network as an isolated "black box" component and how the inputs could be affected in a way that is imperceptible to human eyes, there is previous work in this field of deceiving neural networks and in some ways the approach can be considered similar to a GAN based approach trying to create one network that can fool another.

Related to the previous approach would be the "white box" method where the attacker knows the internals of the neural network and focuses on replacing/changing the network to alter its outputs while maintaining enough of its behaviour to limit detection.

Another approach would be to consider an attacker using specialized hardware that may be used to run inference on and how that could be interfered with to affect the performance of the system.

CPU security has received some attention and improvement with issues like Spectre and Meltdown receiving media attention. Attacks focused on information leaking during transfer (see: https://ieeexplore.ieee.org/document/8715004) in CPUs are common but are TPUs different? How about neural networks deployed to FPGAs?

Will neuromorphic hardware be free from those issues given it doesn't separate memory and storage or will it have a new set of unique issues?

When systems contain sensors without processing at the edge security often focuses on validating the input signals, establishing trust in the hardware/software and looking for "normal" data being received based on historic data. Are there opportunities to build consensus between sensors on events when they can all apply context and describe the event e.g., a person is there because I can see them and hear them? – Can this be used to increase trust in the individual devices and spot disruption?

Topic 11
Responsive access to low-Earth orbit

Key Words: flexible launch capability, resilience, spaceflight services, low cost to orbit, spaceflight, low-Earth orbit (LEO), nanosatellites, CubeSat

Research Topic Description, including Problem Statement:

Nanosatellites (<10kg), including CubeSat constellations, offer rapid revisit times for Earth observation, provide communications options in remote areas, and serve as a baseline platform for technology demonstration. However, an individual nanosatellite may have to wait up to 24 months for a suitable launch opportunity as a secondary payload on a commercial carrier vehicle. A more responsive launch option, to carry out dedicated nanosatellite launches for rapid response to emerging security challenges, constellation repair, or urgent technology demonstration, would add value to these assets. The recent Integrated Review echoes this, noting the need for "greater … flexibility in terms of what the UK puts into space, and when." It is likely that USA and AUS have similar requirements for a novel nanolaunch option.

However, the minimum mass of a commercial carrier vehicle, even with horizontal launch, is not less than several tonnes. This is because, as payloads get smaller, the dry mass of the launch vehicle begins to dominate. Therefore, a nanolauncher must be mechanically simple, to minimise dry mass; and it must produce the highest possible specific impulse, Isp, to compensate for this scaled mass penalty. This indicates high-performance cryogenic propellants stored in tanks that, in turn, become ever less mass-efficient as the size of the vehicle is reduced.

Designing a launch vehicle for payloads in the 1kg range is therefore inefficient, using conventional architectures, and an effective low-cost option for dedicated nanosatellite launch currently does not exist. A method for providing a responsive, low-cost launch solution for small payloads would greatly increase UK access to low-earth orbit. The activity would have potential applications to propulsion technology in other defence domains as well.

This research topic aims to examine medium term options for dedicated nanosatellite insertion. The focus will be on systems that could be deployed from UK spaceports or platforms, using novel techniques to reduce the dry mass of a small launch vehicle – a nanolauncher – to an absolute minimum.

Example Approaches:

Proposals will seek to minimise dry mass by evaluating novel rocket architectures, such as caseless or autophage architectures, launch conditions e.g. air launched systems, and examine if Isp can be increased using novel techniques such as rotating detonation engines. Demonstrated hot-fire testing of the solutions proposed is considered to be a desirable aspect of any development under this topic to meet the medium term timescale.

Initial research in this area has produced a number of feasible options in the pipeline including: miniature rotating detonation engines, hybrid autophage engines and meso reusable rockets.

Topic 12
Characterising the impact and detection of microbiome/microbiota modifications

Key Words: microbiome, microbiota, biosecurity, detection, attribution, disease

Research Topic Description, including Problem Statement:

The links between changes to the human gut microbiota, the expression of genes in the gut and health and disease have become increasingly apparent in the 21st century, with a range of complex diseases such as cancer and autoimmune diseases linked to aberrant changes to the gut microbiome. With these changes, the value in understanding the phenotype of microorganisms expressed in the gut, how gene expression is regulated and the pathways they use to signal changes to the rest of the body have become of increasing interest.

With changes to the human microbiome/microbiota implicated in the initiation and facilitation of disease progression, an ongoing area of research is how the microbiome could be modified to reduce the risk of disease development. However conversely, this also presents a biosecurity risk that the human microbiome could be accidentally or deliberately modified to cause disease within a given individual, with beneficial research leveraged nefariously to cause intended effects. The biosecurity risks related to this growing area of research are poorly understood, including the potential range of impacts that might occur following changes to the microbiome. A better understanding of the risks is necessary to support defense by being able to detect when changes have occurred, if they are natural, accidental or deliberate, and if necessary, attribute any changes.

This proposal seeks to further characterise the potential causes of microbiome changes and understand the range of impacts that could be triggered following microbiome changes in order to support mitigations, detection and if necessary attribution.

Example Approaches:

A possible approach may include:

- Reviewing and exploring existing and novel microbiome research to characterise the range of possible effects and impacts that could occur following changes to the human microbiome;
- Characterising how changes to the microbiome can be directly linked to physiological changes;
- Characterising the differences between natural and deliberate microbiome changes, including signatures and phenotypic markers of natural and deliberate changes to support detection;
- Developing a set of criteria or detection frameworks/assays including required capabilities to identify when microbiome modifications have taken place.

Topic 13
Characterising the impact and detection of synthetic monomers to product semi-synthetic biological products

Key Words: monomers, nucleotides, amino acids, semi-synthetic Organisms, DNA, proteins, synthetic biology, pathogens, toxins, detection

Research Topic Description, including Problem Statement:

Genetic material and proteins can be synthesized using synthetic biological monomers which are not found in the natural world. These can elicit significant structural and functional changes, with the potential for phenotypic consequences in organisms. Semi-synthetic organisms have already been generated incorporating synthetic nucleotides – E.coli using synthetic base pairs have been generated and have been shown to replicate, engineered using synthetic biology techniques. Synthetic or unnatural amino acids with novel characteristics have also been incorporated in protein engineering, with incorporation of unnatural amino acids demonstrated in both prokaryotic and eukaryotic cells, generating proteins with novel biochemical properties.

The ability to generate new forms of life using synthetic monomers could enable organisms to take on modified or new characteristics, including novel harmful effects or increased pathogenicity. Similarly, the incorporation of unnational amino acids into protein structures may allow the development of modified or novel toxins with enhanced or varied effects, such as increased toxicity. These applications for non-natural biological components could therefore present a biosecurity risk that is currently poorly understood.

Changes to fundamental biological building blocks and their incorporation into genetic or protein sequences may also have consequences for detection, whereby the success of current detection technologies are contingent on the recognition of naturally occurring microorganisms or sequences. Unnatural or synthetic components may bypass detection technologies, enabling their existence and impacts challenging to identify and attribute.

In order to address and mitigate these biosecurity risks, this proposal seeks to characterise the potential range of physiological impacts of biological materials and microorganisms comprised of synthetic monomers and better understand the impacts on the utility of current detection technologies, to support future detection and attribution capabilities.

Example Approaches:

A possible approach may include:

- Reviewing and exploring existing and novel research on unnatural and synthetic biological monomers to characterise how their incorporation into biological components and systems to generate semi-synthetic products (from molecules to microorganisms) can lead to changes in properties and structure/function relationships. This might include:

- Developing a method for determining structure/function relationships of semi-synthetic products;
- Understanding how semi-synthetic products have different characteristics compared to naturally occurring products such as increased environmental persistence or resistance to medical countermeasures; enhancement of existing effects; introduction of new targets, mechanisms of action and subsequent effects;
- Characterising how functional changes of semi-synthetic products can result in changes to physiological effects;
- Mapping and testing the ability of existing biodetection technologies to identify semi-synthetic products e.g. if existing/emerging sequencing technologies remain functional for semi-synthetic products;
- Developing novel detection frameworks and technologies to identify semi-synthetic products;

Topic 14
Low shot training and testing of machine learning algorithms for detection of items of concern

Key Words: machine learning, X-Ray screening, artificial intelligence, low shot learning, low shot testing, synthetic imagery

Research Topic Description, including Problem Statement:

- X-Ray scanners are deployed for security screening of bags at various security checkpoints: in airports, other transport hubs, and at critical national infrastructure.
- There is a great interest to assess the effectiveness of machine learning (ML) algorithms deployed on X-Ray scanners to detect concealed items of concerns.
- To date, it has been considered that a large number and variety of images are required to train a ML algorithm for effective threat detection. However, it may not be possible to provide a large image set of items of concern to developers. Therefore, it is of importance to be able to develop effective ML algorithms using a small number of training images – termed low shot training.
- It is also of interest to explore the feasibility of independently testing an algorithm with a small test set of images, termed low shot testing.
- A further option to overcome difficulties with provision of large image sets of images of concern, is to assess the effectiveness of using synthetic imagery.

Example Approaches:

- A small training set of images of items of concern will be provided (open format, not security classified) to the postdoc to be used to develop a low shot trained detection algorithm. A small test set of images will be provided to be used to test the algorithm. A large data set of related images will be provided to train and test an algorithm with a conventional supervised learning approach.
  A comparison is to be made of the low shot learning approach and the supervised learning approach using the large data set. Similarly, a comparison is to be made of the low shot testing approach with testing using the large test set.
- Based on the provided images for items of concern, the postdoc will create synthetic images and develop a study to compare the effectiveness of synthetic images, real images, and a combination of both.
- Combine the approaches of low shot learning and synthetic imagery to assess the most effective way to train a ML algorithm for items of concern in the absence of large data sets.

Topic 15
The cybersecurity of complex adaptive systems

Key Words: cybersecurity, complex systems, general systems theory, cybernetics

Research Topic Description, including Problem Statement:

As edge computing increases support for AI and machine learning in network devices, we expect future cyber-physical systems to grow in complexity and autonomy, and to work in collectives to achieve the scale required for large-scale cyber-ecosystems (such as in smart buildings, connected places, transport/logistics networks, energy distribution, and other critical national infrastructure).

This could result in swarm engineering, or the use of Popperian intelligent agents having an internal model (or representation) of their situation, performance and attainment towards a goal. In either case, there is the potential for new classes of cyber vulnerability based on coercion or deception by an attacker. In addition, we forecast that large-scale collectives of cyber physical systems will increasingly behave as complex systems (CS), or complex adaptive systems (CAS) if learning and/or feedback is present. This too creates new classes of cyber-vulnerability, through the existence of level-points, phase transitions, bifurcation phenomena, percolation phenomena, and other system-wide phenomena new to us. These possibilities therefore need to be understood and prepared for.

A state-based approach has been suggested (Bramson, 2019 [1]) – in which the status and dynamics of the CAS can be represented in the form of a graph.

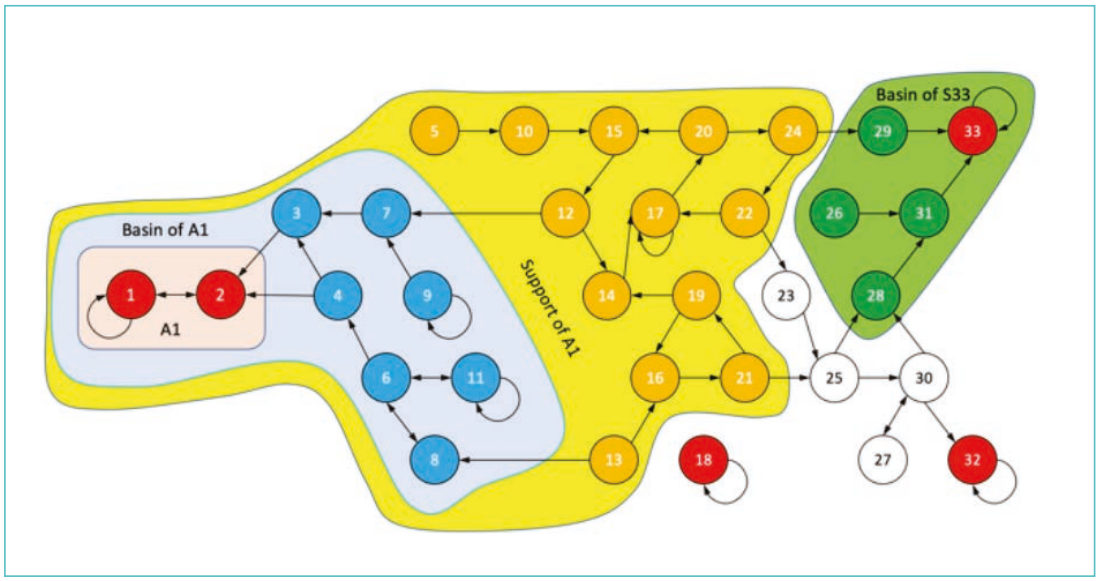


Figure 1:
Graph showing attractor, A1, its basin of attraction (blue), and its support (yellow);
and alternative attractor S33 with its basin of attraction (green) (reproduced from Bramson, 2019 [1] p96)

This topic is to establish a theoretical baseline for describing complex adaptive system states and relating this to properties, such as cyber-resilience and antigrafility. The challenge includes:

- Representing a CAS in simulation and/or with real data
- Effective identification of CAS system states and the corresponding graph (interdependencies) given that the states are tied to emergent properties, and the system may have been constructed generatively
- Determination of state transition probabilities
- Modelling of high-level phenomena, such as strategic balance points (eg balance between cohesive and exploratory forces), and antifragility
- Relating the state-based model to other representations (such as cyber-physical attack graphs)
- The possibility of metrics (based on probability) for key aspects of system dynamics, such as: Sustainability, Susceptibility, Resilience
- Representing actionable anomaly that is traceable to the actions of an attacker (discriminating endogenous and exogenous sources)
- Identifying prerequisites and design criteria for realistic digital twins representing CAS dynamics

Data will necessarily be synthetic, or restricted domain real-world, for this study as real-world wide area data is not yet available (and probably won't be for some time). We anticipate the need for extensive computer simulation (based on trials and observations) to obtain some of the basic values and identifications. The need for training of key system parameters may require the identification of new machine learning techniques.

Ref: [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

Example Approaches:

Complex System science is a development of General Systems Theory (1968) and some of the principles of Cybernetics (late 1940s), however, it remains immature and incomplete despite this pedigree. Although adequate explanations of Complex Adaptive Systems (CAS) remain elusive, techniques that are available include:

- Hierarchical agent-based modelling underpinned by Markov modelling for explaining CAS behaviour
- Generative self-organisation using ideas from Finitely Generated Groups
- CAS dynamics using state-based modelling underpinned by Markov modelling
- CAS adaptation using ideas from robotic social learning (with the possibility of achieving antifragile properties)
- Lookahead action modelling and consequence modelling from robotics using evolutionary game theory
- Reflexive control as a potential attack model suitable for representing deception vulnerabilities.

A major challenge in dealing with CAS is determining which of the possible approaches to modelling the various characteristics and phenomena are appropriate, and how we can reach a realistic model (even if at low resolution) that is useful.

Topic 16
Exploration and exploitation of artificial light: an opportunity or security risk?

Key Words: optics, lasers, LiFi, lens, photogrammetry

Research Topic Description, including Problem Statement:

There has been a series of science and technology advancements in our use of artificial light. Rather than passively consume this, we have created the ability to transmit data over the light spectrum to carry data, therefore than mere passive consumption we now have a dual purpose for this, which could lead to savings in other areas, if this is advanced further. What would the future of Lifi look like and what are the implications for security and privacy, particularly if we are sharing personal, financial or sensitive IP using this method?

What do we consider to be the next advancements of LiFi and why has current uptake of this technology been slow and not more commercially available?

These are just a few examples of the areas of interest in relation to the use of artificial light. We would like to understand the risks associated with the exploitation of all parts of the light spectrum including the proposed Lifi technologies.

We would also like to know what protective measures can be put in place to give greater security if that technology is deployed in sensitive environments.

Example Approaches:

- LiFi – a technology that can be used to carry data.
- https://purelifi.com/technology
- Lifi enabled mobile phone cases as part of IoT

Topic 17
Detecting anomalous small-scale seismic events

Key Words: earthquake, noise floor, drilling, erosion, reverse engineering

Research Topic Description, including Problem Statement:

Seismic activity can come in many forms from many different origins. Detection of seismic activity can help develop early warning signs of earthquakes and prevent loss of life through rapid evacuation. Disaggregating simultaneously occurring seismic events becomes more challenging. The ability to differentiate between events of concern and routine background noise.

From a security aspect we want to detect anomalous seismic events that could affect our buildings. We want to be able to develop techniques that enable us to create a seismic profile of a building and study this over a period of time with the ability to explain the origin, nature and duration of all seismic activity, however subtle.

We need to understand the technology landscape in this area and develop ways of protecting our people and assets from compromise. Detection of subtle seismic events and activities would help the UK protect its science, engineering, industry and critical infrastructure.

Example Approaches:

Current seismic monitoring can enable earthquake detection and prediction of events that require protection of towns and citizens. Early, volcanic activity detection over a wide range and monitoring to aid scientific understanding and protection of neighbouring communities and infrastructure.

Novel drilling techniques for construction proposes to determine if there is likely to be any impact on integrity of a building or infrastructure, while providing benefits of its application for legitimate law enforcement, CT and military operations, see The Almost Silent Drill, courtesy of International Procurement Services Ltd.

Topic 18
Data analysis for national security using artificial neural nets implemented on quantum annealing processors

Key Words: neural nets, D-Wave, non-Restricted Boltzmann Machine implementations, image analysis

Research Topic Description, including Problem Statement:
Artificial neural nets (NNs) show promise for machine learning and artificial intelligence in many application areas but require training using large data sets. This is achieved in either a supervised way, using data which have been previously labelled, or an unsupervised way. Preparation of labelled data sets is slow and expensive. Requiring only minimal human supervision, unsupervised learning avoids the data preparation step by inputting to the neural net large volumes of unlabelled data. The NN learns autonomously to recognise patterns in the unlabelled data (determines a set of numerical weights and biases associated with each node in the net) but requires larger data sets than for supervised learning and the process is challenging for conventional digital processors.

Machine learning is one area in which quantum computers are expected to give quantum advantage over digital processors and D-Wave processors have been used to implement NNs by training Restricted Boltzmann Machines (RBMs) using contrastive divergence and, for image analysis at least, this has been found to give improved learning performance and speed advantage over digital processors.

Programming quantum computers is challenging, however their application to the training of NNs is attractive for several reasons. Using classical methods, the training of NNs can be either very slow (unsupervised) or slow and expensive (when supervised). Quantum computers offer the ability to speed this training up significantly. However once the weights and biases are trained, say on a quantum processor, they can be transferred for rapid assessment onto a classical device. This transfer allows for the training of the NNs to be carried out on the hard to program quantum hardware (realising speed benefits), whilst their deployment can be retained on classical devices.

Neural nets have been implemented in many other ways than RBMs on digital processors and this project will implement, characterise and benchmark some of these different approaches on D-Wave hardware. Working with the Ministry of Defence, and its research arm The Defence Science and Technology Laboratory, the technology will be applied initially to image analysis for feature identification and tracking but in later stages of the project, the methodology will be extended to analyse other types of data (for instance text and natural language). The important metrics will be speed of execution and accuracy as well as robustness to image noise.

Example Approaches:
None provided.