



ASC Division of Cybercrime Newsletter

Volume 1, Issue 1

Spring 2021

"We are just getting started!"

Thank you for the support for the new Cybercrime Division

By Dr. Cathy Marcum
Chair, ASC Cybercrime Division

Hello Division of Cybercrime (DC) members! The Executive Board and I would like to thank you for your overwhelming support since we took over in January 2021. It is extremely important to us to best represent the needs of the membership with the scheduling of events and creation of policies as we move forward. Our goal for 2021 is to expand the sponsored experiences by the DC, stressing the importance of well-rounded exposure to all the facets of cybercrime and cybersecurity. In addition, it is of utmost importance to facilitate opportunities for graduate students in the field to network and participate in events.

A huge thank you to our Historian, Dr. Jennifer LaPrade, for her amazing work on our new DC newsletter! This newsletter and future publications will feature upcoming events involving our members, as well as opportunities for membership participation. We were very excited about our spring workshop series which highlighted



the work and expertise of many of our DC members and those in the cybercrime and cybersecurity fields.

In June 2021, the White Hat Conference will also highlight many of our DC members, facilitating an amazing experience for students and academics in the field. Further, we have six roundtables sponsored by the DC under submission to the American Society of Criminology program committee.

I personally want to thank our officers, Dr. Sinchul Back and Dr.

Claire Lee, as well as the Executive Counselors, Dr. Erica Fissel, Dr. Jordana Navarro and Dr. Kevin Steinmetz, for all their work on taking the DC to the next level. Thank you to the committee members on the Constitution & Bylaws and Awards Committees for their hard work, as well as all our Liaisons to our international organizations. Lastly, I am extremely grateful for the support of the DC leadership who recently transitioned off the board: Dr. Adam Bossler, Dr. Kyung-Shick Choi and Dr. Tom Holt.

We are just getting started! If you have any ideas for events, workshops or other activities for our members and individuals in the field of cybercrime and cybersecurity, please reach out to me or any of the Executive Board members. We are happy to help facilitate and promote these opportunities. If you have not found us on social media, follow us on Twitter at [@AscCyber](https://twitter.com/AscCyber) or on Facebook on the [ASC Division of Cybercrime](#) group page.

This is going to be a great year!

Follow us on Twitter [@ASCyber](https://twitter.com/AscCyber) and [Facebook](#)!

SPRING WORKSHOP SERIES

Dark Web & Cyber Fraudsters

The ASC Cybercrime Division hosted its first virtual workshop in the spring series on March 26, with Dr. Scott Belshaw, associate professor and Director of the Cyber Forensics Lab at University of North Texas, sharing his groundbreaking work on dark web research.

About four years ago, while working with law enforcement officials on digital forensics, Dr. Belshaw was able to obtain grants to expand this work and started the Cyber Forensics Lab. The lab is now a research institute focusing on two major issues--the dark web and gas pump skimming.

The first issue is the dark web. "I started talking to a lot of law enforcement and they just didn't have an understanding of the dark web," Dr. Belshaw said. Dark web research in academia was also sparse, therefore, he believed his lab could help increase knowledge and understanding of the dark web.

To achieve this goal, Dr. Belshaw said the university installed a separate subnet so that he could access the dark web without fear of intrusions, since so much malware comes through the dark web.

Secondly, Dr. Belshaw found there was a lack of research on gas pump skimmers, which capture



"The dark web is essentially a criminal neighborhood that has never been looked at. There is a huge need for more research in this area."

----Dr. Scott Belshaw

credit card information of unknowing users at the gas pump. Therefore, the lab also works to gain a better understanding in this area.

This presentation focused on his lab's work on the dark web. "The dark web is essentially a criminal neighborhood that has never been looked at," Dr. Belshaw said. "There is a huge need for more research in this area."

His new book, *Dark Web: Unfiltered* examines the dark web and how it is used for a wide variety of illegal activities. He explains that the dark web is a place, below the surface internet that most of us use, where people can anonymously exchange information such as illegal porn and make drug sales. In some countries, such as China, getting on the dark web is punishable by prison time. "What I'm trying to do for us as academics is illuminate the need to go beyond that top part of the internet because the bottom part is where all the criminal activity is going on," Dr. Belshaw said.

Dr. Belshaw encourages criminal justice faculty to include teaching about the dark web in their classes. He said we are in this movement to teach cyber and the importance of cybercrime and cybersecurity to criminal justice professionals,

but to really accomplish this we must include the dark web. He said as soon as we do that, we train our students to not only become better scholars, but better law enforcement officers and practitioners.

Dr. Belshaw shared the types of data he is collecting from the dark web and encourages more work and collaboration in this fascinating underworld of the internet.

Call for Papers

Effectiveness of International Cybercrime & Cybersecurity Efforts

The Division of Cybercrime is sponsoring a special issue with the *International Journal of Cybersecurity Intelligence and Cybercrime* on the effectiveness of international cybercrime and cybersecurity efforts. Manuscript submissions due by October 15, 2021. For more details click [here](#) or email Cathy Marcum at marcumcm@appstate.edu.

Link Between Online and Offline Victimization and Behaviors

ASC's Division of Cybercrime and Division of Victimology are collaborating on a special issue in *Victims & Offenders* on the link between specific forms of online and offline forms of victimization. See V&O website for details or email marcumcm@appstate.edu.

Anti-Asian Racism & Violence

Dr. Claire Lee, DC Secretary/Treasurer, is co-guest editor for the Anti-Asian Racism and Violence special issue in *Race & Justice*. Please see below for the full call for papers and contact Dr. Lee at Claire_Lee@uml.edu with questions.

Chapters Needed

Authors are needed for chapters in the "Handbook on Crime and Technology," edited by Drs. James Byrne and Don Hummer. Chapters needed on embezzlement, corporate espionage, spread of virus/malicious code, and theft/sale of personal data. Deadline extended to July 15. Contact Dr. James Byrne at profbyrne7@gmail.com for complete details and chapter requests.



Check out the new ASC Division of Cybercrime website created by our webmaster Divya Ramjee!

<http://ascdivisionofcybercrime.org>

SPRING WORKSHOP SERIES

Achieving Success in the Cyber Field

The ASC Cybercrime Division hosted its third virtual workshop in its spring series on Wednesday, April 28 on the topic of “Achieving Success in the Cyber Field.” Moderated by division chair Dr. Cathy Marcum, four cybercrime scholars shared their tips for success.

The first speaker on the panel, Dr. Kyung-Shick Choi, from Boston University, puts a lot of focus on teaching and mentoring new scholars in the field. “I’m a strong believer in a simple equation--student success equals to my success.” Dr. Choi said.

He also shared that the field is incredibly broad and always changing with new technology, so it’s important to stay current and always continue to learn. He also emphasized the importance of looking at cybercrime globally. “Cybercrime is not just one nation’s problem,” he said. “It’s everyone’s problem.”

The second speaker was Dr. Thomas Holt, from Michigan State University, who said to achieve success the first thing you must do is set a clear set of goals that one can reasonably

achieve and make sure you are not setting unrealistic expectations.

Dr. Holt also discussed the concept of failure and how it relates to success. “You are going to fail. That’s how this field works,” he said. “Papers get rejected, grant proposals aren’t funded, ideas don’t always pan out.” But how you deal with



that failure is what matters. Learn how to keep going, take constructive criticism, and find the best outlets for your work.

Dr. Claire Lee, from University of Massachusetts at Lowell, shared her thoughts on success in the field also starting with failure. “Always be prepared to fail or be rejected,” she said. “It’s better to have a lot of things your pipeline--under review, under revision, or writing,” she said. “So when you do get rejected, it

talking about success since the two concepts go hand-in-hand.

“We need to talk more constructively in academia about this notion of rejection and the fact that good projects don’t get funded and good articles don’t get published,” she said. Dr. Cross emphasized the need for perseverance and having a thick skin in the field. “Be able to separate the professional from the personal. We are not defined by our number of publications, by our number of citations, or by the grants we receive.”

Dr. Cross said one of the things that has helped her the most is support from other academics. “Find your people,” she said. “One of the most joyful things in my research and my

academic life is finding people who will support me and that I can support as well. Finding those who have got your back.”

Dr. Cross has also been in a writing group which has contributed to her success. And finally she encouraged, “As academics we need to be kind to each other.”

“Find your people. One of the most joyful things in my research and my academic life is finding people who will support me and that I can support as well.” ---Dr. Cassandra Cross

keeps you moving forward.” Dr. Lee also said a writing group has been very beneficial to her success.

The final speaker on the panel was Dr. Cassandra Cross from Queensland University of Technology, who also started with the importance of looking at failure when

Meet the new ASC Cybercrime Division Leaders



Dr. Cathy Marcum
Chair

*Professor & Assistant Chair
Appalachian State University*



Dr. Sinchul Back
Vice Chair

*Assistant Professor
The University of Scranton*



Dr. Claire Lee
Secretary/Treasurer

*Assistant Professor
University of Massachusetts
at Lowell*



Dr. Erica Fissel
Executive Counselor

*Assistant Professor
University of Central Florida*



Dr. Jordana Navarro
Executive Counselor

*Assistant Professor
The Citadel*



Dr. Kevin Steinmetz
Executive Counselor

*Associate Professor
Kansas State University*

Meet the new ASC Cybercrime Division Leaders

Liaisons to the Asian Society of Criminology



Dr. Kyung-Shick Choi
Professor
Boston University



Katelyn Wan Fei Ma
Ph.D. Student
York University



Dr. Jennifer LaPrade
Historian
Assistant Professor
Missouri State University



Divya Ranjee
Webmaster
Ph.D. Candidate
American University

Liaison to the Australian/New Zealand Society of Criminology



Dr. Cassandra Cross
Associate Professor
Queensland University of Technology



Dr. Yi Ting Chua
Research Associate
Cambridge Cybercrime Centre



Dr. Fernando Miro-Llinares
Dean & Chair
Miguel Hernandez University



Dr. Katalin Parti
Assistant Professor
Virginia Tech University

Liaisons to the European Society of Criminology

Upcoming Events

ASC Annual Meeting Palmer House Hilton Chicago, IL November 17-20, 2021

Chairs: Charlotte E. Gill and
Thomas Anthony Loughran IV

Theme: Science and
Evidenced-Based Policy
in a Fractured Era

Posters, roundtable abstracts, and
lightning talk abstracts due:
May 21, 2021

The ASC Division of Cybercrime
plans to make a strong showing
at this year's annual meeting with
five roundtable discussions and many
presentations by members sharing
their latest cybercrime research.

A full schedule of ASC
Cybercrime Division events
will be detailed in the October 2021
Division newsletter.

*We look forward to
seeing you in Chicago!*

International White Hat Conference **Virtual Conference** **June 1 -2, 2021**

Boston University Cybercrime Investigation and Cybersecurity (CIC) Lab will host the 2nd International White Hat Conference which will take place virtually on June 1 - 2, 2021. Registration is free and open now. For more details, see [page 8](#) of this newsletter.

Royals Cybercrime Investigation Camp **University of Scranton** **July 13 - 15, 2021**

The University of Scranton will host the inaugural Royals Cybercrime Investigation Camp at its campus on July 13 - 15, 2021. There is no fee for attending and the camp is open to students who will be in 10th, 11th, or 12th grade and Fall 2021. For questions or more information, contact Dr. Sinchul Back at sinchul.back@scranton.edu.

The Human Factor in Cybercrime **Montreal, Quebec** **November 21 - 23, 2021**

After two first successful events, the 3rd Annual Conference on the Human Factor in Cybercrime will take place in Montreal immediately after the ASC's conference in Chicago. There are daily flights between the two cities, with flight times of about 2.5 hours. Conference organizers expect travel restrictions to ease by Nov. 2021 and are planning an in-person event. However, adjustments will be made in accordance with the guidance of public health authorities and the event will transition online should the expected improvements be delayed. More information about the exact location will be announced soon. If you have any questions, please contact Benoît Dupont (benoit.dupont@umontreal.ca) or Fyscillia Ream (fyscillia.ream@umontreal.ca).

JUNE 1-2, 2021

2021 White Hat Conference

The Future of Cybercrime and its Challenges: Innovative Solutions Against Cybercrime

Registration is now open for the 2nd International White Hat Conference held virtually on June 1 - 2, 2021 where Cybercrime Investigation and Cybersecurity experts and guest speakers from 15 countries will share their knowledge for combating cybercrime as a global White Hat community.

The two-day conference is free to attend and organized by creator and cybercrime scholar Dr. Kyung-Shick Choi of Boston University. The event is hosted by Boston University Cybercrime Investigation and Cybersecurity (CIC) Lab and supported by the Department of Justice's (DOJ) Bureau of Justice Assistance (BJA).

During the event, ASC Division of Cybercrime Members will facilitate the conference as discussants and moderators for the major conference sessions including the Cyber-



an effort to better serve students in the areas of cybersecurity, computer forensics, and digital evidence, leading to improved cybercrime investigations and successful prosecutions.

A special feature of the Cybercrime Investigation competition will be that top international competitors must present evidence from their investigation, build a prosecution case using legal codes, and present that case in a Mock Trial format, since the courtroom and prosecution component is an often overlooked area of

fighting cybercrime. A panel of expert judges will score the competitors based on how clearly they present their evidence and how well they justified their case using the legal codes.

Please contact Dr. Kyung-Shick Choi at kuung@bu.edu with any questions. Watch a [video here](#) for more information.

Hope to see you there!

Register for free here:
<https://live.bu.edu/whitehat>

crime Investigation Competition and Student Paper Competition.

This White Hat conference program will be a foundational effort that seeks to enhance the current capacities of higher education in

Member achievements

Royal-Cyber Warriors Win 2021 Cybercrime Investigation Competition



Dr. Sinchul Back, Assistant Professor at the University of Scranton, led his cybercrime investigation team Royal-Cyber Warriors to victory last month winning First Place in the 2021 US Cybercrime Investigation Domestic Competition, hosted by Utica College and funded by the U.S. Department of Justice's Bureau of Justice Assistance grants. The competition began at 9 a.m. and ended at midnight. Ten United States university teams participated in the competition. Congratulations!

Share your good news!

Send member achievements that you would like to include in our newsletter to jlaprade@missouristate.edu.

Not yet a member of the Division of Cybercrime and want to join?



Click [here](#) or contact marcumcm@appstate.edu with questions.

We look forward to working with you!

Nominations are now open!

Annual ASC Cybercrime Awards

Led by Awards Committee Chair Dr. David Décary-Hétu, the committee has established four annual awards for the new ASC Division of Cybercrime. Awards will be presented each year at the ASC Annual Meeting. The four awards are Lifetime Achievement, Early Career, Outstanding Contribution, and Outstanding Practitioner. General rules for awards include:

Eligibility

With the exception of the Outstanding Practitioner Award, only Cybercrime Division members are eligible. Executive board members and Award committee members are not eligible to nominate, or win an award while serving. Executive Board members and Award committee members cannot be co-authors of publications that receive an award.

Nominations

Cybercrime Division members can self-nominate for an award. They can also nominate other Cybercrime Division members. Nominations can be made through a Google

Form on the [Cybercrime Division website](#). Nominated members will be contacted with the decision regarding the award.

Repeat winners

With the exception of the Outstanding Contribution Award, a person cannot win the same award more than once.

Regularity

Depending on nominations, Award committee members may decide not to give out an award for one or more years.

Format

Awards are presented as plaques each year at the Cybercrime Division meeting at the ASC conference.

Calendar

The Award committee starts accepting applications on the first Monday of May of each year. Applicants have until the end of day, first Friday of September of each year to apply.

Lifetime Achievement Award

Description

This award recognizes sustained outstanding professional contributions by an individual to the broadly defined areas of cybercrime research or control. The award is not given for any single research project or study but rather for a body of research developed over one's career. Professional contributions also include advocating for cybercrime research as an area of scholarship within criminology and related disciplines and mentoring graduate students. Persons who have made substantial practical contributions to the field are also eligible to receive this award.

Eligibility

Recipients must be a late career scholar in the field. Retired scholars can be considered.

Application material

Award applications must include a letter of presentation (max. 1,000 words), curriculum vitae, up to three letters of support, and up to two supplemental submissions of lifetime achievement.

Contact

Please send any questions related to the Outstanding Contribution Award to subcommittee chair Dr. David Décary-Hétu at david.decary-hetu@umontreal.ca.

Early Career Award

Description

This award recognizes the achievements of scholars who show outstanding merit at the beginnings of their careers. Outstanding merit may be based on a single book or work, including a series of theoretical or research contributions to the field of cybercrime.

Eligibility

Early scholars working by themselves or as part of a team of co-authors who are currently employed in an academic program. The nominee have must earned a Ph.D. within the last eight years and be non-tenured.

Application material

Award applications must include a letter of presentation (max. 1,000 words) as well as a curriculum vitae. In addition to general application material, it is recommended that other evidence to support the nomination be submitted.

Contact

Please send any questions related to the Early Career Award to subcommittee chair Dr. Hyeyoung Lim at hyeyoung@uab.edu.

Nominations are now open!

Annual ASC Cybercrime Awards

Outstanding Contribution Award

Description

This award recognizes outstanding service contributions to the Division on Cybercrime. Service may include mentoring, serving as an officer of the Division, committee work for the Division, or other related groups in the field of cybercrime.

The criteria for evaluations nominations will include but are not limited to :

- Number of mentorships
- Contribution to the Division of Cybercrime
- Contribution to the field of cybercrime in general

Repeat winners

A Cybercrime Division member may win this award for a second or more time, provided three years have lapsed since the member last received this award.

Application materials

Nominations should include up to three letters of support, and up to two supplemental submissions of evidence of service to the field/division. These should present details of the outstanding contributions of the nominee and their impacts on the field.

Contact

Please send any questions related to the Outstanding Contribution Award to subcommittee chair Dr. David Décary-Hétu at david.decary-hetu@umontreal.ca.

Outstanding Practitioner Award

Description

The Outstanding Cybercrime Practitioner Award recognizes a cybercrime practitioner who has played an integral role in advancing the field of cybercrime prevention and public safety. This may have been accomplished through a variety of methods including, but not limited to the following:

- Implementing major new cybercrime prevention programs or policies
- Leading effective cybercrime prevention initiatives
- Development of partnerships to enhance public safety related to cybercrime
- Increasing community awareness related to cybercrime prevention
- Collaborative research roles that have led to significant improvements in addressing cybercrime

Eligibility

Non-Division members are eligible for this award.

Format

In addition to a plaque, the winner will also earn a one-year membership to the Division.

Application materials

Award applications must include a letter of presentation (max. 1,000 words) as well as a curriculum vitae. Any supporting evidence of outstanding practitioner work is encouraged.

Contact

Please send any questions related to the Outstanding Cybercrime Practitioner Award to subcommittee chair Dr. Jennifer LaPrade at jlaprade@missouristate.edu.

SPRING WORKSHOP SERIES

Best Teaching Practices in Cyber

On April 8, the ASC Cybercrime Division hosted the second workshop in its spring series titled, "Best Teaching Practices in Cyber." Five professors and expert scholars shared the innovative ways they teach cybercrime in their classes.

First, Dr. Shelly Clevenger from Sam Houston State University described one of the creative assignments she uses to engage students in cybercrime learning. Dr. Clevenger's students create comic books and children's books that explain aspects of cybercrime and cyber safety. Once students complete their projects, they take them out to children in the community, read their books to the children, and teach them about online safety. Her students have visited children in places such as homeless shelters and the Big Brothers/Big Sisters organization.

"When we think about cybercrime, people are often only thinking about hacking behaviors and identity theft and it can be a lot more than that," Dr. Clevenger said. "This is a fun way to get students to think about the information and get us out into the community."

Dr. Jordana Navarro, from The Citadel, then shared some of the creative ways she incorporates theory into her cybercrime classes. For example, she has her students do a risk assessment on themselves to discover their suitability as targets for cybercrime, in accordance with routine activities theory.

Another example is that Dr. Navarro has her students walk around campus and assess how aware people are of their surroundings and how

Translating Research into Action

My students and I have engaged in educational efforts to raise awareness in domestic abuse shelters and sexual violence centers about the connection between in-person violence and cybervictimizations in K-12 programs.

These efforts also included raising awareness among the community and providing them materials for the K-12 population.

In order to raise this awareness, my students created books, including comic books, that were easily accessible and relatable to youth.

this can increase their vulnerability.

"Anything that gets students moving and seeing how theory impacts their everyday life, I find particularly meaningful," she said. Dr. Navarro also has students watch cybercrime movies and has them identify the cyber offenses presented to apply what they have learned in class.

Dr. James Popham from Wilfrid Laurier University takes an experiential learning approach in his cybercrime classroom. For example, he brings an old computer to class, takes it apart, and teaches students about computer parts and their vulnerabilities. To teach about networking, Dr. Popham has students stand and bounce rubber balls around the classroom. He also uses experiential activities such as card games and creating podcasts to engage his students.

Dr. Erica Fissel, from University of Central Florida, shared her creative teaching approach of using role immersion, which consists of having students work in small groups, take on specific roles, then act them out

in case-based scenarios related to investigating and prosecuting cybercrimes. "They really enjoyed the assignment because it was different than what they've done before and it forced them to look at these types of cases from a different perspective," Dr. Fissel said.

The final speaker on the panel was Dr. Sinchul Back, from the University of Scranton, who shared his methods of using cybercriminal profiling in his teaching.

"Human factors, or people, are one of the most important considerations to effectively prevent or fight against cybercrime," he said. Teaching using cybercriminal profiling can help students hone their knowledge of cybercriminals using FBI cybercrime cases. Using the SSBACO Cybercriminal Profiling model that he created, students use sociodemographic, situational, and opportunity factors, to analyze real life cybercrime scenarios and create a cybercriminal profile analysis.

All presenters offered to share more details with anyone interested.

Division of Cybercrime Historian's Report

As you can see by the activity reported in this newsletter, the new ASC Division of Cybercrime is off to a great start! In November 2019, Division founders Dr. Adam Bossler, Dr. Thomas Holt, and Dr. Kyung-Shick Choi led the first organizing meeting for the division at the ASC Annual meeting and in March 2020 the new division was officially launched. Despite launching during an unprecedented worldwide pandemic, the division has been very active in its first year.

In Fall 2020, the Division of Cybercrime co-hosted two virtual events: one with the European Society of Criminology's Cybercrime Working Group; and the second with the Korean Institute of Criminology.

In November 2020, nominations opened for the first elected division positions: chair, vice chair, and secretary/treasurer. The founders eliminated themselves from consideration, a full slate of nominees were submitted, and voting began in December 2020.

The following individuals were elected as officers and assumed their positions on January 1, 2021: Catherine Marcum, Chair; Sinchul Back, Vice Chair;

and Claire Lee, Secretary/Treasurer. The newly elected officers chose three Executive Counselors to serve on the Executive Board (EB): Erica Fissel, Jordana Navarro, and Kevin Steinmetz.

A call for participation was sent to the membership to fill other positions and members responded. Social media presence on Facebook and Twitter was created and expanded by the Executive Board. In addition, a division logo was created in March 2021 and the website was launched in May 2021.

Three well-attended virtual workshop events were hosted by the Division in a Spring Workshop series: Dark Web and Cyber Fraud, Best Teaching Practices in Cyber, and Academic and Practitioner Success in Cyber. Furthermore, six themed roundtables were submitted for ASC 2021 and a time slot for the Division meeting was requested. Two special issues were also developed with *Victim & Offenders* and *International Journal of Cybersecurity Intelligence and Cybercrime*.

This brand new Division is off to a great start, but this is only the beginning!

Thank you Division of Cybercrime Founders!



Dr. Adam Bossler
Georgia Southern University



Dr. Kyung-Shick Choi
Boston University



Dr. Thomas Holt
Michigan State University

Newsletter Submissions



Jennifer LaPrade

It is an honor to serve as the Historian of ASC Division of Cybercrime and create this newsletter for our members. My experience working with members of this division has been fantastic. I am so excited to serve this division and do whatever I can to help record and publicize the great work happening in this division and in field of cybercrime.

We plan to publish three newsletters per year: one in late spring, one in the fall (before ASC) and one in the winter (after ASC). Submissions are welcome and encouraged. Please submit your upcoming events, achievements, call for papers, announcements, or anything else you think may be of interest to our members for our newsletter.

Please let me know if you have any questions. Enjoy your summer and I hope to see you in Chicago!

Fall newsletter deadline:
Friday, September 17, 2021
Winter newsletter deadline:
Friday, December 3, 2021
Spring newsletter deadline:
Friday, March 25, 2022

Please send submissions to Dr. Jennifer LaPrade at jlaprade@missouristate.edu.



Thank you to Dr. Sinchul Back and Gibeom Park for creating our new Division of Cybercrime logo!

**Look for
our next
newsletter
in October!**

Follow us on Twitter [@ASCCyber](https://twitter.com/ASCCyber) and [Facebook!](https://www.facebook.com/ASCCyber)