7th Strathclyde International Perspectives on Cybercrime Summer School

19th-23rd August 2024, University of Strathclyde

Organisers: Karen Renaud, Daniel Thomas, Andreas Aßmuth, Richard Frank, and Juraj Sikra.

Sponsored by SICSA

sicsa* The Scottish Informatics & Computer Science Alliance

Hosted by the University of Strathclyde's Academic Centre of Excellence in Cyber Security Research: StrathCyber.

in association with National Cyber Security Centre

UKRI Engineering and Physical Sciences Research Council

Academic Centre of Excellence in **Cyber Security Research**

Organising institutions

University of Strathclyde Glasgow

Ostbayerische Technische Hochschule Amberg-Weiden

SFU SIMON FRASER UNIVERSITY

Table of Contents

Schedule

	Start	Length	Session	Topic	Speaker
Monday research symposium August 19th 2024	9:00	30	Registration		
	9:30	5	Session 1.1	Welcome	Karen Renaud (University of Strathclyde, Computer & Informaiton Sciences)
	9:35	30		IT security and AI	Andreas Aßmuth (OTH Amberg-Weiden)
	10:05	45		Human-Centred Security	Ryan Gibson (University of Strathclyde, Computer & Information Sciences)
	10:50	15	Break		
	11:05	30	Session 1.2	Automated Detection of Human Trafficking Ads Through Machine Learning	Richard Frank (Simon Fraser University)
	11:35	30		AI Security Attacks	Manmeet Mahinderjit Singh
	12:05	15		Policy and Capability in Cybersecurity	Partha Das Chowdhury
	12:20	40	Lunch		
	13:00	30	Session 1.3	Cybercrime and Digital Harm: Community and Response Policing of Local Cybercrime in Scotland	Shane Horgan (Edinburgh Napier University)
	13:30	30		Financially Motivated Sexual Extortion (Sextortion)	Katarzyna Owczarek (Police Scotland)
	14:00	30		Identifying Factors that Promote or Deter Cybercrimes Reporting in Scotland	Juraj Sikra (University of Strathclyde, Computer & Information Sciences)
	14:30	15	Break		
	14:45	30	Session 1.4	Security Concerns of Cloud Computing	Mohammad Tayebi (Simon Fraser University)
	15:15	30		Rethinking Security: Biometric Technologies and Human Rights Protection	Birgit Schippers (University of Strathclyde, Law)
	15:45	30		Investigation and evaluation of modern password cracking methods	Theresa Weber (OTH Amberg-Weiden)

	16:15		End		
Tuesday summer school August 20th, 2024	9:30	10	Session 2.1	Introductions	Richard Frank (Simon Fraser University)
	9:40	45		Data Detectives: The OSINT Workshop	Jamie O'Hare (University of Abertay)
	10:25	45			
	11:10	15	Break		
	11:25	45	Session 2.2	Online Child Sexual Exploitation and Victimisation: A place-based approach	Christine A. Weirich (University of Leeds, Law)
	12:10	45		In The Defence of Realm: Challenges of Cyber Security Professionals	Ali Farooq (University of Strathclyde, Computer & Information Sciences)
	12:55	40	Lunch		
	13:35	45	Session 2.3	The Evolving Legal Framework for Ransomware Attacks: Targeting Perpetrators, Networks, or Victims?	Gaia Fiorinelli (Sant'Anna School of Advanced Studies- Pisa)
	14:20	45		Motivations and decision making of cybercriminals	John McAlaney (Bournemouth University)
	15:05	15	Break		
	15:20	45	Session 2.4	Using Data to Disrupt DDoS	Elliott Peterson (Special agent, DCIS)
	16:05		End		
Wednesday summer school August 21st 2024	9:30	45	Session 3.1	Sharenting and Surveillance: The Dangers of Sharing Children's Lives Online	Chelsea Jarvie (University of Strathclyde, Computer & Information Sciences)
	10:15	45		Peering Pressure: Social action against cybercrime at Internet scale	Ben Collier (University of Edinburgh)
	11:00	15	Break		
	11:15	45	Session 3.2	Cybercrime Perspective in ASEAN countries	Manmeet Mahinderjit Singh (Universiti Sains Malaysia)
	12:00	45			
	12:45	40	Lunch		
	13:25	45	Session 3.3	Security Concerns of Cloud Computing	Mohammad Tayebi (Simon Fraser University)
	14:10	45		Keeping the Lights On: The Challenge of Power Network Security	James Irvine (University of Strathclyde,

					Electronic and Electrical Engineering)
	14:55	15	Break		
	15:10	45	Session 3.4	Cybercrime extortion threat and awareness in Saudi Arabia and Scotland	Abdulaziz Alzubaidi (Umm Alqura University)
	15:55	45		It doesn't end with encryption: A tactical approach to strategic decision making	Mark Cunningham-Dickie (Quorum Cyber)
	16:40		End		
Thursday summer school August 22nd 2024	9:30	45	Session 4.1	CHERI and Memory Safety	Jeremy Singer (University of Glasgow)
	10:15	45		Data rights as a research methodology	Tristan Henderson (University of St Andrews)
	11:00	15	Break		
	11:15	45	Session 4.2	Digital Forensic Evidence in Court – A reflection on two recent cases	Ian Ferguson (University of Abertay)
	12:00	45			
	12:45	40	Lunch		
	13:25	45	Session 4.3	Phishing Workshop	Andreas Aßmuth (OTH Amberg-Weiden) Richard Frank (Simon Fraser University)
	14:10	45			
	14:55	15	Break		
	15:10	45	Session 4.4		
	15:55	45			
	16:40		End		
Friday summer school August 23rd 2024	9:30	30	Session 5.1	Revealing Privacy Concerns by Designing a Conceptual Framework for Smart Tourism	Mona Kherees (University of Strathclyde, Computer & Information Sciences)
	10:00	30		Cognitive processes underpinning children's password practice	Maria Lamond (Abertay University)
	10:30	30		Cybercriminal youth networks	Joeri Loggen (The Hague University of Applied Sciences) - Zoom
	11:00	15	Break		
	11:15	30	Session 5.2	Side-Channel Attacks on Physical User Input	Darren Fürst (OTH Amberg-Weiden)
	11:45	45		Assessing Singularities in Cloud Based Applications	Jide Edu (University of Strathclyde, Computer &

					Information Sciences)
	12:30	40	Lunch		
	13:10	45	Session 5.3	Distributed Denial of Service attacks	Daniel Thomas (University of Strathclyde, Computer & Information Sciences)
	13:55	45		Cumulative Revelations in Personal Data: Some methodological insights	Emma Nicol (University of Strathclyde, Computer & Information Sciences)
	14:40	15	Break		
	14:55	45	Session 5.4	Type-Driven Trustworthy System Design	Jan De Muijnck-Hughes (University of Strathclyde, Computer & Information Sciences)
	15:40	45		Closing thoughts	Richard Frank (Simon Fraser University)
	16:25		End		

Abstracts

Abertay University

Dundee - Scotland

Digital Forensic Evidence in Court – A reflection on two recent cases

R.I. Ferguson

cyberQuarter – Abertay University

ian.ferguson@abertay.ac.uk

Whilst the fundamental processes of Digital Forensics are well understood and accepted, the rapidly evolving nature of technology (particularly the IoT) frequently leads to the need to apply those processes in new contexts. The criminal justice process does not always adapt to such rapid change as well as the underlying computer science. This talk will reflect upon two recent criminal cases in which Digital Forensic evidence was key to the prosecution and examine the difficulties associated with presenting a ‘new’ type of evidence. Whilst *prima facia* the type of evidence and process appeared to be novel, by showing that the process was simply an instantiation of accepted methodology on new hardware the admissibility of the evidence was accepted.

Cognitive processes underpinning children's password practice

Maria Lamond, Suzanne Prior, Karen Renaud & Lara A. Wood

Presenter: Maria Lamond

Abertay University

m.lamond2000@abertay.ac.uk

Background and Aims: Children's increasing access to the internet necessitates an age-appropriate approach to cybersecurity education, but the developmental progression of cybersecurity and related cognitive skills is not well understood. We investigated the cognitive processes underpinning children's password practice

Methods: The preregistered study was correlational and involved 147 seven- to 12-year-olds. Cognitive measures included problem solving and working memory from the Wechsler Intelligence Scale for Intelligence (WISC-V), and selective attention from the test of everyday attention for children (TEA-Ch). Children's password practice was assessed by asking children to authenticate on a computer using a given password and a created password with guidance. Password measures included password strength, authentication success, attempts and latency. Additionally, we measured children's digital experience, password creation strategies, sharing practices, and perceptions of their own password practice.

Results: Problem solving positively predicted creating stronger passwords (B=0.123, SE (0.54), Wald =5.15, p =.02). Working memory negatively predicted authentication attempts (B=-0.22, SE= 0.09, Wald =5.96, p=.02). Password strength scores were weak across all age groups. Younger children were significantly less likely to create their own passwords than older children. Children reported sharing passwords with friends, other class members and "anyone that asked".

Conclusion and implications: Password creation and authentication is a cognitively complex task that relies on working memory and problem-solving capabilities. Children did not create strong passwords and require additional support in password practice informed by addressing the cognitive processes that underpin it. Furthermore, children need guidance on password privacy and sharing.

Data Detectives: The OSINT Workshop

Jamie O’Hare

Abertay University

j.o’hare@abertay.ac.uk

This exercise aims to explore various open-source intelligence (OSINT) techniques. Discover how easily accessible data can be used both ethically and maliciously. Through real-life examples and hands-on activities, you will become familiar with uncovering and leveraging publicly accessible information. You will only need a web browser to participate, be it on your laptop, tablet, or mobile phone.

<u>Bournemouth University</u>

Poole - England

Motivations and decision making of cybercriminals

Prof John McAlaney

Bournemouth University

jmcalaney@bournemouth.ac.uk

Cyber-attacks are instigated by people. Whilst it is important to understand the technologies used by cybercriminals it is also necessary to explore the individuals behind these technologies and criminal acts. This not only improves threat detection and prediction of future attacks, but it also provides opportunities to educate individuals interested in hacking on the legitimate careers that can be pursued in cybersecurity. This may help prevent the criminalisation of individuals, especially young people, who have an interest and passion in computing but who are excluded from a cybersecurity career due to being criminalised for participation in a cybercriminal act.

Research into the motivations and decision making has demonstrated that there are myriad and complex reasons why an individual may become involved in cybercriminal activities. Distinctions have been made between those who engage in cybercrime with clear criminal intent for profit, those who become involved in hacking for political or ideological reasons, and those who hack as a form of recreation. However, the lines between these different groups can be blurred, with further barriers to understanding created by the stereotypes and myths that surround cybercrime and the unsurprising reluctance that some cybercriminals actors have for speaking to researchers. Nevertheless, there are means through which insights can be gained into cybercriminal thought processes, such as through the analysis of posts on forums used by cybercriminals (e.g. the CrimeBB dataset managed by the University of Cambridge) and interviews with cybercriminal actors.

In this session we will discuss some of the factors that can influence the cognitions and behaviours of cybercriminals, with a focus on the social psychological processes that may impact individuals working in a group setting – be it as part of an organised cybercriminal gang or an adolescent participating in an online discussion. This includes processes such as fundamental attribution error, in which we misjudge the motivations and competencies of those around us, and the category differentiation model, which states that group coherence and membership can be strengthened by external factors. In doing so it will be demonstrated how cybercriminals are prone to same type of groupthink and other decision-making errors that have been documented in legitimate business and organisations. These processes will be illustrated through quotes from the CrimeBB dataset and linguistic and thematic analysis that we have undertaken on forum discussions. The practical applications of this work and its relevance for law enforcement and prevention strategies will also be discussed, along with future directions of research such as the use of machine learning to map out and identify group processes in cybercriminal organisations.

Defence Criminal Investigative Service

Cyber West Squad

Using Data to Disrupt DDoS

Elliott Peterson, Special Agent

Defence Criminal Investigative Service
Cyber West Squad

The presenter will discuss long running Law Enforcement operations targeting various DDoS (Distributed Denial of Services) services including botnet-based services and booter / stressor services. Highlighting operations spanning 2016 to 2023, the presenter will discuss efforts academic research into these services into the law enforcement planning cycle, and discuss improvements made as a result of this process.

Organisers' note: Previously Elliott Peterson worked with the FBI as a Special agent, where he played a key role in dismantling the Mirai Botnet among his other accomplishments. See for instance:

BizTech (n.d.). *How the FBI investigated and dismantled the Mirai botnet*. BizTech – Security. Available at: https://biztechmagazine.com/media/video/how-fbi-investigated-and-dismantled-mirai-botnet [Video and online article]

Greenberg, A. (2023). *The Mirai confessions: Three young hackers who built a web-killing monster finally tell their story.* Wired. Available at: https://www.wired.com/story/mirai-untold-story-three-young-hackers-web-killing-monster/ [Online article]

Edinburgh Napier University

Edinburgh – Scotland

Cybercrime and Digital Harm: Community and Response Policing of Local Cybercrime in Scotland

Dr Shane Horgan

Lecturer in Criminology, Edinburgh Napier University

s.horgan2@napier.ac.uk

Dr Ben Collier

Lecturer in Digital Methods, University of Edinburgh

ben.collier@ed.ac.uk

The policing of cybercrime as an object of criminological study has grown in popularity in recent years. Extant literature has tended towards focusing on specialist policing functions. Where conventional police responses are the objective of analysis, accounts have remained preoccupied with the challenges cybercrime poses because of its ephemeral, multi-jurisdictional, legal, and non-routine character. As a result, the role of 'local policing' has been, for the most part, neglected. Typically, cybercrime and fraud has been dealt with at a national level in the UK. In 2019, Police Scotland withdrew from Action Fraud and became the primary recorder and responder to cyber-dependent and cyber-enabled offences enabling an interesting view into the nature of what it means to 'respond' to cybercrime. This talk will discuss the findings of a qualitative study of the experiences of frontline officers in Scotland doing just that. We will interrogate their conceptualisation of their role and the 'service' they are providing and explore their reflections on police-community interactions. We will make sense of those experiences their functionality drawing on classic criminological accounts the police. We will argue that, contrary to the narrative of 'challenge', 'limitation' and 'inability' characterising many accounts of public cybercrime policing, frontline police fulfil an important role in responding to cybercrime and that is interestingly victim centred. However, this role may be contradictory to both police and public imaginaries of the 'real' functions of policing. We will suggest that any return to a UK wide system of reporting and response should be pursued cautiously and consider the potential impacts on public confidence, legitimacy and police-community relationships.

Umm Alqura University

Mecca – Saudi Arabia

Cybercrime extortion threat and awareness in Saudi Arabia and Scotland

Abdulaziz Alzubaidi [1] , Juraj Sikra [2]

[1] Umm Alqura university, Saudi Arabia

[2] University of Strathclyde

aazubaidi@uqu.edu.sa

The digital revolution and transformation are impacting our daily lives, allowing us to perform various activities such as finance, education, communication, gaming and more. However, it introduces a series of threats for societies and individuals, and one of those intimidations is sextortion.

Statistics show that 60% of Saudi population are 35 years or younger, with 99% access to the internet, and 20% reported cybercrime. For that, protecting privacy and confidentiality is crucial due to accelerated innovative attacks. Therefore, we aim to develop a framework that relies on raising subject awareness by building an instrument, recruiting subjects, and applying statistical methods for the analysis results.

This framework aspires to be aligned with another study with Scotland's and UK's people to perform a comparison among different environments and backgrounds with the aim of enhancing collaboration and increasing cross-cultural dialogue in an arena of protecting vulnerable victims of cybercrime facing similar challenges.

University of Edinburgh

Edinburgh – Scotland

Peering Pressure: Social action against cybercrime at Internet scale

Ben Collier

University of Edinburgh

ben.collier@ed.ac.uk

Richard Clayton

Cambridge University

We evaluate a rare successful intervention in the management of Internet infrastructure - an anti-spoofing campaign which has achieved genuine traction against an issue that has dogged the network engineering community for more than thirty years. While much scholarship in the security literature has sought to establish the perverse commercial incentives frustrating action against cybercrime and identify possible ways to alter these, in this case we observe a professional community acting to short-circuit them entirely. We develop the concept of infrastructural capital to explain how key actors were able to relocate the issue of spoofing away from the commercial incentive structures of a decentralised community of competing providers and into the incentive structures of a far more densely networked and centralised professional community of network engineers. This extends previous work applying theory from infrastructure studies to cybercrime economies, developing a new account of how power can be asserted within infrastructure to achieve change, apparently against the grain of other long-standing incentives.

University of Leeds

Leeds – England

Online Child Sexual Exploitation and Victimisation: A place-based approach

Christine A. Weirich & Larissa Engelmann

Vulnerability & Policing Futures Research Centre, University of Leeds

C.A.Weirich@leeds.ac.uk

There is little knowledge about how services identify, assess, refer and respond to online child sexual victimisation. In turn, quality standards to promote consistent, evidence-based interventions and community wide approaches is virtually non-existent. Our project is the first attempt, that we know of, to develop a dedicated quality standards tool for online child sexual abuse with the community at the heart of it. Our study is based in Blackpool and takes local challenges, opportunities and idiosyncrasies into account, whilst developing findings and tools that will be relevant for any area where children have access to the internet.

This paper will explore links between online and off-line child sexual exploitation as they relate to current preventative efforts from organisations across police, education, health, social care and the voluntary sector in Blackpool. It aims to: (i) understand how the police, charities, voluntary groups and the public – particularly parents and children – identify and address online child sexual exploitation and the links with vulnerability; (ii) identify how the police can best work with others, including international partners, to anticipate, respond to and prevent online child sexual victimisation and the harms and vulnerability associated with it; and (iii) co-produce a locality-based online child sexual exploitation quality standards framework that can be applied nationally with scope to develop in an international context.

Further discussion will focus on the journey of co-production in developing quality standards and understanding how online exploitation or vulnerabilities of young people are present in Blackpool. It will explore the locally defined and ranked priorities and reflect on the important role children, young people and parents play in this work. This paper will therefore provide the basis for what will be further developed as a national and international model of quality standards that will be piloted and evaluated in other areas to create internationally relevant standards in the response and prevention of online child sexual victimisation. The findings presented will focus on the process and current state of the development of the tool, whilst highlighting the strengths and challenges of a community focussed approach to addressing online child sexual victimisation.

University of Pisa

Pisa - Italy

The Evolving Legal Framework for Ransomware Attacks: Targeting Perpetrators, Networks, or Victims?

Dr. Gaia Fiorinelli

Sant'Anna School of Advanced Studies – Pisa (Italy)

gaia.fiorinelli@santannapisa.it

Ransomware attacks have become one of the most serious forms of cybercrime today, targeting individuals, businesses, and governments, and are increasingly perceived as a threat to national security (White House, 2024). Attackers encrypt data or entire systems, disrupting the victim's operations, and demand a ransom, typically in cryptocurrency, to restore functionality or avoid public disclosure of the data (T-CY, 2022). Europol (2023) notes that these attacks are often carried out by organized cybercriminal groups operating under a business model known as Crime-as-a-Service (CaaS) or Ransomware-as-a-Service (RaaS), that relies on "membership programs" to attract potential collaborators worldwide.

While the number and severity of ransomware attacks continue to grow (NYT, 2024; ENISA, 2022), with some experts fearing that cybercriminals might even resort to "real world violence" (Callow, 2024), governments worldwide are starting to introduce specific legislation to prevent, mitigate, and combat these attacks (Lubin, 2022).

After discussing recent cases targeting public and private organizations in Europe and around the world, and the success story of Operation Cronos (2024), which disrupted one of the world's largest ransomware actors, the talk will focus on the legal solutions and law enforcement efforts currently being developed at the national, supranational, and international levels against ransomware attacks.

These initiatives include strategies such as: (i) criminalizing ransomware attacks in national or international criminal law or increasing existing penalties for cybercriminals; (ii) disrupting organized cybercriminal groups and networks; (iii) developing new technological tools to investigate cryptocurrency transactions (blockchain analytics) or recover encrypted files; (iv) banning ransom payments or making it mandatory for victims to report attacks; (v) strengthening international cooperation and law enforcement coordination; and (vi) improving cybersecurity measures and promoting cyber awareness. To discuss these strategies with participants, some examples will be considered, such as the position of the Council of Europe's Committee for the

Convention on Cybercrime (2022), the solutions adopted in the United States and the United Kingdom, and a law adopted in Italy in 2024, which introduced the crime of cyber extortion and extended the procedural regime for organized mafia-type crime and counterterrorism to attacks on critical or public digital infrastructure. The aim of the talk is to provide participants with case studies on ransomware attacks, highlighting the challenges in prosecuting them, alongside a critical understanding of the pros and cons of various counterstrategies currently in play, targeting perpetrators, groups, or victims.

University of St. Andrews

St. Andrews – Scotland

Data rights as a research methodology

Tristan Henderson, M.A., MSc., PhD.

University of St Andrews – St Andrews

tnhh@st-andrews.ac.uk

Over the past half-century, data protection laws have evolved with a view of strengthening individuals' fundamental rights around personal data and information. One way in which this is done is by placing obligations on data controllers to uphold the data rights of data subjects about which they hold personal data. Such data rights include the right to access, the right to portability, the right to erasure and the right to rectification. We see such rights in laws such as the EU and UK GDPR, and increasingly in other jurisdictions such as the Canadian PIPEDA, the Californian CCPA or the Singaporean PDPA.

Data rights are intended to give individual data subjects an element of control over their personal data. But collectively they can also be used to discover information about data controllers. In this way they can be considered a type of sensor, and one that has been employed in a variety of experiments and studies by researchers in computer science, law and other disciplines.

In this talk I will discuss how data rights can be used as a research methodology. We will look at some of our previous studies with particular reference to data breaches and how to audit data controllers. We will also consider possible pitfalls and ethical dilemmas that arise through the use of data rights in research. I hope to introduce the audience to a new tool that may be of use in your own research.

Bio: Tristan Henderson is a Senior Lecturer in Computer Science at the University of St Andrews, where he is Director of Postgraduate Research and leads the Responsible Computing Research Group. His current research interests revolve around the intersection between computer science and law, with a particular focus on digital rights. Tristan has an MA in Economics, an MSc and PhD in Computer Science and an LLM in Innovation, Technology and the Law, which perhaps explains why he is so confused about interdisciplinary work.

University of Strathclyde

Glasgow – Scotland

Revealing Privacy Concerns by Designing a Conceptual Framework for Smart Tourism

Mona Kherees, Karen Renaud & Dania Aljeaid

Department of Computer and Information Sciences, University of Strathclyde, Glasgow, UK

Department of Information Systems, King Abdulaziz University, Jeddah, Saudi Arabia

mona.kherees@strath.ac.uk

Smart Tourism is the fastest-growing economic sector in the world. Data lies at the core of all Smart Tourism activities as tourists engage in different and personalized touristic services before, during, and after their trips. A massive chunk of information gathered via a plethora of Smart Tourism Technologies is becoming an increasing concern. This may lead tourists to engage in privacy-protective behaviour such as limiting data disclosure, data fabrication, or hesitating to share requested information. Therefore, service providers motivate users to share their personal data by using persuasive tourism marketing elements based on applying different methods such as Cialdini’s strategies. This study extends privacy concerns research in Smart Tourism particularly by investigating whether the use of persuasion methods puts users in harm or makes them vulnerable intentionally or unintentionally. In this context, the present research uses a sequential exploratory mixed methods approach designed in three study phases to investigate the influence of user characteristics and Cialdini’s persuasion strategies utilized by tourism service providers. The first phase proposed and validated a framework based on the Antecedents - Privacy Concerns - Outcome (APCO) framework. The second phase of the study involved the development and validation of the measurement scales. The third phase included a scenario-based experiment to test the proposed model. With data collected from 209 individuals in Saudi Arabia using an online questionnaire, results highlight the role of three persuasion strategies in influencing tourists' privacy concerns and willingness to share personal information.

Assessing Singularities in Cloud Based Applications

Dr Jide Edu

University of Strathclyde

jide.edu@strath.ac.uk

In the field of physics, a singularity is a fundamental concept that describes a point in space-time where gravitational forces become infinitely strong, and the curvature of space-time becomes infinite. This phenomenon is akin to the conditions found at the centre of a black hole, where the density reaches infinite levels, and traditional physical laws cease to apply. The talk will provide an in-depth exploration of mechanism design for detecting singularities in cloud environments, a critically important topic in our modern digital era. The discussion will delve into the methodologies for assessing a service, program, or component when access to its internal workings is limited and scarce interrogative techniques are required to extract security and privacy attributes from it.

Identifying Factors that Promote or Deter Cybercrimes Reporting in Scotland

Juraj Sikra, Karen Renaud & Daniel Thomas

Department of Computer and Information Sciences, University of Strathclyde, Glasgow, UK

juraj.sikra@strath.ac.uk

Cybercrime is under-reported in Scotland, with the reasons for this being poorly understood. To investigate underreporting, we commenced with a search of the related research and then carried out a review of actual cases. Next, to uncover Scottish-specific factors, we qualitatively interviewed 10 Scottish cybercrime victims. It emerged that victims blamed themselves for falling prey to cybercrime and were reluctant to report the incident. This is arguably a direct consequence of the UK government's cybersecurity responsibilization strategy. Informed by our findings, we articulated a national strategy for promoting cybercrime reporting using the MINDSPACE behavioral influence model. Subsequently, we verified this model with a survey of 380 Scottish respondents, a representative sample of the general population in terms of age and gender. We report on and discuss our findings. Finally, we recommend two interventions to inform a national strategy for improving cybercrime reporting in Scotland.

Note: As of 23 July 2024, the full paper has been accepted with corrections into the peer-reviewed "*Journal of Economic Criminology.*"

Cumulative Revelations in Personal Data: some methodological insights

Emma Nicol[1], Jo Briggs[2], Wendy Moncur[1], Leif Azzopardi[1], Burkhard Schafer[3], Amal Htait[4] & Daniel Paul Carey[5]

[1]University of Strathclyde, [2]Manchester Metropolitan University, [3]University of Edinburgh,[4]Aston University, [5]Independent Researcher

emma.nicol@strath.ac.uk

When pieces from an individual's personal information available online are connected over time and across multiple platforms, this more complete digital trace can give unintended insights into their life and opinions, so called “cumulative revelations”. There remains a lack of awareness around the potential for personal information to be correlated by and made coherent to/by others, posing risks to individuals, employers, and even the state. In this interactive session, findings and methodological insights from the EPSRC-funded project Cumulative Revelations in Personal Data will be presented. Attendees will be invited to try out techniques used to support visual sense making and reflection in research interviews on the project. Prototype tools to support personal reflection on the potential visibility of combined digital traces to spotlight hidden vulnerabilities and promote more proactive action about what is shared and not shared online will be introduced.

Human-Centred Security

Dr Ryan Gibson

University of Strathclyde

ryan.gibson@strath.ac.uk

Digital technologies are the driving force behind a more equitable society in that they present vulnerable and underserved populations with access to support networks and opportunities they may otherwise be excluded from. Nevertheless, being active online is a double-edged sword, with users more likely to be exposed to crimes like harassment, stalking, and fraud. Such crimes can easily be avoided through the appropriate application of privacy settings and security software. Yet these technologies are not often developed with end-users who subsequently find them difficult to employ and remain vulnerable online. Using the AP4L project as a case study, I introduce the concept of human-centred security, where a human-factors approach was taken to co-design privacy-enhancing technologies with individuals undergoing significant life transitions. The resulting technologies enhance a sense of resilience throughout the transition and crucially fit into the common disclosure practices being utilised by end-users e.g. monitoring disclosures made across multiple social media profiles, one of which may be dedicated to the individual's transition-related identity.

Sharenting and Surveillance: The Dangers of Sharing Children’s Lives Online

Chelsea Jarvie

University of Strathclyde & CENSIS

Chelsea.Jarvie@strath.ac.uk

Sharing pictures and videos online about family life has become a societal norm, with some parents even making a living as influencers by sharing their parenthood journey. The term “sharenting” refers to parents sharing content about their children online. While sharenting has its benefits such as staying connected with family and friends and helping to create online communities, it also raises critical questions about the privacy and security of children now and as they grow up.

This presentation explores the motivations behind sharenting, such as the desire to maintain connections, the ability to seek advice and support from the parenting community, and to keep an “online scrapbook” to reminiscence about. While discussing these benefits, the risks and concerns will be examined for children’s privacy and the lasting impact this invasion can have as they progress into adulthood. It is prudent to examine the cybersecurity threats posed by sharenting, such as the exposure to predators, identity theft, and the ethical implications of consent and autonomy.

The societal shift to constantly share pictures and videos online has naturally taken the ability to consent away both from adults and children. The ethical implications of parents consenting on behalf of their children and the privacy paradox which follows is a wider impacting risk which needs more attention. This talk aims to provide a comprehensive understanding of the balance needed between sharing online and protecting children’s digital well-being.

Finally, this presentation will explore the emerging risk of surveillance which goes hand in hand with sharenting. As society continues to feed online platforms with rich data about themselves and each other, both governments and corporate entities have a reason to be interested in information about the future generation of our societies. By willingly giving up this private data and information, we must stay abreast of the emerging risks and consequences of current online behaviours, and in particular how this will impact children as they grow into adults and start to navigate modern society on their own.

Keeping the Lights On: The Challenge of Power Network Security

James Irvine

PNDC, Electronic and Electrical Engineering, University of Strathclyde

j.m.irvine@strath.ac.uk

Just as American and British English are ‘quite’ similar – until they’re not! – the security requirements and challenges faced by the Operational Technology (OT) networks used for industrial control are subtly different from the those faced by IT systems. These differences include the fact that the CIA triad – Confidentiality, Integrity, Availability – has different priorities in industrial control systems, and data is less likely to be a focus. This can make attack for financial gain is less likely, but such systems often form part of critical national infrastructure and so nation state actors are a concern. Also, such systems often have a very long working life, meaning systems have to cope with threats which were not even contemplated when they were deployed.

PNDC, an industry engagement centre at the University of Strathclyde, has a large test bed facility to validate the performance of equipment in electrical distribution networks. Cyber security forms an increasing part of this activity, as the grid becomes smarter and more distributed, leading to more opportunities for attackers to compromise the network.

This talk will give an overview of security in OT networks, using power distribution networks as a focus. It will cover the principles of security in such networks, how they are often deployed, key threats and countermeasures including some example attacks, and how these networks are evolving from a security perspective.

Type-Driven Trustworthy System Design

Jan de Muijnck-Hughes

University of Strathclyde

jan.de-muijnck-hughes@strath.ac.uk

The disconnect between System specification and implementation affects system trustworthiness by enabling the risk that our Computer Systems contain vulnerabilities stemming from the disconnect.

We can, however, fundamentally change the way we engineer systems by interlinking specifications and implementations using state-of-the-art advances in programming language research.

In this lecture I will introduce the idea of what type-driven software engineering is, how it can fundamentally enhance system trustworthiness, and the impact on how we develop our computer systems.

Rethinking Security: Biometric Technologies and Human Rights Protection

Dr Birgit Schippers

Strathclyde Law School University of Strathclyde

birgit.schippers@strath.ac.uk

The proliferation of biometric technologies (hereinafter ‘biometrics’) such as facial recognition technology (hereinafter ‘FRT’) in domains as diverse as policing, housing, education or retail, is frequently legitimised with respect to the individual or national security, which these technologies proclaim to provide. Such appeal to security is underpinned by assertions about the accuracy and efficiency of FRT and other biometrics. However, framing security through either individual or national lenses can exclude the experiences of minoritised groups and communities, including ethnic minorities, gender and sexual minorities, and women. They can view the deployment of biometrics, especially FRT, as a form of enhanced surveillance. Instead of providing security, FRT (and other biometrics) is frequently experienced as generating *in*security. This juxtaposition, between the experiences of minoritised groups on the one hand, and the discursive framing of security, which prioritises individuals and states, on the other, has led critical scholars, activists, and the United Nations to propose a shift towards the notion of human security. Human security is defined by its focus on the protection of fundamental freedoms; the protection from threats; and the creation of political, environmental, economic, and military systems that protect people’s survival and their dignity.

This paper argues that a further, more granular shift is required. To understand the group-based and structural dimensions of security, beyond state and individual, this paper prioritises the effects of biometrics such as FRT on groups, specifically groups with protected characteristics, and on human rights, such as freedom of expression or freedom of assembly, which are enjoyed or exercised in concert with others. It also emphasises an analytical focus on FRT’s attending impact on values that are intimately connected with the collective exercise of rights, such as democracy and the rule of law. The conceptual shift proposed in this paper aims to contribute to a better understanding of the complex layers of security, and to develop novel legal responses to the use of biometrics that acknowledges the collective, or social, dimensions of human rights.

In The Defence of Realm: Challenges of Cyber Security Professionals

Dr Ali Farooq, SMIEEE

University of Strathclyde

Ali.farooq@strath.ac.uk

Despite global efforts, cybercrimes are on the rise. The role of cyber security professionals is becoming more crucial than ever. Their expertise is the key to combating the rising tide of security breaches, which have resulted in billions of pounds of damages worldwide, including in the UK. While end-users are frequently labelled as the "weakest link," there is a need to understand the "human factors" beyond the end-users. Security Professionals are also human beings and are susceptible to errors, biases, and limitations that can compromise organisational security.

In this talk, we will explore the multifaceted challenges faced by cyber security professionals by departing from the prolific stance of "end-users as the weakest link" and extending the umbrella of the "human element" to cyber security professionals. We will look at the psychological and cognitive burdens, complexities of decision-making under pressure and consequences when things go wrong. In doing so, we will delve into the impact of workload, stress, and burnout on the performance and well-being of cybersecurity professionals. Moreover, we will discuss the strategies to mitigate these challenges.

This talk will delve into these topics, offer insights from recent research and real-world examples, and broaden the understanding of human factors in cyber security beyond end-users.

Distributed Denial of Service attacks

Dr Daniel R. Thomas

University of Strathclyde

d.thomas@strath.ac.uk

Distributed Denial of Service attacks, where attacks are directed against online systems from many different IP addresses, remain a significant cybercrime type with thousands of attacks per day ranging in severity from kids cheating in online games by using booter services, to actions by nation state actors. This session will introduce Distributed Denial of Service Attacks and detail some of the things we have learnt from studying these attacks since 2014 including the impact of various interventions by law enforcement and their involvement in international events such as physical wars. The main focus will be on UDP reflection-based amplification attacks. The amplification provided by these attacks allows one rented server to generate significant volumes of data, while the reflection hides the identity of the attacker. Consequently, this is an attractive, low risk, strategy for criminals bent on vandalism and

extortion. Nevertheless internationally, police have implemented a range of different types of intervention aimed at those using and offering booter services, including arrests and website takedown.

Publications that will be touched on include the following, as well as work currently under review or accepted for publication:

Vu, A., Thomas, D., Collier, B., Hutchings, A., Clayton, R., & Anderson, R. (2024). Getting bored of cyberwar: exploring the role of low-level cybercrime actors in the Russia-Ukraine conflict, *WWW '24: Proceedings of the ACM on Web Conference 2024* (pp. 1596–1607).
https://doi.org/10.1145/3589334.3645401

Collier, B., Thomas, D. R., Clayton, R., & Hutchings, A. (2019). Booting the booters: evaluating the effects of police interventions in the market for denial-of-service attacks. *In IMC 2019 - Proceedings of the 2019 ACM Internet Measurement Conference* (pp. 50-64).
https://doi.org/10.1145/3355369.3355592

Thomas, D. R., Clayton, R., & Beresford, A. R. (2017). 1000 days of UDP amplification DDoS attacks. *In APWG Symposium on Electronic Crime Research (eCrime) IEEE.* https://doi.org/10.1109/ECRIME.2017.7945057

University Sains Malaysia (USM)

Penang - Malaysia

Cybercrime Perspective in ASEAN countries

Manmeet Mahinderjit Singh

School of Computer Sciences, University Sains Malaysia (USM)

manmeet@usm.my

The ASEAN region's rapid digital transformation has brought significant economic and social benefits while simultaneously increasing exposure to cyber threats. This sharing session aims to provide a comprehensive understanding of ASEAN's digitalisation exposure, associated cyber threats, and regional efforts to enhance cybersecurity resilience. In this session, an overview of prevalent cyber threats within ASEAN and examines regional collaborative efforts to combat these risks through key cybersecurity alliances and initiatives.

A special focus is given to Malaysia's perspective on cybercrime, detailing the country's specific challenges, responses, and strategies. The review extends to the legal and regulatory frameworks within ASEAN countries, assessing their effectiveness in addressing the evolving cyber threat landscape.

Adversarial Machine Learning: A Cybersecurity Perspective

Manmeet Mahinderjit Singh

School of Computer Sciences, University Sains Malaysia (USM)

manmeet@usm.my

Adversarial Machine Learning (AML) poses a growing threat to cybersecurity by exploiting vulnerabilities in Machine Learning (ML) models through techniques like evasion, poisoning, and model inversion attacks. These attacks can lead to incorrect predictions, severely impacting applications in critical sectors such as finance, healthcare, and autonomous systems. This discussion explores the methods adversaries use to deceive models, the implications for cybersecurity, and current defence strategies. By analysing recent advancements and highlighting our research in AML trustworthiness, the importance of continuous innovation and robust defences to protect ML systems from evolving adversarial threats will also be covered.

Ostbayerische Technische Hochschule Amberg-Weiden

Amberg - Germany

IT Security & AI

Andreas Aßmuth

Ostbayerische Technische Hochschule Amberg-Weiden, Amberg, Germany

a.assmuth@oth-aw.de

Artificial intelligence is currently one of the hype topics worldwide. But this overlooks the fact that machine learning has already been used for private, commercial and industrial services and applications for years. Examples include personal assistance systems, the analysis of user behaviour and preferences to make advertising and marketing more effective, or predictive maintenance. The latter is used by industry to recognise any damage to their machines at an early stage to prevent defects and plan maintenance staff deployments more effectively. Machine learning can basically be used for all tasks that involve analysing large amounts of data, recognising special features and patterns in this data, making predictions or classifying this data. In addition, applications of generative artificial intelligence are now also known and in use. Their areas of application include the generation of coherent and contextually appropriate texts, e.g. in chatbots and assistance systems, the generation of programme code in almost any programming language, as well as the generation of realistic images and videos.

During a research semester the intersection of the topics IT security and AI has been thoroughly studied. The focus of this research can be described by three questions:

- How can AI be used to facilitate or improve known cyberattacks?
- What new types of attacks are possible when AI services are targeted?
- How can AI be used to improve IT security against cyberattacks?

In this talk, these three questions will be examined in more detail using examples and possible answers will be given. In addition, two examples of our own work results will be presented: The differentiation of Tor and otherwise encrypted network traffic using three different machine learning methods, specifically investigating the differences concerning the used encryption, and the use of deep reinforcement learning for the purpose of task scheduling in fog computing networks.

Side-Channel Attacks on Physical User Input

Darren Fürst
Ostbayerische Technische Hochschule Amberg-Weiden, Amberg, Germany
d.fuerst@oth-aw.de

A side-channel attack exploits unintended information leaks from a system which is not part of the direct protocol or algorithm to recover information. It is thus referred to as a side-channel as it does not attack the system by obeying only the intended purpose such as breaking an algorithm, but by using ancillary information.

Typical side-channel attacks leverage physical phenomena to infer information such as timing information, power consumption changes, electromagnetic leaks or even acoustic sounds.

One of the first recorded side-channel attacks may be found in a now declassified document from the NSA. During World War II, the US Army and Navy used the Bell Labs' 131-B2 mixing device to encrypt some information. A researcher at Bell Labs noticed that whenever the machine stepped, an electromagnetic spike occurred that could be visualized on an oscilloscope. Upon further investigation, he was able to use these spikes to recover the plaintext from the ciphertext.

After this occurrence, it became evident that while cryptographic methods may be secure in theory, the specific implementation details in hardware and software can also inadvertently provide information that enables the recovery of plaintext information.

In this talk, we will focus on side-channel attacks targeting physical user input, specifically exploring methods to recover information from keystrokes on a keyboard before encryption can be applied.

Common mediums for side-channel attacks on physical user input include:

- Acoustic-based Inference
- Motion-based Inference
- Vibration-based Inference
- Visual-based Inference
- Wi-Fi Channel-State-Information based Inference

We will go over examples for each of these mediums and focus on an acoustic-based attack using a dictionary to recover the typed messages of a target.

Investigation and evaluation of modern password cracking methods

Theresa Weber
Ostbayerische Technische Hochschule Amberg-Weiden, Amberg, Germany
t.weber1@oth-aw.de

The number of cyber-attacks has increased significantly in recent years. You often read in the press that data has been leaked or that a company or authority has been attacked. A very recent example is the attack on TeamView, in which attackers gained access to the company infrastructure. One of the simplest and therefore most frequently used attacks is the cracking of user passwords to gain access to online accounts. This poses an ever-growing threat to users. In addition, artificial intelligence is a global hype and new, efficient AI services are constantly emerging that can be used by anyone - including cybercriminals. Based on these facts, we have analysed and evaluated how effective modern methods for cracking passwords are.

Traditional password cracking attacks are based on dictionaries and rules that are applied to entries of a dictionary. The idea is to use the entries of such a dictionary as candidates for user passwords. A very popular password cracking dictionary is the so-called "rockyou list". This is a list containing passwords from previous leaks. If the candidates don't match user passwords directly, rules are used to modify these dictionary entries, e.g., by appending year numbers or by varying upper- and lower-case letters. Another used dictionary was generated with the help of PassGAN. PassGAN is a neural network that can be trained with passwords to generate any number of passwords independently.

Generative Adversarial Networks (GANs) are a powerful class of deep learning models that can be used to generate highly realistic, synthetic data. They consist of two interconnected neural networks, a generator and a discriminator, which are trained together in a single process. The two networks compete with each other.

We investigated how GANs such as PassGAN can be used to crack passwords. The results of the attacks were compared. The attacks used the dictionary generated by PassGAN on the one hand and the "rockyou list" on the other. We paid special attention to the efficiency, i.e. how many passwords were broken given a certain number of candidates, and to the time, i.e. the duration of the attack.

Finally, we also analysed the quality of the passwords that were cracked. The strength of the passwords, that were broken with the two mentioned methods respectively, was compared.

Police Scotland

Cybercrime Harm Prevention

Dalmarnock - Scotland

Financially Motivated Sexual Extortion (Sextortion)

Katarzyna Owczarek, Police Constable

Police Scotland – Cybercrime Harm Prevention

Throughout 2022 and 2023, in the UK and internationally, there has been an increase in reporting of ‘Financially Motivated Sexual Extortion’– often referred to as ‘sextortion’.
Although victims **of any age** are potential targets, UK-wide data suggests that children aged 15-17 years and adults aged 18-30 are particularly at risk.

The psychological and physical harms caused by sextortion are an immediate safeguarding concern. Victims are extremely fearful of exposure with multiple incidents of self-harm including attempts to complete suicide having been reported.

The presentation will provide a comprehensive overview of sextortion and what it involves, analysis of the crime type statistics, and make recommendations through identifying any gaps or areas for potential action. We will outline what the crime of “sextortion” is, how these crimes are committed and importantly why there has been such an increase in these types of crimes.

What is Sextortion?

Sextortion can refer to a variety of offences committed online. It is most often used to describe online blackmail, where criminals threaten to release sexual/indecent images, unless the victim pays money or carry out their demands.
Sextortion may be:

- Financial blackmail using sexual / indecent images that have been sent to somebody the victim had contact with online.
- Financial blackmail using images that have been stolen from the victim, taken through hacking, or have been faked using AI generators or other image altering technology.
- Blackmail using sexual/indecent images that have been sent to somebody but with a demand for something other than money. This might be a demand for

the victim to do something you don’t want to, like give them use of your bank account or provide more images.

Recognising Sextortion

While victims of Sextortion may feel distressed or blame themselves, they have been tricked or deceived in some way - **it is not their fault.** These threats are often committed by organised criminals motivated only by money. It does not matter if an image was initially shared with your consent or through threats or manipulation - the misuse of your image is an offence **and is never OK.**

Offenders will often pose as other people and send a large number of friend requests to social media accounts quickly. If a new connection engages in sexual chat, or asks for sexual/indecent images, this might be an attempt at sextortion. Sextortion attempts can escalate very quickly or take place over a longer period of time.

Typical signs of sextortion attempts may include:

1. **They’re moving too fast**. They try to develop a relationship very quickly. They might be flirty, tell the victim they like them very soon, or ask for sexual / indecent images and videos. Some may even send a sexual / indecent image first.
2. **They pressure the victim to do things they’re not comfortable with**. They may repeatedly ask the victim to do sexual things they don’t feel comfortable with.
3. **They might tell the victim they’ve hacked you or that they have access to their contacts**. Some blackmailers might tell them they’ve got embarrassing images or information about them from your device. They might threaten to share this information unless money is given to them.

Quorum Cyber

Edinburgh - Scotland

It doesn't end with encryption: A tactical approach to strategic decision making

Mark Cunningham-Dickie

Principal Incident Response Consultant for Quorum Cyber

The speaker has over 20 years of experience in the technology industry, including over a decade working in offensive and cyber investigative roles for law enforcement and other government funded positions.

Grappling with the aftermath of a ransomware attack, organisations face a host of challenges beyond the technical aspects. This presentation delves into the complexities, tactics, and strategies for dealing with legal representation, law enforcement, communications, threat actor negotiations, ransom payment, and managing data release.

Simon Fraser University

British Columbia – Canada

Automated Detection of Human Trafficking Ads Through Machine Learning

Barry Cartwright, Karmvir K. Padda, Noelle Warkentin, Sarah-May Strange, Yuxuan (Cicilia) Zhang, Richard Frank & Mandeep Pannu

Presenter: Richard Frank

Simon Fraser University

rfrank@sfu.ca

Through this project, and through expanded discussions with law enforcement, we identified new adult escort sites that were likely to contain sexual trafficking content, and possibly, newly emerging discourse in the form of images (e.g., animé) and symbols (e.g., emojis or tattoos) that would signify the marketing of the services of sex trafficking victims. We used this information to update and expand our web-crawling scripts, and to scrape as much data as possible from previously identified and newly identified suspect web sites. This data was then input to six different machine-learning (ML) models to understand the effectiveness of ML models in discerning between online escort ads that are likely to involve sex trafficking (and that therefore warrant further investigation by law enforcement officials), and online escort ads that are likely to be posted by consensual sex workers, which would be of little of no interest to law enforcement.

Security Concerns of Cloud Computing

Mohammad Tayebi

Simon Fraser University

tayebi@sfu.ca

According to Gartner, by 2027, over 70% of enterprises will be leveraging industry cloud platforms to drive their business initiatives, a significant rise from less than 15% in 2023. As cloud adoption grows, organizations will need to increase their investment in technology to secure their data, applications, and infrastructure services.

Ensuring the security of cloud technologies involves multiple layers of protection. This includes essential functions such as authentication, authorization, encryption, workload security, and access controls. Additionally, these technologies are crucial for meeting regulatory and compliance standards. They offer robust capabilities for threat detection, risk management, auditing, and monitoring. Furthermore, long-term logging, artifact storage, and detailed activity analysis are integral to maintaining a secure cloud environment.

In this talk, I will delve into the pressing concerns surrounding cloud security. We will examine the inherent risks and vulnerabilities associated with cloud adoption, the difficulties in maintaining compliance with evolving regulations, and the challenges in implementing comprehensive security measures. By highlighting these issues, I aim to provide a clear understanding of the obstacles organizations face in securing their cloud environments.

The Hague University of Applied Sciences

The Hague - Netherlands

The local embeddedness of cybercriminal youth networks: A social network analysis approach

Joeri Loggen[1][2], Asier Moneva[1][3], Arjan Blokland[2][3] & Rutger Leukfeldt[1][2][3]

[1] The Hague University of Applied Sciences

[2] Leiden University

[3] Netherlands Institute for the Study of Crime and Law Enforcement

J.Loggen@hhs.nl

This paper focuses on criminal youth networks engaged in cybercrime. Over the past decade youth involvement in traditional crime has declined, while they are increasingly involved in cybercrime. However, organizations responsible for addressing juvenile crime lack visibility into the cybercriminal activities of traditional criminal youth networks, let alone those focused entirely on committing cybercrimes. Therefore, this paper examines the presence and characteristics of cybercriminal youth networks in the Netherlands. We did this by analyzing 53 police registrations on cybercrime covering September 2022 to September 2023. The registrations consisted of 109 unique suspects and 352 edges, forming 26 co-offending networks, ranging from two to 23 members. Co-offending networks were involved in online fraud (n = 24), sextortion (n = 1), and stalking (n = 1). Moreover, we investigated the local embeddedness of co-offending networks by analyzing travel time between network members, using zip codes and data from Statistics Netherlands regarding travel motives and means of transportation in different age groups of the general population. Based on the largest difference in travel time, mean difference and shortest travel time within each co-offending network, we identified five categories of local embeddedness. First, scattered clustered co-offending networks (n = 5) are characterized by clusters of members living in close geographical proximity to each other, alongside members who are geographically distant. Second, in scattered individual co-offending networks (n = 1), members are spread out, without forming local clusters. Third, locally spread co-offending networks (n = 5) are characterized by members living close to each other, but not forming distinct local clusters. The fourth category consists of co-offending networks (n = 2) that comprise of one or more local clusters, with one or a few members living further away. Last, locally embedded co-offending networks (n = 11) consist of networks with members forming local clusters within small geographical

areas, with sometimes some members living close by, though not part of the networks. Our findings suggest that most co-offending networks in our data exhibit some degree of local embeddedness, though some are more geographically dispersed. This highlights the need for local authorities to enhance their collaboration with partners in other regions to effectively disrupt these networks.