UniKentCyberSec

UniKentCyberSec

Institute of Cyber Security for Society (iCSS)

University of Kent | Institute of Cyber Security for Society (iCSS)

NEWSLETTER

Autumn-Winter 2022-2023

Welcome to the latest issue of the iCSS Newsletter. Every quarter or half a year we send a roundup of the latest news, activities and events we think members of iCSS, external colleagues and organisations will be interested in. If you have any suggestions or feedback, would like to share your news with us, or subscribe to this newsletter, please email cyber-info@kent.ac.uk

We maintain an archive of past newsletters on our website: cyber.kent.ac.uk

Page 2


Page 5


Page 6


Page 8

News

How to be a Cyber Superhero: iCSS aims to get young people engaged with Cyber Security with new animated video

Using electronic devices has become almost a necessity in our day-to-day lives. For this reason, it's never been more important for us to be cyber aware.

The increasing digitalisation of the modern society has been reshaping how we live and do business. This also leads to many new challenges about protecting people and organisations from malicious actors who can now launch attacks in the cyber space more easily than before. Therefore, educating children about cyber security and online safety so that they know how to protect themselves and develop an early interest in a cyber career pathway is very important. This will help fill the current gaps in cyber workforce in all sectors and make our society more prepared for future cyber security threats.

The Institute of Cyber Security for Society (iCSS) at the University of Kent has been active in cyber security and online safety outreach activities, including producing free educational and awareness resources that can be used by schools, teachers, parents and pupils. The latest addition of iCSS's activities in this area is an animated video entitled *How to be a Cyber Superhero*, which was produced to explain to young children in primary schools and early secondary schools about the importance of socio-technical and multi-disciplinary nature of cyber security and a diverse range of career choices. The video was a collective effort of academics, an ICT teacher, and two young school pupils, and professional animation video producer, Scriberia.

Professor Shujun Li, Director of iCSS and the Executive Producer of the animated video, said, 'While online safety is more understood as a socio-technical and multi-disciplinary topic, many people have a misunderstanding that cyber security is such a technical subject that only those who with great ICT skills can do it. We hope the video we made can let more people appreciate the fact that socio-technical and multi-disciplinary nature of cyber security as well as online safety, and all can play a role in making our world securer. We encourage schools, teachers and parents to use the video to introduce more children into the world of cyber security and help diversify our future cyber security workforce.'

To see more about why cyber security is important and where we are with pre-university cyber security education, please read the 2022 report produced by iCSS: 'Pre-University Cyber Security Education: A report on developing cyber skills amongst children and young people'.

Visit YouTube to watch the video.

How can organisations understand the causes of cyber attacks?

iCSS PhD student **Clare Patterson** talked to Dell Technologies on their 'Need to Know' podcast about how organisations can learn to understand incident causation and the underlying causes of cyber attacks. Listen to the full podcast on Spotify.

Clare gained a MSc in Information Security degree in the 1990s, when the organisations principally interested in cyber security were the military and banks. Over the last 30 years, she worked as a consultant and then in industry and decided to take time out to study a PhD degree in Cyber Security at the University of Kent. Her research focuses on how organisations can learn more from cyber security incidents.

The 'Need to Know' series invites leading cyber security specialists and experts to probe into issues and share best practises to combat current and emerging cyber security threats. On this episode of the podcast, Clare talked about her current research into how organisations learn from incidents.

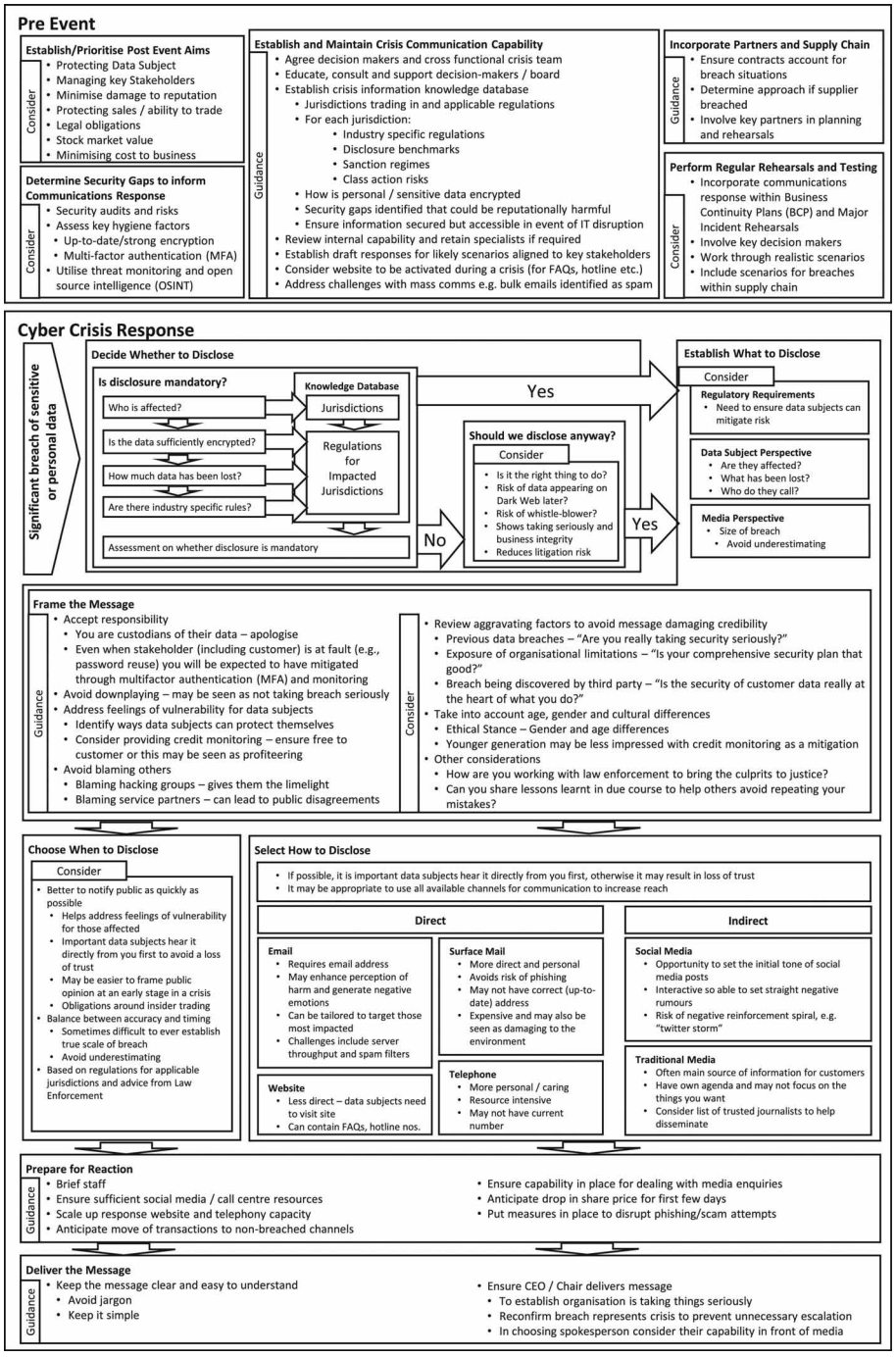
This episode covers the common causes of cyber incidents. Where organisations are under significant pressure to deliver more at lower cost, with over-stretched teams. Although employees try their best, they are often being pushed to deliver more with constrained resources. It can be tempting for practitioners to be enticed by an illusion of 'paradise by prevention' where you have full compliance and full control. However, the requirement to have complete reliability on people and systems isn't realistic in the world that we operate within. When it is understood incidents are enabled by flaws in the overall ecosystem rather than simply caused by one faulty component organisations can tackle the underlying causes to become more resilience. Good learning from incidents – needs leaders who involve the right people and set the right approach to learning.

News

Kent research inspires Cyber Incident Communications Toolkit for universities

On 3 March 2023 the UCISA, a professional body for digital practitioners in education, launched the Cyber Incident Communications Toolkit, created for UK higher education institutions to plan the communications response during a major cyber incident.

The toolkit, which is based on research by **Dr Jason Nurse** focuses on the importance of collaboration both internally and with partners to ensure provision of an effective and coordinated communications response with students, staff, funders, and other stakeholders.



Dr Nurse's research, 'A framework for effective corporate communication after cyber security incidents', details a framework for communications in the event of a cyber incident, and highlights the best practices for effective data breach announcements. The framework is grounded in a systematic review and real-world case studies and includes interviews with senior industry professionals to allow for framework evaluation and refinement.

Dr Nurse's framework can complement security incident response and management in institutions and businesses. He said: 'Universities have increasingly become targets of ransomware and other cyber-attacks. Such attacks can result in major disruption of operations, with significant financial and reputational impact. With the increasing risk of institutions being the target of cyber-attacks, so too has the need grown to understand exactly what is effective communication after an attack and how best to engage with customers, partners and other stakeholders to address their legitimate concerns.

'This research seeks to tackle this problem through a critical, multi-faceted investigation into the efficacy of crisis communication and public relations following a data breach. It does so by drawing on academic literature, obtained through a systematic literature review, and real-world case studies.'

UCISA's use of the framework is the latest in a series of promising impacts of Dr Nurse's work in industry and government. Thus far, the framework has been recommended by CyberScotland, it has been featured in industry, and has won an award at a top cyber security conference.

Dr Jason R C Nurse is a Senior Lecturer (Associate Professor) in Cyber Security in the School of Computing at the University of Kent and the Public Engagement Lead of iCSS. His research 'A framework for effective corporate communication after cyber security incidents' was published in *Computers & Security* in 2020.

The toolkit and accompanying resources are available to UCISA members via login.

News

iCSS hosts the 24th International Conference on Information and Communications Security (ICICS 2022)

From 5 to 8 September 2022, iCSS hosted the 24th International Conference on Information and Communications Security (ICICS 2022) at the main campus of the University of Kent, in Canterbury, Kent, UK. The conference took place as a hybrid event and saw a number of presentations, posters and demonstrations delivered by participants across the world.

The first keynote of the conference, 'Future Challenges in Security Engineering', was presented by **Professor Ross Anderson**, Professor of Security Engineering at University of Cambridge and University of Edinburgh, UK. In this talk, Professor Anderson discussed how the right to software updates for goods with digital elements will affect durable safety-critical goods with software and network connections, like cars and medical devices. If a customer expects software updates for a reasonable time period after purchase, how will teams support security patches and safety for 10+ years, for example? This challenge becomes more complex when taking into account machine learning components, as well as associated costs and practical design limits.

Our second keynote, 'Underspecified Foundation Models Considered Harmful', was delivered by **Dr Nicholas Carlini**, a research scientist at Google Brain. Dr Carlini argued that,

while neural networks are commonly trained to behave as a 'foundation' for future models, this comes at a cost to their security. Although this method may benefit accuracy, unlabelled datasets could, for example, be 'poisoned' to perform various attacks. To address these challenges, new categories of defences would be required, that can simultaneously allow models to train on large datasets while also being robust to adversarial training data.

The third keynote, 'Toward Practical Privacy Protections for Blockchain Networks', was presented by **Professor Guang Gong**, Professor and University Research Chair in the Department of Electrical and Computer Engineering at University of Waterloo, Canada. In this talk, Professor Gong examined the current research in permissionless and permissioned blockchain systems and their potential for applications where value or data is transferred, stored and processed. Professor Gong also provided an example of zk-SNARK (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) schemes.

In addition to the three keynotes, at the Conference there were a total of 11 technical sessions, each of which included 3 or 4 papers. Visit our website for more information on the programme or watch the recorded presentations on YouTube. This year's event also saw winners of six awards, all sponsored by iCSS.

iCSS were delighted to welcome so many visitors to Kent and thank the authors, the presenters and everyone who helped to organise and run the day.

How to transform cyber security learning and make content more engaging

Although many software applications have transformed the way we collaborate and communicate, cyber security training has not advanced in the same way and is often still delivered via web-based learning management systems.

In this Help Net security video, **Dr Jason Nurse**, iCSS's Public Engagement Lead and Director of Science and Research at CybSafe, discusses how delivering cyber security content can be more engaging.

News

Cyber Security & Society: Jason Nurse comments on the internet as it turns 40

On 1 January, the internet turned 40. This date is considered the official birthday of the Internet, thanks to the switch from Network Control Protocol to Transmission Control Protocol and Internet Protocol, a key transition that paved the way for today's Internet.

During its brief but busy life to date, it has revolutionised the way we work, communicate, shop, manage our finances and much more. However, it has also introduced new forms of security risk to our lives, relationships, and business.

Dr Jason Nurse, Senior Lecturer (Associate Professor) in Cyber Security at the Institute of Cyber Security for Society (iCSS) and School of Computing at Kent, has reflected on just how much cyber-crime has affected society over the past four decades, and what we need to look out for as the net continues to evolve. He said:

'As the internet grew, new opportunities for criminals arose. Compared to physical crimes, where there's the relatively high possibility of being caught by law enforcement, cyber-criminals quickly noticed that it was a completely different ball game in the digital sphere.

'A lot of cyber-criminals work in an international context, and for that reason it becomes harder to attribute a crime to someone or to know who has committed what crime. What's more, if they are tracked down in an overseas country, then it is often also more challenging to get them extradited and prosecuted. Once criminals recognised this, and how they could profit from exploiting people online, this is when cyber-crime really took off.

'With the birth of e-commerce, and as more people moved online, attackers recognised the substantial amount of money that could be made via scams, hacking, extortion, identity theft/fraud and a host of other crimes. This catapulted the prominence of cyber-crime. Scam websites started to emerge more and more frequently, and criminals attempted to exploit consumer shopping habits eg Black Friday sales and Christmas (which is why today, online retailers urge customers to be cyber-aware when shopping online). And general hacks skyrocketed on of everything from internet service providers to retailers.

'Retailers had to respond to different forms of technology that consumers used to shop, and in turn, the financial industry and e-commerce really had to prioritise embedding security in the into their systems, and create safe and secure websites and apps. Shoppers needed to know that retailers could protect their credit card information, along with banks – who needed to ensure banking apps were safe, and banks were called on to provide an extra layer of security for customers shopping online.

'The need for cyber security in society reached far beyond e-commerce, however. 'Ransomware', a type of cyber-attack which threatens to block user from accessing a device, and nearly crippled the NHS five years ago, is another big and current cyber security problem. Much like the mentioned NHS incident, the internet has often brought with it risks which needed a quick cyber security response. And whilst experts have acted quickly to respond to threats – as cyber criminals turned their attention from businesses to individuals – consumers have taken a little longer to understand and recognise the risks online.

'Today we are much more educated. We understand the risks involved in online shopping, for example. One area that we still need to make consumers more aware of however, is phishing attempts and wider identity theft. There are a variety of phishing attempts every day, where criminals try to entice people to click on a link to lead them to an unsafe website or action. These websites are incredibly well crafted, so it's often hard to tell if it's a genuine website or not. They're also often based around current events, for instance, in the run up to the World Cup there were a lot of scam emails sent to individuals with the promise of free tickets to Qatar to watch the games if users clicked on a link and entered personal information. These types of attacks are dynamic and the criminals are very mindful of the fact that the average person might not consider the risks when clicking on a link.

'In today's world, social media also poses identity fraud risks to users. Overexposure and oversharing, means that people are often exposing themselves to crime. Users posting names of their pets, or their partner, can be utilised by criminals for password-hacking. Posting where you are, or where you are not, can also translate to an offline risk, along with get-rich scams and online grooming.

'As the internet continues to evolve, we need consumers to be more aware of the risks. The newest technology to the market which carries risks is the Internet of Things – which includes devices such as Nest and Ring smart doorbells. Already we have seen instances where criminals have tried to capitalise on these, such as a man hacking a Ring camera in 8-year-old girl's bedroom, and some of my recent research looks into how misuse of technology, eg tracking apps, can facilitate domestic abuse. Which means that it's not just cyber criminals misusing technology – the evolution of the internet has meant the everyday person can now take advantage of it in the wrong ways.

'However, things are looking more positive as we're moving towards a place where we can start to get people to use the Internet more responsibly. There will be opportunities for things to go really, really wrong, but the aim and the hope is that we can put things in place to address the challenges as and even before they emerge/worsen, whether related to scams, technology-facilitated domestic abuse or online harassment.

'Parliament has recently approved the Product Security and Telecommunications Infrastructure Bill, which seeks to address issues of smart technologies and technology infrastructure to try to ensure that these devices are more safe in their design and implementation. This bill will have a significant impact on what the future, what the future Internet in the UK looks like, and it will have an impact on technology companies such as TikTok, Meta and Twitter – calling on them to make the Internet a safer place, tackling things such as misinformation and addressing online targeting – which must be our priority as the internet continues to grow.'

Dr Jason Nurse is a Senior Lecturer (Associate Professor) in Cyber Security in the School of Computing and the Institute of Cyber Security for Society (iCSS) at the University of Kent. His research interests span smart home technologies, security and privacy awareness, and ways to keep people safe online.

New research projects

A pragmatic approach for generating synthetic data for protecting young people from online harm

iCSS Members Dr Rogerio de Lemos, Dr Marek Grzes, Dr Virginia Franqueira (iCSS Deputy Director) and Dr Tracee Green (Head of Centre for Child Protection) have been awarded £84,409 by the EPSRC-funded REPHRAIN research hub for the project 'A Pragmatic Approach For Generating Synthetic Data For Protecting Young People From Online Harm.'

The overall vision of this project is to investigate the role and provision of synthetic data for developing, evaluating, and comparing techniques for protecting young people from online harm. Since there is no similar initiative in generating and using synthetic data in developing age assurance techniques, the aim of this project is to evaluate the challenges associated with the generation of synthetic datasets. Although we hope to obtain real data or partially synthetic data from relevant stakeholders from which synthetic datasets could be generated, an alternative approach is to use simulations for obtaining fully synthetic datasets. The latter approach is more realistic in the context of dynamic environments, which is the case of social networks where online harm takes place.

This project aims to first, identify and document reference scenarios that are representative of contact online risks. Second, identify key features that are representative of the reference scenarios. Third, evaluate different methods for generating synthetic data in terms of identified features. Fourth, develop a proof-of-concept tool for generating synthetic data associated with the reference scenarios.

Fifth, evaluate the generated synthetic dataset in terms of realism and bias. This theoretical and practical research exercise will provide the groundwork for future research on the field of synthetic data for age assurances by gathering what has been done on related application domain, like insider threats, and by developing a tool that would allow to generate and evaluate synthetic datasets.

Other new research projects funded

A number of other new research projects have been funded via calls from different funders:

- Julio Hernandez Castro and Budi Arief, 'Child-protection based strategies to fight against sexual abuse and exploitation crimes (ALUNA)', funded by the European Commission (Horizon Europe), funding amount to Kent £230,938, 2023-2025
- Marek Grzes and Rogerio de Lemos, 'Reward shaping for network defence based on reinforcement learning', funded by Dstl, funding amount (all to Kent) £301,229, 2023-2024
- Xiaowei Gu and Gareth Howells, 'An explainable generic design of self-evolving intelligent security systems for cyber attack detection', funded by Dstl, funding amount (all to Kent) £122,556, 2023-2024
- Anna Jordanous, Özgür Kafalı and Ioanna Giorgi, 'Discovery knowledge graphs', funded by Dstl, funding amount (all to Kent) £120,272, 2023
- Vineet Rajani and Marek Grzes, 'ML4CI: Machine learning based causal inference for cyber security', funded by Dstl, funding amount (all to Kent) £81,616, 2023
- Budi Arief, 'Playing cyber security games', funded by Dstl, funding amount to Kent £72,835, 2023
- Simon Cooksey and Mark Batty, 'Embedded rust for Morello in defence applications', funded by Defence and Security Accelerator (DASA), funding amount (all to Kent) £87,763, 2023

Education and outreach

Teaching the cyber professionals of tomorrow: CyberFirst sessions for schools

On 28 February 2023, iCSS hosted about 70 Years 8 and 9 school pupils across two CyberFirst sessions of the NCSC (National Cyber Security Centre, part of GCHQ). CyberFirst activities are designed to inspire and encourage students from all backgrounds to consider a career in cyber security. The Trailblazers and Adventurers events are intended to get students thinking about how Computer Science can play a key role in future career prospects and help them to start considering what GCSEs they will choose. Four local schools sent their selected pupils to the day who learn more about cyber security.

Trailblazers

CyberFirst Trailblazers is a free half day event for Year 8 pupils. The students learnt the following:

- Go Create – Learn the basics of how to customise a website and generate enthusiasm to contribute to the World Wide Web
- Digital Detective – Use digital forensics to identify the first person who has contracted a disease and learn how open source intelligence can lead to finding out more information about this person
- Creative Computing – Look into how creative design, arts and technology work together. Take a closer view on how the media industry and advertising combine these elements while having the chance in teams to create your own advert sequence using stop motion.

Adventurers

CyberFirst Adventurers is a free half day event created for Year 9 pupils. The event comprised:

- The Data Games – Understand and use big data to create the perfect team using a set of sports results, compare with others and learn the interpretation of data
- Crack the Code – Against the clock work within teams to unlock various devices, get a taste of cryptography, language analysis and understand some cyber security terms
- Engineering – 3D printers have started to revolutionise the engineering industry, have a look into how technology and engineering fit together and move into the future in partnership. Have the chance to create a model using 3D design software.

The pupils had a great time and were still talking about the day even after it happened!

'I really enjoyed tracking patient zero, and it really opened my eyes to how unsafe our information on the internet.' Peter, Year 8.

Education and outreach

Cyber 9/12 Challenge 2023

The UK Cyber 9/12 Strategy Challenge is a competition designed to foster the cyber security leaders of the future. The competition generates blended learning, effective teamwork and communication skills, critical thinking and analysis and the complementary skill sets that are recognised as essential across all professions and industries that are involved in cyber security, yet often overlooked.

In 2023, iCSS sponsored the four students from the University of Kent to compete in Cyber 9/12. The team had the opportunity to network with employers as well as the other teams, and they were invited to a formal dinner and a keynote speech delivered by the Commander of the UK's National Cyber Force.

Dr Gareth Mott, iCSS's Student Engagement Lead and the University of Kent team's coach: 'It was absolutely fantastic to support our University of Kent Cyber 9/12 Challenge team for the 2023 competition. Having coached two previous teams in the 2021 and 2022 online versions, this year's competition at the BT Tower was a treat for everyone involved. The organisers go out of their way to make the event a unique and challenging experience for the competing students, and the simulation really gets to the crux of the contemporary cyber crises that our interconnected societies could (and do) face, whether tomorrow, in one month's time or in the coming years. Whilst we did not make it to the final stages of the competition, our team received high praise from the judging panel. I'm extremely proud of our team, including for all of their hard work in preparation for the competition and for handling the pressure on the day. Leah, Nur, Utkarsh and Toby – whether you dabble in cyber or delve into cyber for your career pathways, I'm confident you'll excel. Well done.'

Nur Tekin, a team member (School of Politics and International Relations): 'The competition was a challenging but ultimately incredible experience. In the months leading up to it, our team had to tackle various issues and use many skills such as effective communication, delegation, and problem solving. I'm thankful to our coach Gareth for making every effort to help us through this process. On the actual days of the competition, I had a chance to meet and connect with cyber security professionals from both the public and the private sector. This provided me with not only valuable insights into the latest trends and developments in the field, but also potential career opportunities. Although not making it to the final round was disappointing, the efforts made by our team were still recognised by the judges. I was also proud to represent my university and be supported in return. Overall, the Cyber 9/12 Challenge was a once-in-a-lifetime opportunity, and I am thrilled to have participated.'

Leah Arlaud, another team member (School of Politics and International Relations): 'The Cyber 9/12 Strategy Challenge was a truly amazing experience. Even though the preparation took a lot of time and giving a presentation in front of the judges seemed scary at first, it was a very fun and inspiring experience. Even though we did not advance to the next round of the competition, I am very proud of our team's achievements – particularly of our written policy brief which was explicitly praised. Thanks to our coach, we knew what to expect and how to prepare. Talking to different cybersecurity experts also showed me that my non-technical background does not prevent me from starting a career in this field, but that it can even be an advantage. I am also thankful for the financial support that we have received from the University of Kent for traveling and staying in London. It was really a special experience and I am glad I could be part of it!'

Education and outreach

Kent Cyber Security Festival (KCSF) at Kent Youth Summit 2022

iCSS held its Kent Cyber Security Festival (KCSF) 2022 at this year's Kent Youth Summit organised by the University of Kent. The Festival was an opportunity for school pupils in Years 9, 10 and 11 to learn how they can stay safe online, as well as what cyber security might mean in a personal context and as a potential future career.

Two sessions, led by PhD student and iCSS Research Assistant **Krysia Waldock**, was based on mis- and disinformation and the impact of fake news. Disinformation is false information that deliberately causes damage or harm, and misinformation is false information that does not intend to cause harm. In the session, pupils took part in a 'telephone game' to show how fast information can change and be distorted. They were surprised at how fast the message changed at various points down the telephone line! We also compared photographs against deep fake images, including two pictures of cats that were both deep fake images in spite of how lifelike they looked. Pupils really enjoyed the sessions and were able to take some of the critical thinking about different sources away with them.

Krysia said: 'Informing pupils about mis- and disinformation is vitally important given how much information we take from internet sources during our personal and professional lives. This is important knowledge irrelevant of the career path they take.'

iCSS PhD students **Sarah Turner**, **Nandita Pattnaik** and **Matthew Boakes** ran two other sessions focusing on how to keep personal data safe online. This is a tricky topic to talk to teenagers about: they are often heavy users of social media and already know a lot about the types of data they might be providing to these services. The facilitators used this knowledge to introduce different ways that, and the different points at which, data could be compromised when provided to different types of online services.

In order to try and get the participants to start to think about the different reasons people or groups may want to act in certain ways relating to personal data, they were asked to consider the pros and cons of using an encrypted messaging app: What are the benefits that a political activist might see in using such an app? Might the police view the same app as beneficial in the same way? And just how much of your information is protected through the encryption when you use such systems anyway?

Sarah said: 'The provision of – sometimes quite extensive – amounts of personal data in exchange for access to online services is ubiquitous. Teenagers today have grown up with the understanding that such an exchange is fair and, usually, safe and secure. It is important, then, to make sure that as today's teenagers become tomorrow's adults, they understand the positives and the negatives about how these services work, as they are the ones that will have to manage the use of and norms around digital technologies in the future.'

Visit YouTube to watch the festival highlights.

Education and outreach

MSc students completed specialist EC Council certifications

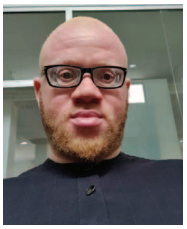
In autumn 2022, we announced an exciting opportunity for our students on the MSc Cyber Security degree course at the University of Kent to further enhance their skills in the competitive job market. This initiative from iCSS sponsored five students on the NCSC-certified MSc Cyber Security, or MSc Computer Science (Cyber Security), towards one of the following EC-Council certifications:

- Certified encryption specialist (ECES)
- Certified incident handler (ECIH)
- Certified security operations center analyst (CSA)
- Certified threat intelligence analyst (CTIA)
- Certified network defender (CND)
- Certified disaster recovery professional (EDRP)

Dr Virginia Franqueira, iCSS's Deputy Director (Education), said: 'This is a concrete opportunity for our cyber security students to graduate with a well-regarded certification on their CV. The sponsorship covered costs related to access to all EC-Council training material for the chosen certification (eg, eBook and iLab) and the corresponding certification exam (one sitting). We were very happy to see the students' success.'

Here's what some of the students had to say about the opportunity on passing their exam.

Cassandra: 'I had the opportunity to take an EC-Council Incident Handler (ECIH) certification, alongside my Masters in Cyber Security at the University of Kent (Canterbury). Having the chance to do courses and certification specifically on incident handling, has allowed me to enrich and improve my knowledge and ability to anticipate, detect and respond to incidents in a theoretical as well as practical way. This is a real asset in the context of my studies with the aim to work as a SOC Analyst.'



Seun: 'I recently completed the EC-Council Disaster Recovery Professional (EDRP) v3 certification, which was self-paced and offered easy-to-understand materials and guided lab sessions. Overall, the EDRP has provided me with a valuable set of skills and knowledge to further my career as a disaster recovery professional. With this certification, I have enhanced my ability to effectively plan, implement, and manage disaster recovery processes for organizations. I look forward to utilizing these skills in my future work and continuing to develop my expertise in this field.'

Gabriel: 'The iCSS' sponsorship of my EC-Council ECIH certification was a not-to-be-missed opportunity that has proved very valuable to my professional development. The training was seamless, and I was particularly impressed by the reactive support of all parties throughout the course. The provided book was also comprehensive, containing a great amount of detail, and the templates provided came in handy in real-life scenarios. The benefits of obtaining the certification were numerous. Not only did it help me gain legitimacy as a professional in my field, but it also allowed me to better understand incident handling-related topics and sharpen my answers to these challenges. Overall, I am grateful for the opportunity provided by iCSS and believe that their sponsorship of my EC-Council certification has had a significant impact on my career growth as a junior cybersecurity consultant.'

Futurum Careers article and Safer Internet Day 2023

On Safer Internet Day 2023, Professor Shujun Li and PhD student Krysia Waldock delivered two sessions, one for Year 7 pupils and the other for Year 8 pupils, at St Edmund's School, using iCSS's new animated video *How to Be a Cyber Superhero* to inspire pupils to think about how everyone can do something to keep the world safer. This is the first time the new video was used in school outreach events, and we encourage more people to use it for such purposes.

They also delivered two other sessions, one for a group of Year 9 pupils at Simon Langton Girls' Grammar School and the other for Year 7 pupils at Kent College, on mis- and disinformation.

The mis- and disinformation sessions drew on an article that iCSS created in conjunction with *Futurum Careers*, 'Online battles: combatting false information and reducing online risks'.

This article is designed to education primary and early secondary school pupils on the dangers of misinformation and the risks that are inherent when interacting online. The accompanying activity sheet helps students to consider the impact of false information via games and discussion topics. These materials are released under the CC BY-NC 4.0 license and we welcome their use for cyber security outreach activities with schools.

CYBER SECURITY

ONLINE BATTLES: COMBATTING FALSE INFORMATION AND REDUCING ONLINE RISKS

These days, we are all online, but it is difficult to have a full understanding of the risks this entails. **Professor Shujun Li** and his colleagues, **Sarah Turner**, **Dr Rahime Belen-Saglam** and **Dr Virginia N.L. Franqueira** at the **Institute of Cyber Security for Society (iCSS),** University of Kent in the UK, are working on enhancing people's awareness of the risks of online false information and sharing personal data online.

PROFESSOR SHUJUN LI

Professor of Cyber Security of School of Computing and Director of the Institute of Cyber Security for Society (iCSS), University of Kent, UK

Related research work

Investigating online false information, cyber fraud, online privacy risks, data protection, cyber security and online safety education

Funders

Engineering and Physical Sciences Research Council (EPSRC)/UK Research and Innovation (UKRI), National Cyber Security Centre (NCSC)/Government Communications Headquarters (GCHQ), Defence

TALK LIKE A... CYBER SECURITY EXPERT

Artificial intelligence (AI) — computer algorithms and systems able to perform tasks that would typically require human intelligence

Crowdsourcing — getting input or information by enlisting a large number of people to contribute

Deepfake — manipulation of existing digital media (image, video and/or audio) – e.g., by swapping faces and changing voices – or creation of new media, typically using machine learning-based techniques such as deep learning

Deep learning — technology able to automatically learn from a large

been learnt to manipulate or create sophisticated media

Machine learning — AI algorithms and systems able to automatically learn from data to perform a specific task

Metadata — a (large) set of data giving information about other data

Misinformation — false or inaccurate information created and spread without an intention to harm others

Disinformation — false or inaccurate information created and spread maliciously, often used for deceptive purposes

Personal data — information

so combining their powers is often a more effective way of identifying false information.

It is not only words that can be misleading, but also non-textual data such as digital images and videos. The rise of powerful image- and video-editing software means that it is easier than ever to construct digital images and videos that look real but are fake or misleading. While some are easy to spot, the advent of more advanced fake-making technologies, such as those behind 'deepfakes', is making it harder to tell fact from fiction. However, advances in technology are combatting this. "Many methods using AI have been developed to automatically detect fake images and videos, and can help human fact-checkers do their job more easily," says Shujun.

Trustworthy experts

To differentiate fact from fiction, Shujun advocates the 'STOP, THINK, CHECK' technique from the Irish *Be Media Smart* campaign (**www.bemediasmart.ie**). "Stop to take time to think, and then think about if and what you need to check," he says. "Stop' involves taking time to read beyond a headline

good reputation on the subject matter, or a media platform with a long-term reputation for accurate reporting," he says.

Personal data sharing

"Sharing some personal information online with some online users is necessary for being part of cyber space," says Shujun. The cyber world offers lots of positives, but many of us are quite lax with our personal data, which is a valuable commodity that can be dangerous if it falls into the wrong hands. "Digital services suck up data about us in different ways," says Sarah Turner, Research Student at the iCSS. "Often, sharing data is an important part of getting full use of a digital platform, helping us connect with friends and contacts, for instance. Additionally, many apps and other digital platforms require access to your data to work correctly."

Threat modelling

Data can seem abstract, and it is all too easy to click the 'Accept' button without thinking too much about the consequences. Sarah suggests thinking about how you share your data in a more structured way.

cause you problems if they access certain bits of your personal information," says Sarah. "What if a possible employer finds questionable tweets you wrote five years ago? What if a mischievous sibling deleted your coursework because they knew your password?"

Games and data

While games can be a great way to relax and escape, they are not excluded from the online data-gathering world. "Most games want to hook you with the gameplay, which can be enriched by using your personal information," says Sarah. "For example, *Animal Crossing: New Horizons* uses your birthday to celebrate your big day and personalise the experience." Games can go further and encourage engagement with other online players, exposing your data more broadly. "Games also collect metadata," she says. "For instance, they can recognise what device you're playing on, and at what times, and details about your internet connection."

Names and birthdays may seem like harmless information to share widely, but Sarah points out it can be problematic. "Data can be stolen and sold to

New publications

Selected new publications

Below are some selected recent research publications of our members:

Altuncu, Enes, **Franqueira, Virginia N L** and **Li, Shujun** (2022) 'Deepfake: Definitions, Performance Metrics and Standards, Datasets and Benchmarks, and a Meta-Review'. arXiv:2208.10913 [cs.CV]. doi:10.48550/arXiv.2208.10913

Bada, Maria, Furnell, Steven, **Nurse, Jason R C** and Dymydiuk, Jason (2023) 'Supporting Small and Medium-sized Enterprises in using Privacy Enhancing Technologies'. Accepted to the 5th International Conference on HCI for Cybersecurity, Privacy and Trust, to be held from 23 to 28 July 2023 in Denmark.

Bard, Dan, **Kearney, Joseph** and **Pérez-Delgado, Carlos A** (2022) 'Quantum advantage on proof of work'. *Array*, 15:100225, Elsevier. doi:10.1016/j.array.2022.100225

Bhattacherjee, Sanjay and Sarkar, Palash (2022) 'Voting Games to Model Protocol Stability and Security of Proof-of-Work Cryptocurrencies'. In *Decision and Game Theory for Security: 13th International Conference, GameSec 2022, Pittsburgh, PA, USA, October 26–28, 2022, Proceedings*, pp. 297-318, Springer. doi:10.1007/978-3-031-26369-9_15

Cartwright, Anna, Cartwright, Edward, MacColl, Jamie, **Mott, Gareth**, **Turner, Sarah**, Sullivan, James, and **Nurse, Jason R C** (2023) 'How cyber insurance influences the ransomware payment decision: theory and evidence'. *The Geneva Papers on Risk and Insurance – Issues and Practice*, 48:300-331, Springer. doi:10.1057/s41288-023-00288-8

Franqueira, Virginia N L, Annor, Jessica A. and **Kafalı, Özgur**. (2022) 'Age Appropriate Design: Assessment of TikTok, Twitch, and YouTube Kids'. arXiv:2208.02638 [cs.CY]. doi:10.48550/arXiv.2208.02638

Jones, Keenan, **Altuncu, Enes**, **Franqueira, Virginia N L**, **Wang, Yichao** and **Li, Shujun** (2022) 'A Comprehensive Survey of Natural Language Generation Advances from the Perspective of Digital Deception'. *arXiv*:2208.05757 [cs.CL]. doi:10.48550/arXiv.2208.05757

Lu, Yang, **Li, Shujun**, Freitas, Alex and Ioannou, Athina (2022) 'How data-sharing nudges influence people's privacy preferences: A machine learning-based analysis'. *EAI Endorsed Transactions on Security and Safety*, 8(30):e3, EAI. doi:10.4108/eai.21-12-2021.172440

Mott, Gareth, **Turner, Sarah**, **Nurse, Jason R C**, MacColl, Jamie, Sullivan, James, Cartwright, Anna and Cartwright, Edward (2023) 'Between a rock and a hard(ening) place: Cyber insurance in the ransomware era'. *Computers & Security*, 128. Article Number 103162, Elsevier. doi:10.1016/j.cose.2023.103162

de Moura, Ralf Luis, **Franqueira, Virginia N L** and Pessin, Gustavo (2022) 'Non-IP Industrial Networks: An Agnostic Anomaly Detection System'. In *Anais do Xxiv Congresso Brasileiro de Automática – CBA 2022*. Presented at the XXIV Brazilian Congress of Automatics (CBA 2022), Brazil: Brazilian Society of Automatic (SBA).

Panteli, Niki, **Nurse, Jason R C**, Collins, Emily and Williams, Nikki (2022) 'Trust disruption and preservation in the Covid-19 work from home context'. *Journal of Workplace Learning*, 35(3):306-321, Emerald. doi:10.1108/JWL-02-2022-0017

Pattnaik, Nandita, **Li, Shujun** and **Nurse, Jason R C** (2023) 'A Survey of User Perspectives on Security and Privacy in a Home Networking Environment'. *ACM Computing Surveys*, 55(9):180, ACM. doi:10.1145/3558095

Pattnaik, Nandita, **Li, Shujun** and **Nurse, Jason R C** (2023) 'Perspectives of Non-Expert Users on Cyber Security and Privacy: An Analysis of Online Discussions on Twitter'. *Computers & Security*, 125: 103008, Elsevier. doi:10.1016/j.cose.2022.103008

Raza, Ali, Tran, Kim Phuc, Koehl, Ludovic and **Li, Shujun** (2023) 'AnoFed: Adaptive anomaly detection for digital health using transformer-based federated learning and support vector data description'. *Engineering Applications of Artificial Intelligence*, 121, Article Number 106051, Elsevier. doi:10.1016/j.engappai.2023.106051

Sağlam, Rahime Belen, **Altuncu, Enes**, Lu, Yang and **Li, Shujun** (2023) 'A Systematic Literature Review of the Tension between the GDPR and Public Blockchain Systems'. *Blockchain: Research and Applications*, in press, Elsevier on behalf of Zhejiang University Press. doi:10.1016/j.bcra.2023.100129

Sağlam, Rahime Belen, Miller, Vincent and **Franqueira, Virginia N L** (2023) 'A Systematic Literature Review on Cyber Security Education for Children'. *IEEE Transactions on Education*, in press, IEEE. doi:10.1109/TE.2022.3231019

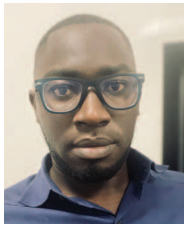
Xu, Yang, Guo, Jie, Qiu, Weidong, Huang, Zheng, **Altuncu, Enes** and **Li, Shujun** (2022) '"Comments Matter and The More The Better!': Improving Rumor Detection with User Comments". In *Proceedings of the 2022 21st IEEE International Conference on Trust, Security and Privacy in Computing and Communications*, pp. 383-390, IEEE. doi:10.1109/TrustCom56396.2022.00060

Zahrah, Fatima and **Nurse, Jason R C** (2022) 'Terrorism and online extremism'. In *Encyclopedia of Technology and Politics*, pp. 62-67, Edward Elgar Publishing.

iCCS Team news

iCSS welcomes the following new members:

Early Career Researcher Members



Rodney Adriko is starting as a PhD student on 08th May 2023 at iCSS, working on Cyber Insurance under the supervision of Dr Jason Nurse.

Rodney has previously completed an MSc in Cyber Security degree at the University of Kent and a BSc in Information Technology from the Makerere University in Uganda. Prior to joining iCSS, Rodney lived in Uganda where he led the Information Technology Audit team of one of the country's biggest players in the Financial Services Sector. He has also previously led similar teams in Cyber and Technology Risk Advisory and Consulting in the Big 4. For his research on Cyber Insurance during his study as a master's student, Rodney was awarded the Chartered Institute of Information Security (CIISec) Student Project of the Year Award from the cyber security student cohort at the University of Kent (2022) and nominated for the inaugural Fred Piper Awards. His PhD research project expands the state of the art by critically investigating how cyber insurance adoption can be increased in Small-to-Medium-sized Enterprises (SMEs) and specifically for the purpose of supporting an enhanced level of security risk management. Rodney is a long-distance runner, footballer and has a great passion for classical music. He is also currently learning to play the flute. He can be contacted via email at ra596@kent.ac.uk

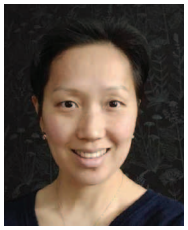
Zsofia Baruwa received BSc Economics (International Marketing and TQM with Upper Second-Class) in Budapest, Hungary. After several years in industry, she persuaded and gained MSc Business Analytics (with distinction) at University of Kent in 2022. Currently she is a PhD Business Analytics student with GTA scholarship under the supervision of Dr Zhen Zhu and Dr Preetam Basu at the Kent Business School. Her research and its associated analyses intend to explore thorough details about priorities, driving forces and econometrics in the process of transitioning towards what we call the future of transportation that could be mined from Social Media. Her particular focus is on autonomous vehicles and how people are ready and willing to adopt this new technology. Her research incorporates methodologies such as big data analytics, social media mining, machine learning, optimization and simulation. At the end of her master's study and the beginning of her PhD study, she worked on an iCSS-funded seedcorn project on blockchain/cryptocurrency as a part-time Research Assistant, under joint supervision of Dr Sanjay Bhattacherjee and Dr Zhen Zhu. The project led to a research paper, which is expected to be published in the near future. More recently, Zsofia started working on the EPSRC-funded project PriVELT as a part-time Research Assistant, working on automatic construction of B2B (business-to-business) ontology, under the supervision of Professor Shujun Li and Dr Zhen Zhu. This new project is closely related to her PhD research topic. More information about Zsofia can be found on the Kent website and on LinkedIn.

Dr Amalia Damianou received an Ing. Diploma in Information and Communication System Engineering from the University of Aegean, Samos, Greece in 2016 and MSc in Information Security from the Royal Holloway, University of London, UK in 2017.

She earned her PhD in Cyber Security and Digital Forensics with her research focusing on Digital Forensic Readiness in Smart Circular Cities from the Bournemouth University, under the supervision of Professor Vasilis Katos and Dr Marios Angelopoulos, in 2022. Currently, she continues to work as a Research Associate in Cybersecurity at the School of Computing under the supervision of Professor Julio Hernandez Castro, working on the European Union's HEROES project, on children protection against sexual exploitation and human trafficking crime and protect their victims. Her research interests include Digital Forensics and Digital Forensic Readiness, image similarity on P2P network, and Blockchain.

Tom Johansmeyer is starting as a PhD student on 23 January 2023 at the Institute of Cyber Security for Society, University of Kent. He is supervised by Dr Gareth Mott and Dr Jason Nurse. Tom is awaiting the results of his thesis for an MA in Global Diplomacy from SOAS, University of London, and has previously completed an MBA at Suffolk University (Accounting) and BA at Ripon College (Philosophy and History), both in the United States. Tom lives in Bermuda, where by day he leads the PCS team, which estimates the insurance industry impact of major risk and catastrophe events, at Verisk Analytics. Under Tom's leadership, PCS expanded from natural disasters into man-made risks, including cyber and political violence. His work has been recognized with awards from CIR Magazine (including the Political Risk Award and Risk Management Champion Award in 2022), Insurance ERM (including risk transfer and ESG over several years), and others. This aligns with the subject of Tom's research, which focuses on impediments to the flow of capital to the cyber insurance market and the attendant economic security implications. Tom is an avid distance open-water swimmer and cyclist (on and off road), a former U.S. Army soldier, and proud father. His work has appeared in Harvard Business Review, Bulletin of the Atomic Scientists, World Economic Forum Agenda, and The SAIS Review of International Affairs, among others. He can be contacted via email at trj5@kent.ac.uk or here.

Associate Members



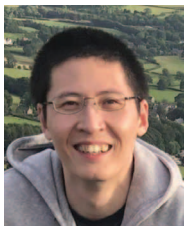
Dr Elena Botoeva is a lecturer at the School of Computing. She received PhD in Computer Science and a Master degree from Free University of Bozen-Bolzano. Prior to joining Kent Elena was a Research Associate in the Verification of Autonomous Systems Group at Imperial College London and a Researcher in the KRDB Research Centre for Knowledge and Data at Free University of Bozen-Bolzano. She has a wide range of research experience with theoretical and practical AI problems such as Knowledge Graphs, query answering over ontologies, accessing relational and NoSQL databases using ontologies, and verification of autonomous systems with neural network components. Her current research interests mainly focus on neural-symbolic architectures for AI applications and applications of machine learning to solving problems from more traditional symbolic domains. More information about Elena is available on the Kent website.

Dr Alexandra Covaci is a researcher in the field of immersive technologies, currently Lecturer in Digital Arts and Technology at the University of Kent. Her research interests include

iCCS Team news

human-computer interaction, with a specific focus on designing and evaluating immersive multisensory technologies for wellbeing, as well as on creative and reflective thinking in design. Her work explores the transformative power of mixed reality in our daily habits such as learning, collaborating, performing / attending performances, or eating. Her publication track includes top journals such as the IEEE Transactions on Visualization and Computer Graphics, International Journal of Human-Computer Studies, ACM Computing Surveys, ACM Multimedia, VRST, CHI and DIS conferences. More information about Alexandra is available on the Kent website.

Dr Tracee Green is the Head of the Centre for Child Protection (CCP) and Senior Lecturer at the University of Kent's School of Social Policy, Sociology and Social Research (SSPSSR). She has taught on CCP's multidisciplinary postgraduate programmes, provided CPD training in child protection and led in the creation of the University of Kent's Social Worker Degree Apprenticeship. She is a registered social worker with 14 years of experience working with children and families. She is currently the PI on an ESRC funded collaboration between CCP and Kent Police aimed at creating a simulation trailing tool promoting trauma informed approaches within police work with young girls who have lived experiences of child sexual exploitation. She is also working on a REPHRAIN funded project looking to develop a synthetic database for research exploring online harms. Tracee's interests are in child protection and education-based research. Her faculty research page can be found on the Kent website.



Dr Xiaowei Gu is a Lecturer in Computing at the School of Computing, University of Kent. Prior to his current appointment, Xiaowei was a Lecturer in Computer Science at the Aberystwyth University, and a Senior Research Associate at the Lancaster University. He received the PhD degree in Computer Science from Lancaster University in 2018, and the MEng and BEng degrees from Hangzhou Dianzi University, China in 2015 and 2012. Xiaowei's research is focused on developing novel machine learning models that 1) have a transparent system structure and human-interpretable reasoning process, and 2) are capable of offering the state-of-the-art performance but with less demand of human expertise involvement. He is also interested in developing explainable semi-supervised machine learning models to tackle streaming data problems. More information about Xiaowei can be found on the Kent website.

Dr Rui Guan is a Lecturer in Economics at the School of Economics. He received his PhD in Economics from the Universitat Pompeu Fabra, as well as Master's degrees from the London School of Economics, Barcelona Graduate School of Economics, and Universitat Pompeu Fabra. Rui's research focuses on behavioural economics and experimental economics that 1) understand how people make decisions, and 2) help them make better decisions. He is especially interested in developing testable behavioural models incorporating evidence from the cognitive sciences and data from emerging technologies. More information about Rui is available on the Kent website.

Dr Mark J Hill is Lecturer in Computational Social Science in the School of Social Policy, Sociology and Social Research. Prior to his role at Kent he was a Postdoctoral Researcher in Digital Humanities with the Computational History Research Group at the University of Helsinki, a Political Theory Fellow in the government department at the London School of Economics, and completed his DPhil in the History of Political Thought at the University of Oxford. His substantive interests grow from a background in political theory and intellectual history with a particular interest in the structural and cultural factors behind political change. His methodological interests meet at the intersection between qualitative data and quantitative methods with a current focus on quantitative text analysis and social network analysis. His current research looks at structural similarities between historical and contemporary social networks. He has been invited to speak at various international events and won awards for both his research and teaching. Mark's faculty page can be found on the Kent website.

Dr Christina Kim is a Senior Lecturer in Linguistics at the University of Kent, and the Director of the Linguistics Lab. Her research combines questions from linguistic theory with methods from the behavioural sciences. Much of her work has focused on aspects of context sensitivity in meaning and interpretation, using behavioural measures such as Visual World eye-tracking, self-paced reading, magnitude estimation, and dialogue games. She has published in high impact linguistics and cognitive science journals, such as Linguistics and Philosophy, Cognition, and Language, Cognition and Neuroscience, and presents regularly at major international conferences in psycholinguistics such as Architectures and Mechanisms of Language Processing and Experimental Pragmatics. More information about Christina is available on the Kent website and on her website here.

Dr Giuseppe Maglione is a Lecturer in Criminology in the School of Social Policy, Sociology and Social Research at the University of Kent, where he is also the Director of the Restorative Justice Clinical Program. He has conducted research on the historical development, philosophical underpinnings and local delivery of restorative justice at the universities of Durham, Cambridge, Oslo and at the Max Planck Institute in Freiburg. His recent works have been published in *The International Handbook of Restorative Justice, Theoretical Criminology, Criminology & Criminal Justice, Critical Criminology and Social & Legal Studies.*

Additionally, he has worked extensively as a victim-offender mediator and trainer in restorative justice in Italy, Scotland and Norway. More information about Giuseppe and his work can be seen on the Kent website.

Dr Lex Mauger is a Reader in Exercise Physiology and the Director of Research and Innovation in the School of Sport and Exercise Sciences.

His principle interests are in restoration and optimisation of human performance, and his research primarily focuses on how unpleasant sensations during exercise impair physiological function and psychological desire to exercise. He is particularly interested in how science and technology can help overcome these deleterious effects.

Within the scope of iCSS, Lex has worked on projects where AI techniques have been paired with wearable technology to help restore (or make decisions on) human physical performance. Therefore, Lex's current interests in iCSS collaborative research are around how enhancing/optimising the human might improve HCI and human-in-the-loop systems,

iCCS Team news

and how AI and HCI technologies might be used to enhance or restore human performance. Lex regularly collaborates across disciplines including computer sciences, psychology, engineering, neuroscience, and pharmacy, and has worked with partners and multidisciplinary teams in industry, healthcare, academia, and the public. His research encompasses young, old, healthy, clinical, and elite athlete populations, and has employed interventions that include non-invasive brain stimulation, virtual reality, pharmacological analgesia, experimental pain induction, and environmental extremes. Using a psychophysiological approach, Lex uses a range of laboratory techniques in his experiments, that include transcranial magnetic stimulation, peripheral nerve stimulation, electromyography, online gas analysis, think aloud, and post-exercise interview. Over the last 10 years his work has received significant funding from NIHR, Dstl, the World Anti-Doping Agency, Research England EIRA, and Arthritis Action. Lex is based in the Division of Natural Sciences, and his webpage can be found here.

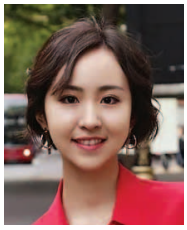
Dr Ben Turner is Senior Lecturer in Political Theory in the School of Politics and International Relations. His research interests lie at the intersection of political theory and the philosophy of technology. He completed his PhD in Political and Social Thought at Kent in 2018 on the work of the philosopher of technology Bernard Stieger, and his first monograph on the relationship between technology and political judgment in the work of Stiegler was published in 2023 with State University of New York press. His current research projects explore the normative foundations of post-work politics, the impact of algorithmic management on workplace democracy, and the political and social impact of quantum computing. In the latter project he is particularly interested in the way that technology can shape democratic and epistemic agency. Up to date information on his work can be found here.

Dr Nikhaela Wicks is a Lecturer in Criminology and she joined the School of Social Policy, Sociology and Social research in September 2021. Prior to this, she taught at the University of Portsmouth (2020-2021) and the University of Westminster (2016-2019). Nikhaela's interests are in policing (both formal and informal methods), race and ethnicity and nightlife and she is a keen ethnographer. Her PhD research, which was awarded a studentship from the University of Westminster, involved a year-long police ethnography with the police, door staff, licensing officers, venue manager and street pastors in the South of the UK. This research involved day and night-time participant observations, interviews and group discussions and draws critical conclusions regarding the racist and discriminatory ways nightlife is governed.

Nikhaela is passionate about sharing her research findings and connecting with scholars in this field both nationally and internationally. She is a member of the International Night Studies Network and the Night Governance working group. She regularly shares her research findings at conferences in the UK and won the 'Best Presentation Award' at the 14th Annual Ethnography Symposium at the University of Portsmouth in 2019. More information about Nikhaela and her work can be seen on the Kent website.

Dr Oscar Zhou is a Lecturer in Media Studies at the School of Arts, University of Kent. Prior to his current appointment, Oscar researched and lectured at the University of Sussex, the University of Brighton, and the University of Hertfordshire. He trained as a communicator and technician scientist at the undergraduate level, before studying for a master's degree in Globalisation and Communications at the University of Leicester, and a PhD in Media and Cultural Studies at the University of Sussex. Oscar's research interests lie at the intersections of ethnographic research, digital communication, mental health studies, and critical youth studies. His work has been published in journals such as Communication, Culture and Critique, Feminist Media Studies, Sexualities, and China Media Research. Drawing upon algorithmic ethnography, Oscar is currently researching and developing how to use TikTok as data, method, and creative digital intervention in youth-led participatory research. More information about Oscar can be found on the Kent website.

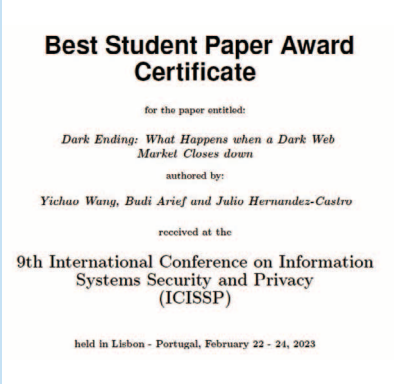
Honorary Member



Dr Xuechen Chen is an Assistant Professor in Politics and International Relations at Northeastern University London and a Visiting Research Fellow at the London Asia-Pacific Centre for Social Science, King's College London. Her research interests include EU external relations with the Asia-Pacific region, China's foreign policy, and norm diffusion in international politics (with a particular focus on global cyberspace governance and non-traditional security issues). Her recent works have been published in International Spectator, European Security, Journal of European integration, and Asia-Europe Journal. Collaborating with Dr Gareth Mott and Dr Harmonie Toros as at iCSS, Xuechen has secured a joint PhD studentship as part of a partnership scheme between Northeastern University London and the University of Kent, on 'Creating, regulating and securing cyberspace: from AI governance, digital trade, to norm diffusion'. More information about Xuechen and her work can be seen on Northeastern University's website.

iCSS PhD student won Best Student Paper Award at ICISSP 2023

Congratulations to iCSS PhD student **Yichao Wang** and his supervisors, Dr Budi Arief and Professor Julio Hernandez-Castro, for winning the Best Student Paper Award for their paper 'Dark Ending: What Happens when a Dark Web Market Closes down,' at the 9th International Conference on Information Systems Security and Privacy (ICISSP 2023).



Best Student Paper Award Certificate

for the paper entitled:

Dark Ending: What Happens when a Dark Web Market Closes down

authored by:

Yichao Wang, Budi Arief and Julio Hernandez-Castro

received at the

9th International Conference on Information Systems Security and Privacy (ICISSP)

held in Lisbon - Portugal, February 22 - 24, 2023

iCCS Team news

Dr Jason Nurse joins Research Institute for Sociotechnical Cyber Security (RISCS) as Co-Chair of Advisory Board

The Research Institute for Sociotechnical Cyber Security (RISCS) is funded by the National Cyber Security Centre (NCSC) and hosted at the University of Bristol. RISCS is the UK's first academic research institute to focus on understanding the overall cyber security of organisations, including their constituent technologies, people, and processes.

The mission of the Advisory Board is to advise on the strategic priorities of the Institute, as well as to support the activities of the RISCS research community and to maximise the impact of this work. The Institute's commitment to deep interdisciplinarity sees the 'real world' expertise of industry and community groups as foundational to its research programme. Accordingly, the Advisory Board members will be asked to advise on:

- growing national capability and expertise in sociotechnical cyber security
- supporting the community of researchers involved in this area
- framing core research questions and future strategic priorities in policy for this area
- reviewing and providing 'critical friend' feedback on research activity.

iCSS's Public Engagement Lead and Senior Lecturer (Associate Professor) in Cyber Security at the School of Computing, Dr Jason Nurse, joins RISCS as Co-Chair of the Advisory Board. In this role, Dr Nurse will guide and support the Board in its remit, and act as a primary contact point with the Director of the Institute.

Dr Nurse currently conducts research in the areas of cyber security, cyber insurance and ransomware, and more broadly concentrates on investigating interdisciplinary approaches to enhance and maintain cyber security for organisations, individuals and governments.

You can read more about his RISCS research in the *RISCS Annual Report 2022/2023*.

PhD Student Sharifah Roziah Binti Mohd Kassim wins Best Paper Award at IEEE DSC 2022

Sharifah Roziah Binti Mohd Kassim, 3rd Year PhD student at iCSS and the School of Computing, together with her PhD supervisors Professor Shujun Li (iCSS Director) and Dr Budi Arief (iCSS Innovation Lead), won the Best Paper Award (Experience and Practice Track) at the IEEE DSC 2022 (5th IEEE Conference on Dependable and Secure Computing), which was held on 22-24 June, 2022, in Edinburgh, UK and online as a hybrid event. The title of their award-winning paper is 'How National CSIRTs Operate: Personal Observation and Experience from MyCERT', co-authored with Dr Solahuddin Shamsuddin, Chief Technology Officer of CyberSecurity Malaysia.

This is an outstanding achievement, as the IEEE DSC Conference is a prestigious conference sponsored by the IEEE Reliability Society.

In 2022, the IEEE DSC conference also includes a category for experience and practice papers on recent findings that predominantly contribute to design know-how or the extension of the community's knowledge about how the security protection of known techniques fares in real-world operations.

Sharifah said: 'We are very pleased to have received this award for what we believe is a significant piece of work that connects research with practice for improving the real-world operations of Computer Security Incident Response Teams (CSIRTs) and the wider security operations.'

This paper provides personal observations and opinions regarding critical areas of operational practices in national CSIRTs, ie, the use of tools and data for investigations of cyber incidents, cyber threat information exchange and collaboration with cross-CSIRT organisations. The authors of this paper hope to induce more promising research to address the gaps identified in the study and contribute to national CSIRTs and cyber security practitioners.

iCSS professional activities

Calls for papers / participation 2023

Call for papers: Fighting cybersecurity risks from a multidisciplinary perspective

This special issue aims to offer a mixture of selected extended versions of papers presented at the European Interdisciplinary Cybersecurity Conference (EICC'23) and accepted papers originating from the public call. We welcome submissions dealing with the abovementioned risks and problems, new challenges, interdisciplinary issues, and innovative multidisciplinary solutions (defense mechanisms, methods, and countermeasures) for promoting cyber security in the cyberspace. iCSS Guest Editor: **Dr Virginia Franqueira**.

Submission deadline: **15 September 2023**

Visit the website for information on how to submit.

Call for papers: Deepfake media in case investigations: Practical implications, interventions and solutions

This special issue aims to improve understanding and foment discussion about practical implications, possible interventions and feasible solutions to the foreseen challenges of deepfake media evidence across civil and criminal case investigations and justice systems for different jurisdictions. We welcome submissions from a range of disciplines, as long as relevant in the context of deepfake media evidence. iCSS Guest Editor: **Dr Virginia Franqueira**.

Submission Deadline: **1 September 2023**

Visit this website for information on how to submit.

Call for participation: NSS 2023 (17th International Conference on Network and System Security) and SocialSec 2023 (9th International Symposium on Security and Privacy in Social Networks and Big Data)

iCSS will host NSS 2023 and SocialSec 2023 conferences as a co-located event from 14 to 16 August 2023 on the main campus of the University of Kent in Canterbury. iCSS will also sponsor a Best Paper Award and a Best Student Paper Award for each of the two conferences. The accepted papers to both conferences have now been selected and a list can be found at this web page. The registration for the conferences is now open and we welcome researchers and practitioners interested in network security, system security, big data security, and online social networks to participate in the event. The early registration deadline for non-authors is **12 June 2023**.

Visit this page for information on how to register.

Call for participation: HAISA 2023 (17th IFIP International Symposium on Human Aspects of Information Security and Assurance)

iCSS will host IFIP HAISA 2023 from 4 to 6 July 2023 on the main campus of the University of Kent in Canterbury. iCSS will sponsor a Best Paper Award and a Best Student Paper Award. The registration for the conference is now open and we welcome researchers and practitioners interested in human aspects of information security and assurance to attend.

Visit this page for information on how to register.

iCSS Professional Activities

Dr Virginia Franqueira (iCSS's Deputy Director) has been nominated as a member of the European Association for Signal Processing (EURASIP) Technical Area Committee on BForSec (Biometrics, Data Forensics, and Security).

Dr Jason Nurse and **Dr Harmonie Toros** have been appointed as members of the EPSRC Digital Security and Resilience Theme's Interim Advisory Group.

Dr Jason Nurse has been appointed a judge for the SC Awards 2023.

Institute of Cyber Security for Society
Keynes College, University of Kent, Canterbury, Kent CT2 7NP
E: cyber-info@kent.ac.uk

UniKentCyberSec **UniKentCyberSec**

Institute of Cyber Security for Society (iCSS)

https://cyber.kent.ac.uk

University of Kent | Institute of Cyber Security for Society (iCSS)

DPC 133615 06/23