SUMMER SCHOOL
Digital Trust and Security in the Post-COVID World: Theory and Research

20 June – 24 June 2022

Fully online

Overview

Digital systems have transformed – and continue transforming - societal daily routines and economic systems, and the security risks we face. The benefits of digital systems depend on public trust in their safety, reliability, fairness, and maintenance of values, which in turn depend on secure hardware and software, fair and effective technological and behavioural security measures, and a keen awareness of the unintended or collateral consequences of digitisation. Researching each of these elements is key for advancing our understanding of trust and security in the digital world – but research on digital trust and security is not free of challenges.

The digital trust and security landscape is broad and includes issues such as:

- How to protect social and digital systems from cyber-attacks, cyber-breaches and/or sabotage, which threaten citizens, businesses, and institutions. Attacks may be technical (for instance on software, hardware, or networks) and/or social-behavioural (for instance social engineering, malicious insiders).
- Understanding offender behaviour and supporting law enforcement and security actions in digital spaces to mitigate the impact of cyber-criminal activities.
- The impact of increased data surveillance, concentration of data and information in powerful organisations, and potential economic or political harms to minority or at-risk communities. And the impact of current and potential political, ethical, and regulatory systems on harm reduction.
- Understanding what security means across varied geographic and cultural contexts. Internet usage, perceptions of data and privacy, and digitally based communities reveal heterogeneous values on privacy, security, fairness, trust, and autonomy.

This course will enable you to understand the nature of digital harms, from online crimes to the malicious manipulation of information, the influence of behaviours and attitudes, and transcending the digital boundaries to effect physical and psychological attacks. We will explore the different ways in which those harms can be reduced or prevented so that you can make well-informed choices about countering security threats in personal, societal and business contexts. Moreover, we will learn about cross-cutting research on digital trust and society and discuss the methodological challenges and opportunities associated with research in this domain.

Course objectives

- Distinguish the nature and range of cyber threats and ways to counter them;
- Identify the skills and knowledge required by professionals working in the industry;
- Gain a general understanding of the opportunities and threats associated with the growth in digital technologies;
- Gain a general understanding of the opportunities and challenges associated with research on digital trust and security;

- Apply this knowledge in your own personal, societal and business contexts;
- Put acquired knowledge and skills into practice to write a blog post or research proposal in teams.

Course requirements

No particular requirements.

Who is this course for?

The course is open to MRes and PGR students, researcher or practitioner who wants to learn about the emergence of new digital harms, the influence of behaviours and attitudes on digital trust and cyber security, different ways in which those harms can be reduced or prevented, and methodological approaches to researching digital trust and security.

Cost

£360

A limited number of bursaries covering 100% or 50% of the course fee are available to current PhD students. To apply, please fill in the following bursary application form no later than two weeks before the course start date: Bursary application form

Book your place

Get your E-store ticket

Course timetable

Monday, 20 June 2022

Afternoon: Introduction to digital trust and security

13:00 – 13:20 Welcome to the Manchester Centre for Digital Trust and Society (Prof Nicholas Lord)

13:20 – 13:50 The digital world (Dr David Buil-Gil)

14:00 – 14:50 Core issues and concepts in digital trust and security (Prof Daniel Dresner)

15:00 – 15:50 Introducing the challenges (Dr David Buil-Gil and Justyna Urbanczyk)

Tuesday, 21 June, 2022

Morning: Digital security and crime: Financial and organised crime

10:00 – 10:40 Financial (cyber) crime (Dr David Buil-Gil)

10:40 – 11:20 Digital currencies and (anti-)money laundering (Dr Katie Benson)

11:20 – 11:50 Organised (cyber) crime (Prof Nicholas Lord)

Afternoon: Digital security and crime: Darknet markets, online sexual exploitation and investigating cybercrime

13:00 – 13:50 Darknet markets (Patrick Shortis)

14:00 – 14:50 The digital component of human trafficking and sexual exploitation (Dr Rose Broad)

15:00 – 15:50 Investigating cybercrime (Prof Daniel Dresner)

Wednesday, 22 June 2022

Morning: Digital harms beyond crime: Data privacy

10:00 – 10:50 Optional sessions

1. How to write a blog post (Dr David Buil-Gil and Justyna Urbanczyk)
2. How to write a research proposal (Dr Chloe Jeffries)

11:00 – 11:50 How do we effectively anonymise data? (Prof Mark Elliot and Dr Claire Little)

Afternoon: Digital harms beyond crime: misinformation, trust in democracy and business

13:00 – 13:50 Reframing Russia for the global mediasphere: From cold war to "information war" (Prof Stephen Hutchings)

14:00 – 14:50 The democratic opportunities and harms of digital technology (Prof Rachel Gibson)

15:00 – 15:50 Impacts of cyberattacks on businesses (Dr Xiuqin Li)

Thursday, 23 June 2022

Morning: Digital systems and cybersecurity: Technology solutions and the workplace

10:00 – 10:40 Cyber security measures for systems (Prof Daniel Dresner)

10:40 – 11:20 Privacy Enhancing Technologies (PETs) to protect user privacy (Dr Mustafa Mustafa)

11:20 – 11:50 Psychological insights to tackle phishing in the workplace (Dr Siddharth Gulati)

Afternoon: Digital systems and cybersecurity: Data analytics

13:00 – 13:50 Data and knowledge-based decision analytics (Prof Yu-Wang Chen and collaborators)

14:00 – 14:50 Geoprivacy and data sharing in research (Dr Eon Kim)

15:00 – 15:50 Challenges

Friday 24 June

Morning: Optional sessions and presentation of challenges

10:00 – 10:50 Optional sessions:

1. Digital tech and crime (Dr David Buil-Gil)
2. Trusted digital systems (Dr Lucas Cordeiro)
3. Workplace and organisational security (Dr Richard Allmendinger)
4. Democracy and trust (Beatriz Buarque)
5. Privacy and trust (Prof Mark Elliot and Dr Claire Little)

11:00 – 11:50 Presentation of challenges

Course leaders

- *David Buil-Gil* is a Lecturer in Quantitative Criminology at the Department of Criminology of the University of Manchester, UK, and Cluster Lead for Digital Technologies and Crime at the Manchester Centre for Digital Trust and Society. His primary research interests are in crime data modelling, victimization surveys, new methods for data collection, and cybercrime. Find out more about his research.
- *Richard Allmendinger* –Business Engagement Lead of Alliance Manchester Business School and Senior Lecturer in Decision Sciences, University of Manchester
- *Katie Benson* – Lecturer in Criminology at the Department of Criminology, University of Manchester
- *Rose Broad* – Senior Lecturer in Criminology at the Department of Criminology, University of Manchester
- *Beatriz Buarque* – PhD Student in Politics at the University of Manchester and Lecturer at King's College London
- *Yu-Wang Chen* – Professor in Decision Sciences and Business Analytics at Alliance Manchester Business School, University of Manchester
- *Lucas Cordeiro* – Reader in ProgAnlys and CyberSec at the Department of Computer Science, University of Manchester
- *Daniel Dresner* – Academic Cyber Security Lead and Professor of Cyber Security at the Department of Computer Science, University of Manchester
- *Mark Elliot* – Professor in Social Statistics at the Department of Social Statistics, University of Manchester
- *Rachel Gibson* – Professor of Political Science in the Department of Politics, University of Manchester
- *Siddharth Gulati* – Research Associate in the Workplace and Organisational Security Cluster of the Manchester Centre for Digital Trust and Society, University of Manchester
- *Stephen Hutchings* – Professor of Russian Studies at the School of Arts, Languages and Cultures, University of Manchester
- *Chloe Jeffries* – Head of Strategic Funding at the Faculty of Humanities, University of Manchester
- *Eon Kim* – Lecturer in Criminology (Digital Tech) at the Department of Criminology, University of Manchester
- *Xiuqin Li* – Research Associate at the Manchester Institute of Innovation Research, University of Manchester
- *Claire Little* – Research Associate at the Privacy and Trust Cluster of the Manchester Centre for Digital Trust and Society, University of Manchester
- *Nicholas Lord* – Professor of Criminology at the Department of Criminology and Director of the Manchester Centre for Digital Trust and Society, University of Manchester
- *Mustafa Mustafa* – Dame Kathleen Ollerenshaw Research Fellow at the Department Computer Science, University of Manchester
- *Patrick Shortis* – PhD Candidate at the Department of Criminology, University of Manchester
- *Justyna Urbanczyk* – Project Administrator at the Centre for Digital Trust and Society, University of Manchester

Recommended reading

Aldridge, J., & Askew, R. (2017). Delivery dilemmas: How drug cryptomarket users identify and seek to reduce their risk of detection by law enforcement. *International Journal of Drug Policy*, 41, 101-109.

Baines, V. (2021). *Rhetoric of InSecurity: The language of danger, fear and safety in national and international contexts*. Routledge.

Barratt, M., & Aldridge, J. (2016). Everything you always wanted to know about drug cryptomarkets* (*but were afraid to ask). *International Journal of Drug Policy*, 35, 1–6.

Brotherton, R. French, C.C., & Pickering, A.D. (2013). Measuring belief in conspiracy theories: the generic conspiracist beliefs scale. *Frontiers in Psychology*.

Elliot, M., Mackey, E., & O'Hara, K. (2020). *The anonymisation decision-making framework*. Second Edition. Manchester: UKAN.

Goldsmith, A., & Wall, D. S. (2022). The seductions of cybercrime: Adolescence and the thrills of digital transgression. *European Journal of Criminology*, 19(1), 98-117.

Holt, T. J., & Bossler, A M. (eds.). (2020). *The Palgrave handbook of international cybercrime and cyberdeviance*. Palgrave Macmillan.

Leukfeldt, R, & Holt, T. J. (eds.). (2019). *The human factor of cybercrime*. Abingdon: Routledge.

Leukfeldt, E.R., Lavorgna, A. & Kleemans, E.R. (2017). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research*, 23(3), 287-300.

Miró Llinares, F., & Johnson, S. D. (2017). Cybercrime and place: Applying environmental criminology to crimes in cyberspace. In G. J. N. Bruinsma & S. D. Johnson (Eds.), *The Oxford handbook of environmental criminology* (883-906). New York: Oxford University Press.

Yar, M., & Steinmetz, K. F. (2019). *Cybercrime and society*. SAGE