ASC Division of Cybercrime
Newsletter

A Conversation with Our Award Winners- Drs. Cassandra Cross and Murray Lee

Thomas Dearden: First, congratulations on winning the best peer-reviewed paper award for the division of cybercrime this past year. For those reading this conversation in the newsletter, I've linked to the award winning paper here. Rather than rehash the paper, I want to learn a little bit about why you decided to tackle romance fraud and fear of crime. What was your motivation for the paper?

Cassandra Cross: I have been studying online fraud victimisation for fifteen years. I first started when I was working as a civilian research analyst within the Queensland Police Service. I remember sitting down with my first romance fraud victim, at a kitchen table in regional Queensland back in 2009, as they recounted the harrowing details of their victimisation. It was evident back then that there was a lack of understanding of online fraud in terms of how it operates, who it targets and the how it impacts individuals. Since then, I have dedicated my research to improving our understandings and responses to online fraud victimisation, and romance fraud remains one of the key categories of fraud requiring attention.

Murray Lee: I've been researching fear of crime on and off for more than 25 years now. One of the big gaps in the research and literature has been knowledge about fear of crime online. We have known it's a serious concern from other research I've been involved in where we asked about people's concerns with online fears. When Cass invited me to write this with her, it was a golden opportunity to explore a component of online fear further.

Thomas Dearden: We've linked to the paper, but if you had to tell us the most important takeaway from the project, what would it be?

Cassandra Cross: I have spoken with hundreds of victims across the years and read through thousands of case reports. While the financial costs of fraud are somewhat obvious, there is a clear and consistent body of research, including my own, which documents the non-financial costs arising from fraud victimisation. This includes a deterioration in physical and mental health, depression, relationship breakdown, unemployment, homelessness and sadly, cases of suicide. These are well known. However, what struck me the most about the findings from this analysis, was the revelation that for a small group of victims, there is an ongoing fear and anxiety in the aftermath of romance fraud, which can have a debilitating and ongoing impact on their wellbeing and sense of physical security.

Read their article here!

Want to be Included?

Send news, events, or stories to Thomas Dearden at tdearden@vt.edu

Cassandra Cross: We often think that when victims cease communication or stop sending money to the offender the matter is over, particularly when the relationship has been conducted entirely online. This is clearly not the case. The results demonstrate that for some, they experience a genuine level of fear and insecurity about their own safety and sometimes that of their families. This fear is real, manifests itself in several different ways and creates an additional level of harm for victims. This is an important factor to note in any efforts to provide support to victims in the future.

Murray Lee: and to elaborate from Cass's response, while intense fear might have been relatively rare in the cohort, for some it was visceral. Some of the stories are actually really hard to read even as short open-ended responses from victims.

> *This fear is real, manifests itself in several different ways and creates an additional level of harm for victims.*

Thomas Dearden: I hear that this is part of a larger project, can you tell us a little bit about the project?

Cassandra Cross: For the past few years, I have been focuses on romance fraud, through analysing over 3,000 deidentified reports received by Scamwatch (an Australian online reporting portal for fraud). Romance fraud sees offenders use the guise of a genuine relationship to gain financial rewards from victims, and it is one of the most brutal types of fraud. Victims experience what is termed the "double hit" of victimisation, where they suffer financial losses, but also must grieve the loss of the relationship. For many, the sense of violation and betrayal is more difficult to cope with than any monetary loss. This project has been examining the free text narratives of these victims to better understand the dynamics behind offending behaviours, and sought to better identify ways to enable improved prevention, disruption, and support. I have looked specifically at the relationship between romance fraud and identity crimes, sextortion and explored the use of military profiles by offenders to target victims. It is a rich, valuable dataset to learn from, but also critical to recognise that each report represents a person who has often experienced something quite traumatic. Their stories deserve action.

Murray Lee: Having been aware of Cass's project for years now, having the opportunity to work together on this paper was an absolute dream. In particular, the data for the broader project provided an opportunity for analysis one rarely get access to.

Thomas Dearden: Certainly we can learn a lot from these victims. Congratulations again, and thanks for taking the time to talk today.

The Division has a Journal? Yes!

The Division Journal is the International Journal of Cybersecurity Intelligence & Cybercrime.

The International Journal of Cybersecurity Intelligence and Cybercrime (IJCIC), a peer-reviewed journal that publishes two issues annually, featuring empirical research articles, policy reports, case studies, and book reviews in the ever-evolving field of cybersecurity and cybercrime. IJCIC's mission is to illuminate the origins, patterns, causes, motivations, and trends of cybersecurity and cybercrime in today's world while also delivering innovative methods and approaches to address existing challenges. The journal homepage can be found Here!

Introductions from the New Executive Board

Kevin F. Steinmetz - Chair: I am a professor of criminology at Kansas State University. My areas of research include hacker culture, online fraud, cybercrime policing, criminological theory, popular culture and crime, inequality and criminal justice, and whatever else seems to catch my interest. I've published multiple books on the subject of cybercrime including Hacked: A Radical Approach to Hacker Culture and Crime (NYU Press), Technocrime and Criminological Theory (Routledge), Cybercrime & Society (Sage), and the forthcoming Against Cybercrime: Toward a Realist Criminology of Computer Crime (Routledge). I was the 2021 recipient of the Critical Criminologist of the Year Award from the ASC Division on Critical Criminology and Social Justice and the 2018 winner of Eastern Kentucky University's Young Alumni Award. I am married to my lovely wife, Pamela, and am the father of two girls, Elsie and Alice. When not working or spending time with my family, I enjoy playing video games. I have spent far too much time thinking about my "Top 5" favorites and think I have them narrowed down to Death Stranding, Earthbound, Silent Hill 2, Bloodborne, and Dark Souls. I'm also a big music lover and play guitar. My favorite artists (at the moment) include Nick Cave and the Bad Seeds, Andy Timmons, The Offspring, Mark Knopfler, and Barenaked Ladies. I recently formed a two piece band tentatively named Flayer and the Ceremorphs.

Claire Seungeun Lee - Vice Chair: I am an assistant professor in the School of Criminology and Justices Studies and a faculty member of the Center for Internet Security and Forensics Education and Research (iSAFER) at the University of Massachusetts Lowell (UML). My research areas include cybercrime, cyberterrorism, cybersecurity awareness and education, and social media. I am a Donahue Ethics Fellow (2021-2023) at UML and a recipient of the U.S.-Korea Future Generations Fellowship (2022-2023) by the Center for International and Strategic Studies. I was honored to be awarded as the 2021 recipient of the Young Faculty Award of the Korean Society of Criminologists in America (KOSCA). I was part of a core team of Northeast Collegiate Cyber Defense League (2022-2023), where we successfully hosted one of the Lazarus members. I love traveling and learning new things and languages. In fact, I won Chinese Language Contests and am a professional Chinese interpreter/translator. As a mother of a young pandemic preschooler, I care much about making the Internet safer and developing a tool for teaching cybersecurity to young kids. I am delighted and fortunate to work with the Division of Cybercrime members as the former Treasurer/Secretary and the current Vice-Chair of the Division. I look forward to having a fruitful discussion about the field, collaborating with you, and getting to know you more!

Cassandra Doge - Secretary/Treasurer: I am an Assistant Professor and Digital Forensics Lab Coordinator in the Department of Criminal Justice and Criminology at Georgia Southern University's Armstrong campus in Savannah, GA. My research areas under the cybercrime umbrella range from the impact of anonymity on online behaviors, to perceptions of online threat, to cybersecurity behaviors. Considering my prior service in the Air Force, it may not be surprising that, outside of cyber, I also study military justice systems, in particular the processing of military sexual assault cases. I'm very much a homebody; I enjoy spending my downtime with my two corgis, Camden and Oaklie, who have been with me for over a decade. When out and about, I am a self-proclaimed performer and vocalist. This occasionally results in participation in musical theater, but I am most likely to scratch that itch through karaoke (less time commitment). I am also an "elder emo" - if the opportunity arises, you can find me at concerts that fit the genres of pop punk, emo, metal, or honestly any rock show.

Lauren Shaprio - Executive Counselor:
My academic path to becoming an Associate Professor in Private Security at John Jay College with an interdisciplinary approach to teaching and research is rooted in my education in computer science, psychology, criminal justice, and law. My research covers three overlapping areas of research—private investigation (e.g., interviewing, evidence), physical security (e.g., offender stereotypes, criminal justice system biases, prejudicial proactive loss prevention strategies), and interpersonal cybercrime (e.g., predators, victims, laws, investigation, harm, security)—and is applicable for criminal and civil cases involving minors as eyewitnesses, victims, or perpetrators. My scholarly work has been published in books and in academic and professional journals; presented at conferences and in workshops; and discussed by reporters in newspapers, television, and podcasts. Beyond what you may learn about me in my bio, my three sons are an equine vet starting rotations, a computer engineering embarking on his career, and a high schooler who is vacillating between a future major in animal science or game design. Like many Developmental Psychologists, I have included them as participants in my research and used their personal experiences to help my students learn various concepts.

Jordana N. Navvarro - Executive Counselor: I am a (soon to be) associate professor of criminal justice at The Citadel in Charleston, South Carolina. My areas of research mainly center on cybervictimization and intimate partner abuse and how these two separate social problems intersect in cyberspace and offline spaces. I am equally passionate about my teaching and research, which has several books about teaching difficult topics using active learning (Understanding Victimology: An Active-Learning Approach, Routledge; Teaching Criminological Theory, Cognella). Aside from service to the Division of Cybercrime, I am very active within the Division of Victimology where I have been recognized for my books and teaching. When I'm not engaged in teaching, research, and service, I am with my partner, Jaret, and our two beautiful young boys (Colton and Jackson). I also maintain a close network of academics, via Discord, where we bond over shared love for World of Warcraft.

James Popham - Executive Counselor: I am an associate professor and the chair of the department of criminology at Wilfrid Laurier University. I started researching music piracy in 2003 for my honours thesis and have continued to study the subject in one form or another since then. My inspiration to study this subject came from personal experiences with pre-napster forms of piracy, which included frequent visits to various IRC channels to locate FTP coordinates. I'm currently under contract with the Oxford University Press to write An introduction to cybercrime in Canada, with additional projects on grade-school interventions to mitigate online hate, adults' experiences seeking support following online harassment, and developing methods for analyzing online discord. I often balance the primarily digital nature of cybercrime research with in-person fieldwork that supports non-profit and community organization, focussing on strategic planning, policy development, and program evaluations. Outside of my academic occupations I spend most of my time with my partner Cara and our two sons Riley (11 years old) and Allister (7 years old). This involves many peanut butter sandwiches and frequent visits to our seasonal campsite near Paris, Ontario. Like Kevin, I'm a frequent gamer: my xbox tag is PoppsJ and if you find me please feel free to trounce me in a friendly game of Halo.

Cathy Marcum - Immediate Past Chair: I am a professor of Justice Studies, as well as the Chair of the Department of Government and Justice Studies, at Appalachian State University. My areas of expertise include personal cybervictimization and offending, as well as correctional issues and sexual victimization. I have over 60 peer-reviewed publications and multiple textbooks in these fields. I was honored to be awarded the 2022 Indiana University of Pennsylvania Distinguished Alumni Award and the 2020 ACJS Corrections Section Member of the Year. I am extremely fortunate to have a very patient husband, Jeff, and two children, Drew and Maddy, who are willing to have unusual conversations at the dinner table about these issues. My dog, Lego, could care less. When not contemplating ways to make the Internet safer for young people, I enjoy watching British baking shows and movies from the 80s and 90s with my kids. I absolutely love to travel to new places, and my life goal is to meet the Mandalorian (yes, he is real, so don't judge).

Thomas Dearden - Archivist: I am an assistant professor of Sociology at Virginia Tech. My research focus is technology and crime. I currently have 15 peer-reviewed articles and more than 30 professional conference presentations. Recently I had an opportunity to lend techincal expertise to bestselling author David Baldacci. I've also conducted research and consulted for organizations and law enforcement agencies across the globe. This work has led to numerous professional reports, one patent, and educational courses in more than 70 jails. I love all things outdoors, especially kayaking, mountain biking, and frisbee golf. Recently I've been reconsidering these adventures after having a wasp flying into my mouth while biking. Also my professional photo shows that I have two ears. This is a lie.

Jin R. Lee - Early Career Award

I asked Jin R. Lee, our Early Career Award winner, what led him to cybercrime research and where he was planning to go from here:

My interest in cybercrime and cybersecurity research stems from my fascination in understanding the role and impact of digital technology on human behavior. Growing up, I witnessed the positive advancements computer technology has on society, as well as the negative consequences it can have if misused for harm and abuse. My initial research interests in cybercrime and cybersecurity revolved around understanding the causes and correlates of online interpersonal violence, including cyberbullying and online harassment. The enthusiasm around developing a deeper understanding of online interpersonal violence was a direct result of my exposure to peers and family members who had experienced these behaviors. While I remain passionate about examining the etiology of online interpersonal violence behaviors and identifying effective intervention measures to combat these offenses, I have expanded my research agenda to exploring various computer-dependent crimes with harder to reach samples. This includes examining the predictors of computer hacking, online fraud, and illicit Dark Web market economies.

Both my current and future research plans involve building an evidence-based understanding of cybercrime and cybersecurity. While research exploring cybercrime has grown in recent years, limited studies have identified evidence-based solutions for various online behaviors and cybersecurity inquiries. While theoretical knowledge and insight remain crucial to our understanding of online phenomena, my ongoing research agenda strives to generate translational knowledge that identifies effective policies and mechanisms that mitigate the negative consequences of cybercrime and online deviance. This includes implementing novel data collection methods, greater collaboration with computer science and engineering researchers, and conducting innovative analysis techniques to further our comprehension of cybercrime and cybersecurity in emerging areas.

My favorite upcoming project involves using a variety of different machine learning and artificial intelligence (AI) tools to identify key features in influential online extremist posts and develop novel ways to counteract mis-, dis-, and mal-information across mainstream online communications platforms. This project has the potential to combat domestic extremism across the ideological spectrum through effective counternarrative campaigns. Overall, this upcoming project represents a novel, multi-level, and multi-platform AI-assisted approach to countering both the dissemination of extremist content and the mobilization of violent extremism.

Book Review
Cyberpredators and Their Prey
by Lauren Shapiro
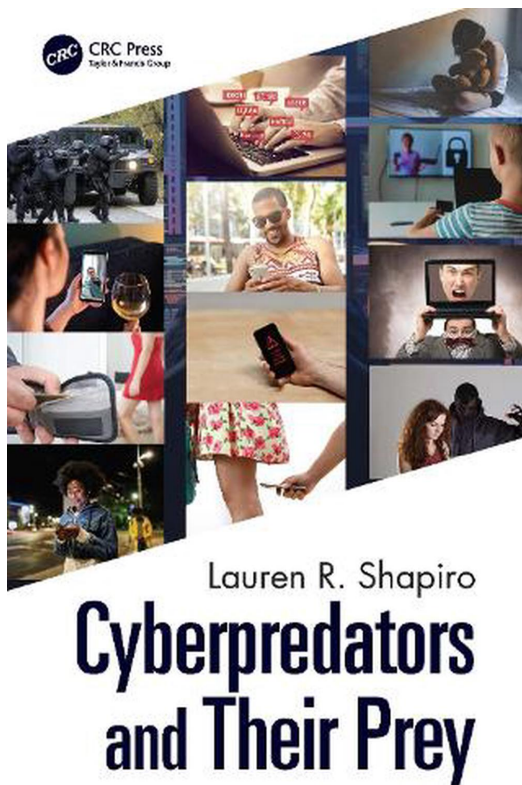
Computer-related crime manifested itself on the world stage roughly in the early 1980s. Yet to this day the theories of Beccaria (1762) and Lombroso (1876) continue to dominate criminal justice curricula. Cybercrime, digital forensics, et al, have yet to take their place as the force de jour among criminal justice courses, as they should in the Information Age. The author is not the first to recognitive the need to crawl out of this discipline's basement. But this scholar has done an impressive job of clambering into the 21st century. What is offered in support of this claim?

First and foremost, this textbook does an extraordinarily credible job of discussing its primary objective: child exploitation and the mindset of its cultists. Among other nuggets of gold, the sources are virtually all from this century; citations are current (most from the past five years). In and of itself this is noteworthy because it is atypical. Pick up any CJ textbook; too many are replete with 20th century--or older--sources. The preface identifies five areas intended to provide practical information to readers. "Most importantly is the issue of whether Internet and social media platforms are taking responsibility for their role in cybercrime . . ." This is accomplished adroitly and succinctly. Thus, practitioners will be better served than by a purely theory-based discussion of topics.

A masterful job is done of addressing the statutes used to prosecute these particularly loathsome miscreants. The case studies of both criminal prosecutions and civil cases are instructive. References are conveniently placed at the end of each chapter rather than collectively at the end of the text. Cyber security tactics also follow each chapter. These differences elevate the text from mere theory alone to its stated objective of providing practical information to readers. Thus, the heart of this text it true to its stated goal.

A discussion of Routine Activity Theory is addressed in the concluding chapter, the theoretical link. But the majority of the text's topics are pragmatically based. This too will appeal to practitioners as well as those intending to seek employment in law enforcement.

No text nor tome on any subject can cover every topic within a genre. However, suggested for the second edition of this fine work should include: A chapter on the Dark web and Deep Web of the Internet, wherein cyber predators lurk, searching for new ways and means to elude detection by law enforcement. Overall, Dr. Shapiro's Cyberpredators and Their Prey is a worthy contribution to this subject's literature.

William L. Tafoya, University of South Florida

Announcements!

Job Posting:

Senior Lecturer in Criminology (Level C) - University of Adelaide, Australia

$125,537 to $144,368 per annum plus an employer contribution of 17% superannuation.

Continuing (tenured), balanced (research and teaching), and full-time opportunity.

This Senior Lecturer in Criminology opportunity is available immediately. While the area of research specialisation is open, priority will be given to applicants with a track record in cybercrime, digital criminology, policing, or digital forensics. The successful candidate will have demonstrable experience in the field of Criminology. This will include tendering a strong track record of high-quality research outputs in the discipline, as well as having had experience designing and delivering Criminology courses, as well as using innovative teaching methods.

The School of Social Sciences is an intellectually stimulating place to work – combining an innovative teaching environment with a strong research culture. It is also home to both the Adelaide Cybercrime Laboratory (www.adelaidecybercrime.org), and Stretton Institute (www.adelaide.edu.au/stretton/) which are both vibrant research hubs at the University of Adelaide.

Applications close May 21. For more information visit:
https://careers.adelaide.edu.au/cw/en/job/511808/senior-lecturer-criminology

The 2023 White Hat Conference, hosted by Boston University Metropolitan College's Criminal Justice Graduate Programs and the Center for Cybercrime Investigation & Cybersecurity with support from the Department of Justice's (DOJ) Bureau of Justice Assistance (BJA), will gather cybersecurity stakeholders from government, the private sector, and academia to highlight challenges modern law enforcement face in combatting online child abuse and address developing and potential solutions.

You can now register for the Fourth Annual International White Hat Conference, May 31–June 2, 2023, hosted by the Criminal Justice Programs and Center for Cybercrime Investigation & Cybersecurity at Boston University's Metropolitan College (MET).

This year's gathering of cybercrime-fighting professionals will explore "Targeted Means to Combat Online Child Exploitation and Victimization." You can choose to attend on campus or virtually, and, as before, the conference is free to attend.

Join us at the 2023 White Hat Conference, a free, hybrid event (both virtual and in-person) dedicated to combating the online sexual exploitation of children. Register now to be at the forefront of this crucial fight and help make a difference

https://live.bu.edu/whitehat/