CREST CENTRE FOR RESEARCH AND EVIDENCE ON SECURITY THREATS

Centre for Research and Evidence on Security Threats

Understanding and Countering Online Behaviour

UNIVERSITY OF BATH

Team Members

Adam Joinson, Professor of Information Systems (Bath), Programme Lead
Brittany Davidson, PhD student, University of Bath (Social media profiles)
Joanne Hinds, Research Associate, Bath (Online Behaviour, digital footprints)
Samantha North, PhD student, Bath (Young people, digital radicalisation and cyber security)
Lukasz Piwek, Lecturer in Data Science, Bath (Digital footprints)
Nicholas Ryder, Professor of Law (Terrorist finances, networks), UWE Bristol.
Awais Rashid, Professor of Computer Science, University of Lancaster
Laura Smith, Lecturer in Psychology University of Bath (Radicalisation)
Tommy Van Steen, Research Assistant, University of Bath (Footprints review)

Overview of programme

The work in this programme is centered around understanding and shaping online behaviour in a security context. This work is focused on three strands, alongside inter-disciplinary work connecting networks, finance and online behaviour.

Strand 1: Radicalisation online. Following the completion of an in-depth review of the state of the art understanding of radicalisation and the internet, we have conducted studies that seek to identify patterns of increasing radicalisation through language and behaviour (using Twitter – Smith, and Facebook – Joinson).

Strand 2: Digital footprints. Two systematic reviews completed that provide a summary and analysis of the current literature linking online behaviour to individual characteristics such as personality, demographics and political affiliation. Over 12,000 papers reviewed.

Strand 3: Shaping behaviour online. Ongoing research into using social norms to alter trangressive behaviour on Twitter (Joinson, with Twitter, MIT and Harvard), and designing studies to track how types of engagement (e.g., like vs. comment vs. share) lead to increased 'real life' action (or otherwise).

Case study: digital footprints

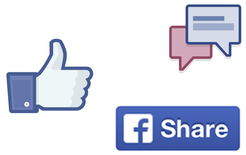
The idea of 'behavioural residue' has a long history in psychology, with the traces we leave behind in the physical and virtual environment providing clues to personality, socio-demographics and group and interpersonal dynamics such as agreement and rapport. In a security and intelligence context, being able to interpret the 'residue' subjects of interest 'leave behind' as they interact in virtual environments can provide important clues about their current state of wellbeing, stress levels, personality, likely responses to outside events, and the dynamics within a group.

We have conducted two large scale systematic reviews (and one meta-analysis) to collate and evaluate the evidence-base for connecting digital footprints to individual characteristics. We are now designing studies to examine how that evidence may help predict people's responses to interventions in an online space.

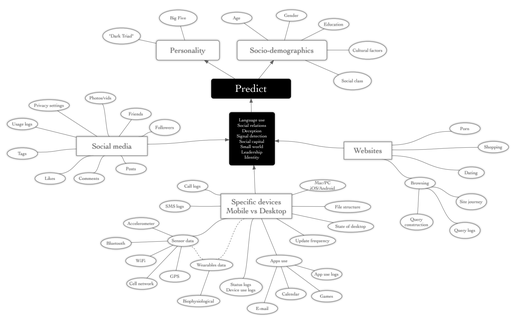
Case study: what's in a 'like'

Not all levels of engagement in an online space are equal. For instance, 1.9m people 'like' Britain First on Facebook, but each post they make gets substantially less engagement – we scraped the most recent 100 Britain First Facebook posts, and found that each one gained an average of:

- 420 'likes',
- 343 'comments' and
- 327 'shares'.



We currently are scraping a range of ideological groups to examine the pattern between 'likes' and other forms of engagement, and if engagement increases over time, and for particular people. This work is influenced by our digital footprints review that identified that 'retweeting' is a better predictor of political affiliation than 'following'. Finally, we are designing experiments to test if different forms of engagement lead to more commitment or risk of action in the offline world.



Knowledge synthesis and bite-size guides

Bite size guides (forthcoming in *italics*)

- Phishing
- Messaging
- *Influence online*
- *Measuring effects*

Synthesis reviews:

- Radicalisation online
- Digital footprints
- *Influence online*

Roundtables

- Social media use and protective security
- Digital footprints
- Influence and effects

Workshops

- Influence online
- Computational Linguistics and security
- *Digital remote assessment*

Original research

The early focus of the programme has been on synthesis of existing knowledge. This is now being supplemented by original research. The topics for this work include:

- Developing and evaluating methods of online influence
- Studies of digital footprints and remote assessment of personality
- Language and engagement in ideological online forums
- Blockchain, social media and terrorist financing
- Methods for characterising typical and atypical social media users
- Language and rapport.