Project acronym and full title:

ACCEPT: Addressing Cybersecurity and Cybercrime via a co-Evolutionary aPproach to reducing human-relaTed risks

Funder:

Project website:

http://accept.sccs.surrey.ac.uk/

Brief summary of project:

Researchers and practitioners have acknowledged human-related risks among the most important factors in cybersecurity, e.g. an IBM report (2014) shows that over 95% of security incidents involved "human errors". Responses to human-related cyber risks remain undermined by a conceptual problem: the mindset associated with the term 'cyber'-crime which has persuaded us that that crimes with a cyber-dimension occur purely within a (non-physical) 'cyber' space, and that these constitute wholly new forms of offending, divorced from the human/social components of traditional (physical) crime landscapes. In this context, the unprecedented linking of individuals and technologies into global social-physical networks - hyperconnection - has generated exponential complexity and unpredictability of vulnerabilities.

In addition to hyperconnectivity, the dynamic evolving nature of cyber systems is equally important. Cyber systems change far faster than biological/material cultures, and criminal behaviour and techniques evolve in relation to the changing nature of opportunities centring on target assets, tools and weapons, routine activities, business models, etc. Studying networks and relationships between individuals, businesses and organisations in a hyperconnected environment requires understanding of communities and the broader ecosystems. This complex, non-linear process can lead to co-evolution in the medium-longer term.

The focus on cybersecurity as a dynamic interaction between humans and socio-technic elements within a risk ecosystem raises implementation issues, e.g. how to mobilise diverse players to support security. Conventionally they are considered under 'raising awareness', and many initiatives have been rolled out. However, activities targeting society as a whole have limitations, e.g. the lack of personalisation, which makes them less effective in influencing human behaviours.

While there is isolated research across these areas, there is no holistic framework combining all these theoretical concepts (co-evolution, opportunity management, behavioural and business models, ad hoc technological research on cyber risks and cybercrime) to allow a more comprehensive understanding of human-related risks within cybersecurity ecosystems and to design more effective approaches for engaging individuals and organisations to reduce such risks.

The project's overall aim is therefore to develop a framework through which we can analyse the behavioural co-evolution of cybersecurity/cybercrime ecosystems and effectively influence behaviours of a range of actors in the ecosystems in order to reduce human-related risks. To achieve the project's overall aim, this research will:

(1) Be ***theory-informed***: Incorporate theoretical concepts from social, evolutionary and behavioural sciences which provide insights into the co-evolutionary aspect of cybersecurity/cybercrime ecosystems.

(2) Be ***evidence-based***: Draw on extensive real-world data from different sources on behaviours of individuals and organisations within cybersecurity/cybercrime ecosystems.

(3) Be ***user-centric***: Develop a framework that can provide practical guidance to system designers on how to engage individual end users and organisations for reducing human-related cyber risks.

(4) Be ***real world-facing***: Conduct user studies in real-world use cases to validate the framework's effectiveness.

The new framework and solutions it identifies will contribute towards enhanced safety online for many different kinds of users, whether these are from government, industry, the research community or the general public.

This project will involve a group of researchers working in 5 academic disciplines (Computer Science, Crime Science, Business, Engineering, Behavioural Science) at 6 UK research institutes, and be supported by an Advisory Board with 14 international/UK researchers and a Stakeholders Group formed by 14 non-academic partners (including LEAs, NGOs and industry).

The project is part of Phase 2 of RISCS (Research Institute in Science of Cyber Security).

Start date:

1 April 2017

Duration:

2 years (will be extended due to the expected late start of RAs)

Project budget (funding amount):

£~1.1m (80% full economic costs = £~881k)

Research call:

EPSRC Human Dimensions of Cyber Security (2016)

https://www.epsrc.ac.uk/funding/calls/humandimensionscybersecurity/

Project partners and people:

University of Kent (lead institute): Shujun Li (consortium lead, partner principal investigator), Full-time Research Fellow (to be recruited)

University of Surrey: Michael McGuire (social area lead), Roger Maull (co-investigator), Helen Treharne (co-investigator), Sotiris Moschoyiannis (co-investigator), Part-time (30%) Research Fellow (recruited, to start)

University College London (UCL): Hervé Borrion (partner principal investigator), Gianluca Stringhini (co-investigator), Paul Ekblom (co-investigator), Full-time Research Fellow (recruited, to start)

University of Warwick: Irene Ng (partner principal investigator), Xiao Ma (co-investigator, technical manager), Susan Wakenshaw (Part-time Research Fellow), Andrius Aučinas (Part-time Research Engineer)

University of Birmingham: Ganna Pogrebna (co-investigator)

TRL Ltd: Shaun Helman (partner principal investigator), Rebecca Posner (named researcher), a number of other researchers to be involved

Past member of TRL Ltd: Alan Stevens (partner principal investigator)

Objectives:

The main objectives of the project include:

(O1) To develop a more comprehensive understanding of the key (co-)evolutionary trajectories of human behaviours in cybersecurity and cybercrime ecosystems.

(O2) To compile a knowledge base including evidential and theoretical information to assist solution designers and crime preventers to out-innovate adaptive cybersecurity offenders.

(O3) To develop a cybercrime ontology with an internally-consistent glossary that can make the cybercrime knowledge base machine readable for automated processing.

(O4) To produce a practical framework for reducing human-related cyber risks, which incorporates theoretical concepts and needed software tools for better user engagement via personalisation and contextualisation.

(O5) To validate the developed framework in selected real-world use cases.

Use cases:

Use Case 1) Human-related cyber risks within global transaction and exchange networks. Example scenarios in this use case include transactions involving: (traditional) currencies – specifically the use of money mules for online banking attacks and reshipping mules for online credit card frauds; virtual currencies – specifically bit-coin and block-chain based frauds; objects – specifically trade of stolen or fake goods (e.g. vehicles and diamonds).

Use Case 2) Human-related cyber risks within hybrid transportation networks. Examples include organised crime (e.g. theft) of connected vehicles, cyber attacks on rail infrastructures, pirates collecting intelligence on ships in order to plan physical attacks, etc. This can be built on TRL's extensive research work in the transportation sector, the project team's previous work in a recently-complete project POLARBEAR (led by the project PI Li) and an ongoing project EP/N028295/1 (led by the project CI Treharne).

The use cases will be focused in Year 2 of the project, and in the first year the project will study more scenarios to decide what use cases should be selected. Input from the project's Stakeholders Group and Advisory Board will be sought for the final choices. The project also welcomes wider stakeholders and the general public to inform us about the most important use cases the project should choose.

Expected deliverables:

- A socio-technical framework combining both theoretical concepts and technical tools to facilitate better understanding of human behaviours in cyber security and cybercrime context, sufficiently adaptable to accommodate future developments
- A structured knowledge base of evolution of cybercrime and human-related risk

- A cyber risk and cybercrime ontology (and an internally-consistent glossary derived from this), and a machine-readable knowledge database with related tools which allow automatic knowledge visualisation
- Various tools for handling different data sources to capture information for the knowledge base
- Various tools for supporting risk management and personalised/contextualised cyber risk communications to individuals
- A set of typical cyber risk and cybercrime use cases and scenarios where human behaviours play a key role, with possible intervention points, and accounts of the wider implementation process to realise those interventions in practical terms, including mobilisation and partnership issues
- Various indicators (metrics and qualitative analysis) of findings out of two focused real-world use cases to which the above framework and tools are applied
- Research papers summarising our work and research findings
- A public-facing document with recommendations for future actions of all stakeholders including suggestions and insights for business managers, policy makers and law makers to adjust their strategy towards crime prevention and victimisation reduction in the medium-to-long term

Project Stakeholders Group:

LEA (Law Enforcement Agencies): Surrey & Sussex Police, British Transport Police (BTP), Metropolitan Police Service, South East Regional Organised Crime Unit (SEROCU), Europol

Other governmental bodies: Highways England

Industry: IBM (CyberInvest), NCC Group (CyberInvest), Crossword Cybersecurity plc (CyberInvest), BAE Systems (CyberInvest), Lloyds Banking Group, International Union of Railways (UIC)

NGOs: Neighbourhood and Home Watch Network, HAT Community Foundation

We will try to engage more organisations for our activities around stakeholders. NCSC (National Cyber Security Centre)/GCHQ will be engaged via Surrey/UCL ACEs-CSR, Shujun Li's membership of RISCS (Research Institute in Science of Cyber Security), and CyberInvest companies, which are all (co-)funded by NCSC/GCHQ.

Advisory Board:

1. Pieter H. Hartel (**Chair**): Professor of Cyber Security, Delft University of Technology; Professor of Cyber Security and Crime Science, University of Twente (The Netherlands)
2. Francesca Bosco: Project Officer, Emerging Crimes Unit, United Nations Interregional Crime and Justice Research Institute (UNICRI); Co-founder, Tech and Law Center; Advisory Board Member of Europol EC3; Member of HORIZON 2020 Advisory Group on Secure Societies, European Commission (Italy)
3. Noellie Brockdorff: Associate Professor / Dean of Faculty of Media & Knowledge Sciences / Head of Department of Cognitive Science, University of Malta, Malta
4. Joseph A. Cannataci: Chair in European Information Policy & Technology Law, University of Groningen (The Netherlands); Head of the Department of Information Policy & Governance, University of Malta (Malta)
5. Kim-Kwang Raymond Choo: Associate Professor, University of South Australia (Australia)
6. Adam Doupé: Assistant Professor, Co-Director of Laboratory of Security Engineering For Future Computing (SEFCOM), Arizona State University (USA)
7. Marco Gercke: Director of Cybercrime Research Institute (Germany); Visiting Professor, University of Oxford (UK)
8. Richard Jones: Lecturer in Criminology, School of Law, University of Edinburgh (UK)

9. Marianne Junger: Professor of Cyber Security and Business Continuity, University of Twente (The Netherlands)
10. Daniel Keim: Professor, University of Konstanz, Germany
11. Stuart Macdonald: Professor (criminal law and counterterrorism), Swansea University (UK)
12. Ken Pease: OBE, Visiting Professor of Criminology, UCL / Loughborough University / Manchester Business School / Chester University (UK)
13. Fabio Roli: Director of PRA Lab (Pattern Recognition and Applications Lab), University of Cagliari (Italy)
14. Alan Woodward: Independent Security Consultant; Visiting Professor of University of Surrey; Academic Advisor of Europol EC3 (UK)