ESRC Policy Fellowships 2021: Opportunity description

Fellowship Title: HO Cyber Crime

Host department: Home Office

Host team: Home Office Analysis and Insight

Summary: Evaluating the impact of cyber security behaviour change interventions

Policy topic: Cyber Crime, Cyber Security

Potentially relevant academic disciplines: Behavioural Sciences, Psychology, Criminology, Sociology, Cyber Security, Computer Science

Relevant research career stage: No preference – open to early or mid-career

Practical details

Start of 3-month inception phase: January 2022

Length of core placement: 12 months

FTE for core placement (range): 0.6 - 1

Location requirements: Remote working is possible and expected to some degree. Subject to Covid restrictions, travel to London would be valuable on occasion e.g. once every fortnight, to meet with analytical and policy teams. Depending on the nature of the project, some travel around the UK for fieldwork may also be required, but again can be flexible given the individual's location, personal circumstances and any Covid restrictions.

Necessary level of security clearance: Baseline Personnel Security Standard (BPSS) and Security Check (SC) will be required. It is important to note for SC clearance that applicants should have been resident in the UK for the last 5 years. Advice for those being vetted is here and the Vetting Charter can be found here. Further information on security levels can be found here. Three months should be allowed for arranging security clearance so the person taking up the Fellowship opportunity will be asked to start the security check process as soon as their Fellowship has been confirmed by ESRC.

Detailed description

In recent years the threat posed by serious criminals has changed. There have been high profile cyber-attacks against the UK, with technological changes offering growing opportunities for criminals. As a key part of the National Cyber Security Strategy, Cyber 'Protect' '*ensures that individuals and organisations…are taking appropriate steps to protect themselves, and their customers, from the harm caused by cyber attacks'*.[1] This has led to various government and law enforcement activities to help individuals and businesses protect themselves from cyber crime. This fellowship will seek to better understand the overall impact of 'Cyber Protect' activity.

Key questions include:

- How do we best track and monitor Cyber Protect performance, collectively across government? How do we specifically measure impacts on behaviour change?

[1] National Cyber Security Strategy 2016-21, available at: https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021 See also: Serious and Organised Crime Strategy 2018 - GOV.UK (www.gov.uk)

- Overall, how effective are the Protect initiatives that government and law enforcement have introduced?
- What else could the Cyber Protect community invest in, or improve, in future?

This fellowship provides opportunity to build the evidence base on a high priority area. It requires working closely with policy teams, law enforcement, the National Cyber Security Centre and other analysts to identify and develop appropriate metrics to assess Cyber Protect. The postholder would design and deliver at least one project evaluating the impact of an intervention. As part of a multi-disciplinary analytical team, there would be opportunity for wider day-to-day experience in terms of how evidence informs policy-making.

Depending on the postholder's background, it may also be possible to undertake additional activities, e.g. helping build the evidence base on key threat areas such as ransomware, or providing particular technical cyber security insights. We are happy to discuss additional areas of interest with applicants to develop projects best suited to their expertise.

Opportunity-specific person specification

Applications will be assessed against the following opportunity-specific requirements in addition to the generic eligibility and call criteria.

- Previous experience in cyber crime or cyber security areas would be highly desirable.
- Skills in project and/or programme evaluation and monitoring are also highly desirable.