North West Partnership for Security and Trust
National Cyber Force OFFICIAL Research Challenges
Call for Research Proposals

Summary
The Northwest Partnership for Security and Trust (NWPST) is inviting proposals from researchers from all disciplines at the universities of Lancaster, Manchester, Manchester Metropolitan and Salford to undertake research for the National Cyber Force (NCF). Up to £75K of funding per project per year for the duration of each project will be made available to fund interdisciplinary projects in this area. Please email NWPST@manchester.ac.uk if you have any questions.

Background
The NWPST is a partnership (launched in October 2021) between GCHQ, the UK’s Government Communications Headquarters, and four universities based in the North West of England: Lancaster University, the University of Manchester, Manchester Metropolitan University and the University of Salford. The unique partnership is a vehicle for collaboration between disciplines, institutions, and sectors, focused on the most difficult technology and security problems.

The NWPST fosters collaboration across research, innovation, skills development, and public engagement, to produce new knowledge to benefit national prosperity and societal understanding of issues relevant to national security. Greater Manchester, and the broader North West corridor, is one of the most diverse areas of the UK, and home to some of the country's most diverse Universities. The NWPST will benefit from engaging our varied communities to bring together talented people from different backgrounds to help solve the most difficult national security challenges.

The purposes and guiding principles of the NWPST were developed jointly through discussions between GCHQ Manchester and the four Universities.

The vision of the NWPST is:

1. To facilitate high-quality and impactful research in and across a wide range of disciplines relevant to UK national security challenges.
2. To build relationships with stakeholders across the northwest and throughout the region, including government, industry, and civil society, to identify opportunities to develop new products and services, and enhance the productivity and security of existing provision.
3. To develop and deliver accessible and inclusive skills and apprenticeship provision, to support access to opportunities within the digital and data security sectors for citizens in the North West.
4. To engage with communities, stakeholders and the wider public to inform, explain and educate on issues of trust and security.
More information about the NWPST will be distributed via a Welcome Pack to any potential applicants who express an interest (see ‘How to Apply’). Applicants are required to read the Welcome Pack before applying. The provisions in the Welcome Pack for projects undertaken through the NWPST for GCHQ apply equally to projects undertaken for NCF.

The National Cyber Force (NCF) is a joint organisation led by GCHQ and the Ministry of Defence (MoD). It was established in 2020 to:

- Respond to and mitigate cyber and real-world threats at home and overseas.
- Shape and influence the actions and behaviours of our adversaries.
- Support the rules-based international system.
- Assist in the delivery of foreign policy objectives.

The aim of the NCF is to deliver responsible offensive cyber operations to realise the above objectives and has already made considerable impact. As a responsible cyber power, the UK regulates the conduct of NCF operations within the context of a number of key pieces of legislation: Investigatory Powers Act 2016, Intelligence Services Act 1994, Computer Misuse Act 1990, Wireless Telegraphy Act 2006 and the Law of Armed Conflict (LOAC).

Call Details

The Research Challenges

Introduction

The UK can and must develop and use its own cyber capabilities in order to stay ahead of its adversaries and support its allies across the globe and has therefore established a National Cyber Force (NCF). Led by GCHQ and the MOD, with core partners SIS and DSTL bringing cutting edge espionage and research techniques, the NCF will also draw on wider parts of government that have world-leading expertise.

It is critical that the NCF has access to the full range of technical expertise available, from the traditional defence contractor community to small & medium sized enterprises (SMEs) and academia. In particular, SMEs and academia are likely to possess niche skills and expertise of value to the NCF while not operating within the classified defence and intelligence community. Therefore, the NCF has distilled a set of OFFICIAL research challenges from its classified research portfolio which can be more openly shared with non-traditional industry and academic partners.

This document describes the OFFICIAL research challenges. It is structured as follows. We have identified a number of vertical use cases which are illustrated in the blue boxes in the figure below. Research in these areas would contribute directly to operational outcomes for NCF, and we explain the use cases in more detail below.

There is synergy between the identified use cases which means that we have also identified some cross-cutting research areas that underpin multiple use cases, as illustrated by the yellow boxes below. The cross-cutting research topics are also discussed in more detail below.
We are interested in a mix of short term and long-term research. For example, respectively these may be directed at the specific use cases above or at the more fundamental cross-cutting issues we have identified. However, longer term research projects should plan for the provision of interim deliverables or capabilities. Projects that seek to provide incremental benefit throughout their duration are more likely to be funded.

**Use-cases**

**Understanding and countering malign influence**

A considerable challenge for liberal democracies is the spread of online misinformation and disinformation, as well as extremist material designed to radicalise individuals. This material is malign in the sense that it is designed to weaponise the very openness of such democracies, exploiting the free flow of information and ideas to increase the degree of polarisation and further open up existing fractures in society. This may not always require the promulgation of false information, it may be enough to simultaneously put forward and amplify opposing views in order exacerbate an existing conflict of views. This is not a risk to which authoritarian regimes are subject, they are able to control the narrative and to suppress viewpoints and information which do not accord with the regime’s accepted view.

It would not be in accordance with the UK’s values to engage in similar disinformation/misinformation activities, but we do wish to promote truthful, balanced narratives and to effectively counter extremist messaging in a way that allows people to make informed decisions.

This research area is aimed at improving our ability to counter extremist messaging and narratives as well as disinformation and misinformation from hostile overseas actors. In particular, the following aspects:

- Achieving a robust understanding of how malign actors propagate their influence in the modern online information space, with particular interest in how the changing nature of technology has affected these techniques and made them more or less effective.
- Understanding how culture operates online, both reflections of ethnicity and nation state membership as well as the more chosen and adopted norms of uniquely online groups.
• Developing methods and techniques for analysing and understanding the culture of online spaces, platforms and the groups that exist on them.
• Ensuring that our online presence is respectful of, and effective in, the presence of cultural differences, i.e. ensuring that we effectively promote our values and truthful narratives to people from other nations and cultures while not dismissing the value of diverse cultures.
• Predictive and repeatable measures of effect for messaging and influence interventions, in particular techniques that can be effective across platforms and remain relevant with technological or structural updates.
• Developing principles for effective coordinated social media campaigns across multiple streams and services.

Research questions:

• What are the indicators of a malign influence campaign (e.g. the use of “sock puppet” or fake accounts, polarising or extremist narratives), and how can such efforts be detected at scale?
• How does the underlying platform used affect how information within a malign influence campaign propagates? What features are exploited or are a hindrance to operation? How do changes or updates to a platform affect these efforts?
• Can we identify the fractures and points of contention within a society at which a malign influence campaign is aimed? Can these circumstances be identified ahead of time?
• What makes a malign influence campaign successful and how do we develop strategies to undermine it? How do different types of messaging affect people?
• What sort of interventions should we make to counter a malign influence campaign while remaining true to our values?
• How do we ensure that our interventions land effectively? How do we take into account cultural norms and differences in our target audience?
• To what extent can modelling help to predict the effect of an intervention against a malicious influence campaign?
• How do we efficiently counter a malign influence campaign that has been coordinated across multiple social media platforms?
• How do we mitigate the inherent asymmetry introduced by the fact that it is far easier to generate disinformation than truthful narratives? Can we automate the generation of information for a counter malign influence campaign?
• How do we promulgate factual information to an online audience in a way that they will consume it? How can we ensure that this affects behaviour?
• Can we limit the impact of malign influence even when the recipients will never accept our view of things? How should wider public perceptions of the intelligence, security and defence community affect how we deliver our interventions?
• How do we measure the impact of influence campaigns, both malign and counter-malign? What indicators do we need to measure to quantify this?
• How do we train people to more effectively recognise that they are being targeted by a malign influence campaign?

Datasets required: Online interaction data e.g. social media data, e.g. Twitter, Facebook, Instagram, message boards, YouTube.

Relationships required: NCF will provide introductions and access to relevant teams, as appropriate.
Automated risk and policy assessment

As part of operational planning, we have robust processes in place to assess risk and policy compliance, and the results of our deliberations are routinely recorded. However, we have no easy way of drawing upon this accumulated knowledge to inform the planning of new operations beyond relying on our experts to recall the relevant details of previous operations. We require new ways of processing our recorded knowledge to make it accessible to operational planners, to fully inform our experts who are being called upon to make risk decisions, and to identify long term trends and aggregated risks of which we might not otherwise be aware.

Any research in this area must consider the ethical implications of giving a machine full access to case histories where no human commands the same level of knowledge. For example, we must consider the ethical considerations of pooling data into artificial intelligence (AI) systems. In addition, higher risk cases may need to be identified and flagged for human intervention. We may also need to consider the risk of inherent bias in any AI system which could affect our decision making.\(^1\)

This research area is about developing techniques to process and derive value from large amounts (of the order of hundreds or thousands of documents) of risk management and technical recommendations held within prose documents. These will automatically derive general risk mitigation plans and policy from the principles embedded within them, allowing them to be assessed against an initial baseline and to assure their rapid, fair, and consistent use in subsequent scenarios. In some cases the principles may have been built up over a considerable time, placing significant reliance on experts with enough background to be able to recall the relevant decisions that were made in the past in order to inform current decisions. Policy changes over time will further complicate this as well.

Success in this instance means that we can make robust policy and risk decisions without overly relying on the ability of our experts to recall the details of numerous operations over many years. Our decisions will be informed by emergent risks that our assessment systems are able to identify and surface, of which we might otherwise remain unaware.

Research questions:

- Can we automatically generate policies based on the extant decisions documented in existing documents?
- Can we calculate the aggregate risk implied by the individual risks across a range of documents? How do we identify emergent risks that do not exist within a single document or operation?
- How do we quantify risk so that we can properly compare it across multiple operations?
- Can we make use of prior art in the legal field which seeks to achieve similar goals for case law?

\(^1\) Some of these issues are considered in Alexander Harris, Eleanor S, Emma Bradford and Ardi Janjeva, "Behavioural Analytics and UK National Security," CETaS Research Reports (March 2023).
Can we assess the value of past risk mitigations and identify targeted opportunities to take increased risk?

Datasets required: Large corpus of representative and publicly available documents containing policy and risk decisions exist.
Relationships required: Access to mission policy staff and operational risk assessors.

**Improving the cognitive performance of operators and analysts**

NCF’s operators and analysts are dealing with ever more complex and extensive datasets, and these datasets may connect with one another in ever more complex ways. We would like to scale our capabilities, making decisions differently to the way in which we do now and using data in a fundamentally different manner. We would like our analysts to be able to routinely and effectively work with datasets that a human would not otherwise be able to do without machine support. The seminal paper “The Psychology of Intelligence” by Richards J Heuer (CIA Center for the Study of Intelligence, ISBN 1 929667-00-0, 1999) remains a good base from which to start.

This research is therefore about using human/machine teaming to enhance the ability of human operators and analysts to process and make decisions based on large, complex datasets in real time, for a set of domain areas, e.g.

- Multiple information feeds providing situational awareness to an analyst, where those feeds may be presented in terms of multiple modalities (e.g. video, text, images) and potentially in real-time.
- Analysis of a large system consisting of multiple components that interact in complex ways, often asynchronously.

The goal is to understand what tooling and support will make it possible for humans to efficiently, accurately and intuitively understand and/or interact with significantly more (and/or more complex) data than traditional tooling permits.

Success in this instance means that our operators and analysts can make sound decisions in the presence of large amounts of data, some of which is conflicting, and for longer periods without incurring excessive fatigue.

Research questions:

- Can we develop representations that assist the operator to modify or initially configure complex datasets? Can these representations allow the operator to generate new insights into the data?
- How can automated systems help reduce data down to an accessible amount without compromising nuance or necessary complexity?
- How can we support the navigation and exploration of large datasets without indulging cognitive biases such as confirmation?
- How can we use human-machine teaming to enhance the analyst or operator experience?
- What can we learn from other fields, for example aerospace or radiology?
- Where data is not necessarily sufficiently tagged, how can we measure how consistently and accurately people are using tools?
- How do different visual representations of complex datasets affect the ability of operators to make accurate decisions and judgements dependent on that data?
• What biases do human-machine teaming principles need to take into account or design around when dealing with large datasets?
• How do different dataset and task types differ in the type of tools and support required to work with them?

Datasets required: Experimentally obtained biometrics data (e.g. tracking emotions, attention tracking), task/workflow metrics (throughput, work-in-progress, etc.), mission / operational metrics (to know if current performance is improving on achieving operational goals), capability metrics (to know the availability/relevance/performance of a capability in helping the operator achieve their task), simulated data (e.g. an AI agent may be using reinforcement learning to discover new knowledge to push to the operator and/or finding new ways to help the operator perform their task), knowledge (possibly in form of embedded knowledge graphs or knowledge objects).

Relationships required: NCF will provide introductions and access to relevant teams, as appropriate (e.g. how helpful they are finding a ML model/tool output and assistance).

**Cross-cutting themes**

**Reasoning over unstructured data**

Solutions to the use cases above will require us to develop techniques not just to ingest and process unstructured data, but to reason over the knowledge gained, making inferences and spotting trends. This includes the full range of media, including images, sounds, and video, but primarily focuses on text and semi-structured data such as configuration files and social media posts. This needs to be done at scale, over large numbers of documents and files, which may number hundreds of thousands or even millions, and which may not all be English language documents.

Research questions:

• How can ontological knowledge be generated from unstructured data, rather than just identifying discrete entities?
• How can data from a variety of sources be efficiently and automatically processed, which may be in a multitude of formats?
• What are the effects of partial information over human reasoning and inference abilities? How good are humans at identifying where data is sufficient or insufficient for drawing conclusions?
• How do humans resolve contradictory information? What sources are prioritised and why? What types of data and characteristics of that data (e.g. volume, source) do we use to resolve perceived conflict?
• How should tools communicate uncertainty to users when datasets used for analysis are incomplete or insufficient? How can a dataset define or quantify a level of sufficiency?
• How can we identify which data is important and which we can ignore?
• What is the state of the art in the richness of facts that reasoning over unstructured data can generate?
• How can we mitigate the risks of cognitive bias where the limited information to which we have access is given more weight than the missing data?

Datasets required: Representative publicly available repositories of documents for a particular domain, e.g. research papers, technical documents or horizon scanning papers.
Cultural context

The modern world is a complex, socio-technical system, and the social component of that is key to understanding and predicting how that system will behave. To better understand the system, we need to understand the human component. In addition, we need to understand how cultural differences across different, particularly non-Western, societies affect those interactions. For example, it is likely that the way users react to the information they receive from a social media platform will be very different across diverse cultural groups.

Research questions:

• How can we categorise, systematise and quantify (where possible) cultural factors that influence perceptions and opinions? How can these tendencies be detected from online datasets?
• How does culture affect the way different societies build technological solutions and systems?
• How do different types of cultural influences affect decisions? How does the cultural influence of a nation state compare and interact with that of a person’s professional or personal peer groups online?
• How will social media interventions (posts, thoughts, expressions) be viewed by different societies and cultures? Will these render the interventions more or less effective?
• What can we learn from commercial disciplines such as digital marketing?
• How are Western deterrence measures perceived within other cultural contexts, by other nations, by the targets of those deterrence measures and by neutral states?
• How do cultural aspects affect decision making in national security priority nation states?

Datasets required: Comparative datasets drawn from both Western and other sources.

Intuitive comprehension

Improving the cognitive performance of operators and analysts raises a range of issues about how we present complex information and both structured and unstructured data in ways that allow human beings to:

• Make sense of it.
• Identify the key items of interest.
• Identify anomalies.
• Draw inferences.

This includes visualisations and other novel methods of presenting data so that it can be grasped more intuitively.

Research questions:

• Are there paradigms and metaphors that we can adopt to provide analysts with an intuitive grasp of complex datasets, for example when moving breadthwise across the dataset or when working at multiple levels of detail? How do we ensure that we present users with the right density of information?
• What sort of visualisations (and other representations) allow analysts to more easily comprehend data?
Are there novel modalities such as visualisations or other sensory inputs that we can use to enhance the analyst’s experience?

Datasets required: Large, complex datasets, especially those containing multiple types of media. Complex, real-time data feeds.
Relationships required: NCF will provide introductions and access to relevant teams, as appropriate.

Budget

There is an overall budget for this activity of up to £75K per project per year costed at 100% FEC. As stated below, applicants can propose multi-year projects (maximum of 3 years) provided the maximum cost in each year does not exceed £75K at 100% FEC. Please note that the funding is not available to support staff, equipment or activity outside of the NWPST. We will assess projects individually, with the aim of selecting as many suitable projects as we can within our overall funding envelope.

Nature of Activity

The minimum team size is one researcher. We welcome short projects that can be completed within a few months as well as multi-year (maximum of 3 years) and multi-disciplinary projects. We would welcome applications from a broad set of disciplines including but not limited to, technologists, psychologists, philosophers, and behavioural scientists.

Within the projects a variety of approaches and/or outputs are encouraged. Funding might cover the costs of conducting scoping studies, research engagement with organisations and/or communities, feasibility studies, and demonstrators. Proposals for potential multi-stage projects, where only the first stage is fully specified, are welcome, provided that the overall direction of travel is defined.

Potential data sources are outlined above for illustrative purposes. Proposers should be aware that in general, the NCF will not be able to provide datasets from its own data holdings. However, we would endeavour to engage with projects to provide advice, so that proposers can work with publicly available data that is sufficiently representative of NCF holdings.

Expected outcomes

- Prototype implementations, new methodologies or experimental results
- Recommendations for future work
- Presentation of results

Each project will be assigned an NCF stakeholder who is invested in the outcome of the work. The stakeholder will provide the point of contact between the project and NCF, will mediate access to sources of NCF expertise, and will provide guidance to the project to ensure that it delivers results that are relevant to the Force.

How to apply

Applications are invited from academics at the University of Manchester, Manchester Metropolitan University, University of Salford and Lancaster University, from any discipline and at any career stage. Applicants must be eligible to receive UKRI funding, please see the UKRI Eligibility Guide. Application Forms and any required additional documents should be sent to NWPST@manchester.ac.uk with the subject line “NCF Research Project Application”.

OFFICIAL
All individuals wishing to apply for this call are required to read the “NWPST Welcome Pack” prior to application and the application form requires acknowledgement of this. All Non-UK National and dual nationals intending to apply will be required to complete the “NWPST Non-UK National and Dual National Applicant Details” form prior to application. Please see “NWPST Welcome Pack” Section 6 “Protecting your security” on some considerations when partnering with GCHQ. This should not deter expressions of interest as, where possible, we seek to build diverse and inclusive collaborations through the NWPST.

If you require a copy of the NWPST Welcome Pack or the NWPST Non-UK National and Dual National Applicant Details or you have any queries, please contact NWPST@manchester.ac.uk.

Assessment Criteria

Proposals will be reviewed against the following selection criteria:

- **Plan:** Quality of proposed project and workplan.
- **Project Team:** Quality of the applicants’ research track record and relevant experience of the project team.
- **Research vision:** Quality of the research vision and novelty of the approach to the chosen research topic.
- **Impact:** The potential contribution of the research to the NCF, possibility and value of follow-on activities generated as a result of the project.

Applications will be assessed by a panel drawn from the NWPST Implementation Group.

**Key dates**

<table>
<thead>
<tr>
<th>Date</th>
<th>Item</th>
</tr>
</thead>
<tbody>
<tr>
<td>29th June – 20th July</td>
<td>Pre-call open for expressions of interest</td>
</tr>
<tr>
<td>7th August</td>
<td>Applications open</td>
</tr>
<tr>
<td>22nd September, 5pm</td>
<td>Applications close</td>
</tr>
<tr>
<td>6th October</td>
<td>Funding Panel give in-principle decision</td>
</tr>
<tr>
<td>October</td>
<td>NWPST team will work with the PI’s research support offices to complete contractual work asap. Projects can start as soon as contracts are in place.</td>
</tr>
<tr>
<td>24th November</td>
<td>Latest date by which projects should start</td>
</tr>
</tbody>
</table>

If you have any questions, please email NWPST@manchester.ac.uk. To submit an application, please email NWPST@manchester.ac.uk with the subject line “NCF Research Project Application”.