social machines

At Social Machines we believe in a world where societies are both open and resilient. Our hyper-networked world provides opportunities for malign actors to access and influence all of us more easily than ever: demanding radical change to how we conceive of security and resilience across our societies. Social Machines supports understanding of how people and machines interact together in this environment – how *socio-technical* systems function: we use our knowledge and skills drawn from behavioural and social sciences to build trust and resilience within them.

Our Capabilities

- Core expertise draws from cognitive and social psychology (including cyber psychology), behavioural economics, anthropology, decision science, systems, information and network science.
- Extensive experience and domain knowledge working in cyber security, humans in socio-technical systems, artificial intelligence impacts on socio-technical systems, influence and information operations, behaviour and culture change.
- Our methods include – but are not limited to – evidence base collection and curation, including robust literature review and open source; expert elicitation and information elicitation; qualitative study design (observation and ethnography, interview, focus group) quantitative study design (experimentation and survey); and mixed methods design; behaviour and culture change design – including monitoring and evaluation.
- Our research and innovation work ranges across Technology Readiness Levels 2-9.

Track record

- We work extensively within the UK government defence and security sector.
- Previous work includes construction of an evidence base investigating hypotheses on adversary cognition and decision-making as they conduct reconnaissance, make plans, infiltrate and exploit cyber systems.
- We are currently building on this work, exploring how different adversary motivations interact with a range of cyber defences, as they target these systems. This includes mixed

method study design using experimentation, observation and self-report data collection to make evaluations in settings designed to be as ecologically valid as possible.

- Previous work for UK government includes investigation of how cognition and decision-making in cyber security settings are influenced by factors such as social learning, group influence, and culture.
- Our extensive work for the UK National Cyber Security Centre includes (1) how influencing systemic incentives can alter cyber security outcomes in high level socio-technical systems; and (2) exploration of novel experimentation methods for reducing / avoiding risk in conducting behaviour change interventions in live cyber systems (in which the negative impact of unintended consequences can be very high).
- Designed and led development of a behaviour change capability now operating in the UK Foreign, Commonwealth and Development Office's core policy teams.
- Curated evidence base in relation to behavioural consequences of the impact of machine learning applications on socio-technical systems.

Our Values

We are strongly committed to our core values of empathy, creativity and integrity:

- We aim to understand how others see the world before acting.
- We are creative in thinking of ways forward that meet the needs of those involved.
- We conduct ourselves with integrity at all times.

Contact Details

Email: justinhj@socialmachines.co.uk

Tel: +447748246417

Website: www.socialmachines.co.uk