Volume XLI, Issue 1 January 2016

ACJS Today

Academy of Criminal Justice Sciences

Closing the Digital Divide in Criminological and Criminal Justice Research

David C. Pyrooz, University of Colorado Boulder*
Richard K. Moule, Jr., Arizona State University**
Scott H. Decker, Arizona State University***

There has been substantial growth in the availability and use of communication technologies over the past two decades. The Internet, cellular telephones, and social media are increasingly common components of everyday life. Consider:

- Nearly 90% of adults, and 95% of adolescents, use the Internet (Pew Research Center, 2012b, 2014a).
- Roughly 90% of American adults have cell phones, two-thirds of which are smart phones (Pew Research Center, 2014b).

Continued on Page 4

SPECIAL ISSUE
NEW DIRECTIONS IN CYBERCRIME RESEARCH

President's Message

Brandon K. Applegate, President,

What if there were an event at which scholars, policy makers, students, and professionals from all across the country and the world got together and spent several days talking about crime and criminal justice? I feel very fortunate to have been involved in planning such an experience: The 53rd Annual Meeting of the Academy of Criminal Justice Sciences. With this conference not far off—March 29 through April 2—I've been giving some thought to the reasons that people might attend. Here are my top ten:

#10: Panels, roundtables, open seminars, and other events. More than 400 sessions await!

#9: Networking. Remember those friends and colleagues you haven't seen since the last conference? The ACJS meeting will be a great place to see them again. There will also be plenty of opportunities to make new contacts.

#8: Awards luncheon. Help us recognize remarkable criminal justicians on Friday afternoon of the conference. The lunch only goes so far, so come early to make sure you don't miss out!

#7: Presidential feature events. We will have a keynote address by renowned scholar Owen D. Jones, who will share with us insights about the intersection of law, crime, and neuroscience. Four other panels will highlight Colorado's experience with marijuana legalization, a unique program aimed at altering the self-narratives of justice-involved urban youths, Barry Feld's work spanning three eras of juvenile justice, and Frank Cullen's reflections on critical turning points in his scholarly career.

#6. Giveaways. Of course, everyone will enjoy the amenities that come with registering for the conference. I won't disclose exactly what will be included when you pick up your conference materials, but this year, if you get there early enough, you'll have a choice. Also, if you would like an opportunity to win a Kindle Fire tablet, plan to attend the ACJS General Business Meeting on Friday morning.

#5: Executive board members and ACJS staff. Look for the ribbons on the bottom of the badge holders. We're here to represent you, so track us down to say hello or ask us questions. ACJS Board members and staff will also be available for photo opportunities or to autograph one of those great giveaways—I'm giving each of them a Sharpie so they will be ready!

#4: Karaoke night. Warm up those pipes for a reprise of a popular event from Orlando… with a new twist. On Friday night, enjoy light refreshments while you sing, dance, or just

watch others. Along with the music, there will also be a slide show featuring pictures taken by conference attendees. Check the program book and signage at the hotel for details about how to "Share *Your* ACJS."

#3: Exhibit hall. The exhibit hall will be open Wednesday, Thursday, and Friday. Come see the latest that publishers and others have to share.

#2: Denver. The capital of Colorado. The Mile-High City. Founded as a mining town in 1858, Denver is now a thriving major metropolis, chock full of restaurants, bars, shopping, museums, and plenty more to keep you busy when you venture outside the conference.

And the #1 reason to attend the conference in Denver: So you can tell me what YOUR top reasons are for attending! Seriously, the better ACJS leaders understand what makes ACJS conferences work for all members, the better the conferences will be. Please share your thoughts on all the things you enjoyed… as well as those that can be improved in the future.

*****Brandon K. Applegate*** *is professor and chair of the Department of Criminology and Criminal Justice at the University of South Carolina. He received his Ph.D. in criminal justice from the University of Cincinnati in 1996 and taught for 14 years at the University of Central Florida before joining USC in 2010. He teaches undergraduate, master's, and Ph.D. courses on corrections, juvenile justice, and methodological issues. He has published more than 50 articles, book chapters, and other publications on punishment and rehabilitation policy, correctional treatment, juvenile justice, public views of correctional policies, jail issues, and decision making among criminal justice professionals. He also co-edited Offender Rehabilitation: Effective Correctional Intervention (1997, Dartmouth). Applegate previously served as secretary of the Academy of Criminal Justice Sciences and as president of the Southern Criminal Justice Association. He has served on the editorial boards of Justice Quarterly, Journal of Criminal Justice Education, and the American Journal of Criminal Justice.*

Continued from Page 1

- About 90% of American teens also have cell phones, and three-quarters have access to smart phones (Pew Research Center, 2012c, 2015).
- Three-quarters of American adults who are online use social media, along with 81% of adolescents (Pew Research Center, 2012a).

Not only is a substantial portion of the population online, but many of our daily activities have moved online as well. Many faculty teach, communicate, apply for jobs, submit and review manuscripts, and read journals online. Can anyone imagine going back to the "old days" of collaborating via letters and snail mail journal submissions?

But an increasingly wired world also carries a heavy price. The growing prevalence and use of technology has created new methods for engaging in and combating crime (Holt & Bossler, 2014). The umbrella of cybercrime spans a wide range of activities, including "the usual suspects" of hacking, phishing, fraud, and the sale of illicit goods and services (Holt, Blevins, & Burkert, 2010; Holtfreter, Reisig, & Pratt, 2008; Tcherni, Davies, Lopes, & Lizotte, 2015; Wolfe, Higgins, & Marcum, 2007). There are also "emerging suspects" in the use of the Internet by criminal collectives such as terrorists, hate groups, street gangs, human traffickers, and other active offenders (Gerstenfeld, Grant, & Chiang, 2003; Moule, Pyrooz, & Decker, 2014; Pyrooz, Decker, & Moule, 2015; Weimann, 2006).

These uses of the web are supplemented by other forms of deviant and criminal online behaviors, such as the use of social media—Yelp!, Facebook, YikYak, The Dirty—to bully, harass, and spread vicious rumors and reviews (Patchin & Hinduja, 2006; Patton, Eschmann, & Butler, 2013). These behaviors also include posting and disseminating recordings of police-citizen encounters. There are now multiple platforms on which to post videos of such encounters, some of which include tens of thousands of such videos. Like no other time in history, videos are easily recorded and broadcast on national levels, and may ultimately chip away at institutional forms of legitimacy (Goldsmith, 2010).

The "digital divide," a phrase once used to describe Internet users and non-users (Norris, 2001), aptly applies to research in criminology and criminal justice. Despite new opportunities for research, criminologists have been slow to pay attention to the online realm. The problem with the digital divide in criminological and criminal justice research is that it fails to appreciate the scope of technology in everyday lives and the far-reaching consequences of technology for crime and crime control. The "online" and "offline" worlds of the adolescents, offenders, prisoners, police officers, neighborhoods, agencies, and cities we study are increasingly converging. There are real-world consequences for online behavior, and we are remiss in not paying closer attention to the interdependencies of these worlds.

How can we better incorporate these interdependencies into our field? First, there needs to be an explicit recognition that "cyber" does not operate at the fringe of the discipline. We have previously compared this to the meager attention mainstream criminology gave to the study of terrorism prior to 9/11 (Pyrooz et al., 2015). Second, we need a theoretical and methodological agenda for addressing the growing intersection of technology, crime, and

criminal justice. We use street gangs as an example of an effort to close the digital research divide.

The On- and Offline World of "Street" Gangs: A Case Study

We focus on street gangs for two reasons. First, there are few areas in criminology or criminal justice more anchored to the street than gangs—they literally adopt the names of streets (e.g., Grape Street Crips), hang out on street corners, and carve up neighborhoods as turf of their own. A decade ago, Papachristos (2005, p. 53) wrote, "few gang members ever discuss or mention the Internet. Many don't possess the hardware, software, or technical skills (not to mention the necessary telephone lines) to manage the web." What could be more street oriented, or "offline," than gangs? Much has changed in the past decade.

Second, while we have longstanding interests in gangs, it was receiving funding from Google Ideas that spurred interest in the intersection of gangs and the Internet. We highlight some of that work below, along with other excellent work conducted by colleagues over the past decade, to present a research framework involving the Internet and social media going forward. We see three distinct streams of research, organized by research design.

Cyber-Ethnographic Research

Early work on gangs and the Internet examined how these groups represent themselves online. Street gangs carefully cultivate reputations and gang culture is ripe with mythology (Felson, 2006; Klein, 1971). One of the main strengths of the Internet is that it offers a great amount of control to the user for constructing this image. Womer and Bunker (2010) examined the use of social media among Sureño gangs and Mexican drug cartels. Based on keyword searches, and using terms in the FBI's National Gang Threat Assessment, the authors reported finding an established presence of these groups online and that gangs would actively broadcast gang-related images of weapons, flashing gang hand signs, and showing off tattoos.

Décary-Hétu and Morselli (2011; Morselli & Décary-Hétu, 2013) sought to understand whether an individualized phenomenon like the Internet could engage the collective interests of the group. Similar to Womer and Bunker (2010), they conducted keyword searches on the names of active Canadian gangs, along with well-known criminal groups, on social media sites. Between their data collection efforts in 2010 and 2011, they found that gang activity increased in just a short amount of time. Gangs migrated to Facebook from MySpace, had more followers, and were increasingly online. They also found a great deal of "noise" in online gang content, making it unclear who was posting images and videos. Gangs that wanted digital infamy have to work to get likes, retweets, and views, especially given the evolution of social media.

Similarly, Van Hellemont (2012) aimed to learn about the collective features of gangs on the Internet, focusing on 170 gang-oriented blogs in Brussels, Belgium. Drawing on impression management and the performance aspects of gang life online, Van Hellemont classified blogs

Continued on Page 7

ACJS 2016 Annual Conference

"Advancing Justice on All Fronts"

March 29th – April 2, 2016
Sheraton Denver Downtown Hotel
Denver, Colorado

Program Chairs:

Jennifer L. Hartman, jhartman@uncc.edu
Shelly Listwan, slistwan@uncc.edu

Host Hotel:

Sheraton Denver Downtown Hotel
1550 Court Place
Denver, Colorado 80202

Continued from Page 5

into distinct types, focusing on gang discussions, music, images, and memorializing the dead. She found that the content posted on blogs was important for communicating "gang-ness." Given that the blogs are archived, there was "unprecedented permanence" in the content, reaching audiences beyond the immediate networks of gang youth in Brussels.

Finally, Patton and colleagues (2013) termed online gang content and behavior as "Internet banging." Internet banging involves the promotion of gang affiliations and activities, earning notoriety through participation in violent acts or communicated threats, and sharing information about gangs more broadly. Patton and colleagues held that there are inextricable linkages between internet banging, hip hop, and masculinity, and the Internet is a new mechanism for obtaining street credibility. Along with quotes and videos from *WorldStarHipHop*, the dangerous escapades of Chicago rapper Chief Keef and his experience with virtual and real-world gang violence were used to illustrate these intersections.

Survey Research

Survey research, beginning with King, Walpole, and Lamon's (2007) "surf and turf" article, is used to glean information from gang members directly. Given the sheer amount of "noise" found online, it is important to hear from gang members themselves about their Internet activities. Some survey research also provides control groups to determine just how different gang behaviors are online.

In the Google Ideas study (Decker & Pyrooz, 2011), we surveyed more than 600 current, former, and non-gang members about their online activities. Pyrooz et al. (2015) introduced two perspectives for understanding online identity and behavior: web-facilitated (i.e., identity and behavior would not exist publicly but for the Internet) and web-enhanced (identity and behavior exist publicly regardless of the Internet). Aligning with the latter view, we argued that gang identity and behavior online would resemble offline behavior. This parallelism hypothesis was largely confirmed: Gang members' noncriminal online activities were similar to nonmembers', while their criminal activities were much greater, and gangs used the Internet for symbolic rather than instrumental purposes.

Moule et al. (2014) assessed the factors leading to Internet adoption among gangs (not gang members) using organizational theory. Gang behavior should be influenced by organizational features such as centralization, complexity, formalization, interconnectedness, and organizational slack. As these features become more established, it was expected that adoption of technologies like the Internet would occur. Moule et al. found evidence supporting this argument. Even after accounting for individual biases, more organized gangs engaged in more online behaviors, including having a website, posting videos, and recruiting members.

Other researchers have asked gang members about Internet and social media presence. Sela-Shayovitz (2012a) interviewed gang members in Israel and found they were highly reliant on the Internet. Some members reported a high level of technological competence, and one-third reported that the Internet played a vital role in gang activities.

Densley (2013) viewed the Internet and social media in signaling perspective: What do online activities reveal about gangs and gang members to the outside world, including rival gangs? Based on interviews with London gang members, some gangs used the web to showcase "strength in the numbers." Consequently, Densley viewed social media as inflaming already sensitive tensions on the street.

Big Data Research

A final example of bridging the digital divide in criminological and criminal justice research is found in "big data" studies of gang activity. This research involves automated data collection; algorithms; and large-scale, sophisticated data collections that go beyond the standard training found in CCJ doctoral programs. There is a combination of theoretically rich questions that can be addressed by this research, as well as practical, relevant implications for the criminal justice community. Examples of this are found in the recent work of Patton and colleagues (2015) and Wijeratne and colleagues (2015).

Patton et al. (2015) focused on how gangs and gang members communicate online. Using Twitter, they analyzed 8.5 million tweets in 2013 and 2014 by individuals identified as gang members by the Detroit Crime Commission. After gathering information about street gang terminology and slang to develop keywords, they identified roughly 355,000 tweets organized around themes of violence, crime, and substance use. They found about 80,000 tweets related to grieving the death of a loved one, 267,000 tweets pertaining to gang conflicts, 29,000 tweets about substance use, and 3,500 tweets about firearms. Patton et al. argued that social media could be as an assessment tool for public health.

Social media has clear implications for the criminal justice system, and Wijeratne et al. (2015) developed a tool to assist agencies collect this data. They introduced a three-dimensional platform—in time and space—to monitor the effects of gang activities on communities, discover influential persons, evaluate content, and monitor existing prevention and intervention programs. This platform includes (1) a spatio-temporal-thematic analysis, (2) people-content-network analysis, and (3) emotion-sentiment analysis. They illustrated this in Chicago where, after constructing keywords of gang slang, their automated platform collected 105,000 gang-related tweets and 384,000 location-related tweets over a 10-day period in March 2015.

From Digital Divides to Digital Inequalities

The "digital divide" has shifted from distinguishing users/non-users to digital inequalities, or variability in the skill sets of users and how people use the Internet (DiMaggio et al., 2004). We hope to see a similar shift in criminological and criminal justice research. Where do we go from here? We see "low hanging fruit" and long-term agendas, both of which can address questions of fundamental importance to studies of crime and crime control. We discuss a few directions for this research.

First, it is necessary to understand the contribution of the Internet to criminal activity. Tcherni et al. (2015) held that cyberspace is concealing a property "crime wave," yet we lack reliable data to assess this dark figure. In a similar vein, we have a limited understanding of how

online activities contribute to offline conflict. Pyrooz et al. (2015) reported that online gang behaviors spill over to the street, but this likely occurs for non–gang crimes as well. What are the real-world consequences of the Internet and social media, and can the web reduce or increase crime (Moule et al., 2015)? This consideration has not escaped theorists, who have acknowledged the implications of the Internet for social disorganization and collective efficacy theories (Hampton, 2011; Wahl-Jorgensen, 2015; Warner & Sampson, 2015).

Second, data limitations are ripe for collaboration with "big data" researchers. Can tweets, status updates, and video content help to link offline and online realms? Prior studies have assessed Internet forum and website content (Hutchings & Holt, 2015; Zhou et al., 2005) and provided insights into the beliefs, practices, and fears of various online communities (e.g., skinheads, johns, data traffickers, terrorists). The "big data" elements of the web are also of interest to computer scientists, and recent works have relied on these interdisciplinary collaborations. For example, Westlake and Bouchard (2015), working with the Royal Canadian Mounted Police, gathered information on child pornography websites using web crawlers.

Third, the Internet is a useful tool for the nuts and bolts of research, including sample recruitment and survey administration. The advent of Amazon's Mechanical Turk survey software provides a readily available sample of Internet users, and its use is becoming more common among criminologists (e.g., Fox & Potocki, 2015). Further, recent publications in top-tier criminology journals have used website recruitment and online populations to examine topics such as the sexual solicitation of minors (Schulz et al., 2015).

Fourth, the Internet provides opportunities to assess the generality of theory and criminological facts. Indeed, rather than thinking about "cybercrime" as a niche, it should be used to assess whether and how the Internet moderates peer effects (McCuddy & Vogel, 2015), the victim-offender overlap (van Wilsem, 2011), the age-crime curve, gender and race/ethnic differences in offending and victimization, offender specialization, routine activities, and other established theories in criminology. Surely these are areas of mainstream criminological interest.

Fifth, the use of technology is not limited to offenders. Law enforcement agencies now use the web to combat crime and expand community outreach efforts (Crump, 2011; Denef, Bayerl, & Kaptein, 2013). Social media efforts by the Detroit Police Department, for example, involve community notification of events and successful arrests. Other agencies maintain websites for submitting crime tips and disseminating crime statistics. How this influences community-police relations, including perceptions of legitimacy and community policing efforts, is of fundamental importance.

In the end, the technologies we have discussed here will not go away, and it is imperative that these technologies be taken seriously for criminal behavior and crime control. The online and offline worlds continue to blur, and the real-world consequences of their overlap are not trivial. We have highlighted this overlap and noted a variety of research opportunities offered by new technologies. We

encourage our colleagues to embrace these opportunities.

References

Crump, J. (2011). What are the police doing on Twitter? Social media, the police and the public. *Policy & Internet, 3,* 1–27.

Décary-Hétu, D., & Morselli, C. (2011). Gang presence in social network sites. *International Journal of Cyber Criminology, 5*(2), 876–890.

Denef, S., Bayerl, P. S., & Kaptein, N. A. (2013). Social media and the police: Tweeting practices of British police forces during the August 2011 riots. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (pp. 3471–3480). New York: ACM.

DiMaggio, P., Hargittai, E., Celeste, C., & Shafer, S. (2004). Digital inequality. In *Social inequality: From unequal access to differentiated use* (pp. 355–400). Princeton, NJ: Center for Arts and Cultural Policy Studies, Woodrow Wilson School.

Felson, M. (2006). The street gang strategy. In M. Felson, *Crime and nature* (pp. 305–324). Thousand Oaks, CA: Sage.

Fox, J., & Potocki, B. (2015). Lifetime video game consumption, interpersonal aggression, hostile sexism, and rape myth acceptance: A cultivation perspective. *Journal of Interpersonal Violence*. doi: 0886260515570747.

Gerstenfeld, P. B., Grant, D. R., & Chiang, C-P. (2003). Hate online: A content analysis of extremist internet sites. *Analyses of Social Issues and Public Policy, 3*(1), 29–44.

Goldsmith, A. (2010). Policing's new visibility. *British Journal of Criminology, 50,* 913–934.

Hampton, K. N. (2011). Comparing bonding and bridging ties for democratic engagement: Everyday use of communication technologies within social networks for civic and civil behaviors. *Information, Communication & Society*, *14*(4), 510–528.

Holt, T. J., Blevins, K. R., & Burkert, N. (2010). Considering the pedophile subculture online. *Sexual Abuse, 22,* 3–24.

Holt, T. J., & Bossler, A. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35,* 20–40.

Holtfreter, K., Reisig, M. D., & Pratt, T. C. (2008). Low self-control, routine activities, and fraud victimization. *Criminology, 46,* 189–220.

King, J. E., Walpole, C. E., & Lamon, K. (2007). Surf and turf wars online—Growing implications of internet gang violence. *Journal of Adolescent Health, 41*(6), S66–68.

Klein, M. W. (1971). *Street gangs and street workers.* Englewood Cliffs, NJ: Prentice-Hall.

McCuddy, T., & Vogel, M. (2015). More than just friends: Online social networks and offending. *Criminal Justice Review, 40,* 169–189.

Morselli, C., & Décary-Hétu, D. (2013). Crime facilitation purposes of social networking sites: A review and analysis of the 'cyberbanging' phenomenon. *Small Wars & Insurgencies, 24*(1), 152–70.

Moule Jr., R. K., Decker, S. H., & Pyrooz, D. C. (2014). Internet adoption and online behavior among American street gangs: Integrating gangs and organizational theory. *British Journal of Criminology, 54,* 1186–1206.

Moule Jr., R. K., Decker, S. H., & Pyrooz, D. C. (2015). Kollektive gewalt, gangs und das Internet. In A. T. Paul & B. Schwalb (Eds.), *Über eigendynamik und selbstorganisation kollektiver gewalt* (pp. 147–174). Hamburg: Hamburger Edition.

Norris, P. (2001). *Digital divide: Civic engagement, information poverty, and the internet worldwide*. Cambridge: Cambridge University Press.

Papachristos, A. V. (2005). Gang world. *Foreign Policy*, 48–55.

Patchin, J. W., & Hinduja, S. (2006). Bullies move beyond the schoolyard: A preliminary look at cyberbullying. *Youth Violence and Juvenile Justice, 4,* 148–169.

Patton, D. U., Dungy, L., & Hong, J. S. (2015). *Gang violence, crime, and substance use on Twitter: A snapshot of gang communications in Detroit.* Paper presented at the Society for Social Work and Research. Retrieved from https://sswr.confex.com/sswr/2015/webprogram/Paper23817.html

Patton, D. U., Eschmann, R. D., & Butler, D. A. (2013). Internet banging: New trends in social media, gang violence, masculinity and hip hop. *Computers in Human Behavior, 29,* A54–A59.

Pew Research Center. (2012a). *Social media use over time.* http://www.pewinternet.org/data-trend/teens/social-media/

Pew Research Center. (2012b). *Internet user demographics.* Retrieved from http://www.pewinternet.org/data-trend/teens/internet-user-demographics/

Pew Research Center. (2012c). *Device ownership over time.* Retrieved from http://www.pewinternet.org/data-trend/teens/devices/

Pew Research Center. (2014a). *Internet user demographics.* Retrieved from http://www.pewinternet.org/data-trend/internet-use/latest-stats/

Pew Research Center. (2014b). *Cell phone and smart phone ownership demographics.* Retrieved from http://www.pewinternet.org /data-trend/mobile/cell-phone-and-smartphone-ownership-demographics/

Pew Research Center. (2015). *Teens, social media, and technology 2015 overview.* Retrieved from http://www.pewinternet.org/ 2015/04/09/teens-social-media-technology-2015/

Pyrooz, D. C., Decker, S. H., & Moule Jr., R. K. (2015). Criminal and routine activities in online settings: Gangs, offenders, and the Internet. *Justice Quarterly, 32,* 471–499.

Schulz, A., Bergen, E., Schuhmann, P., Hoyer, J., & Santtile, P. (2015). Online sexual solicitation of minors: How often and between whom does it occur? *Journal of Research in Crime and Delinquency*. doi: 10.1177/0022427815599426

Sela-Shayovitz, R. (2012). Gangs and the web: Gang members' online behavior. *Journal of Contemporary Criminal Justice, 28*(4), 389–405.

Tcherni, M., Davies, A., Lopes, G., & Lizotte, A. (2015). The dark figure of online property crime: Is cyberspace hiding a crime wave? *Justice Quarterly*. doi: 10.1080/07418825.2014.994658

van Hellemont, E. (2012). Gangland online: Performing the real imaginary world of gangstas and ghettos in Brussels. *European Journal of Crime, Criminal Law and Criminal Justice, 20,* 165–80.

van Wilsem, J. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. *European Journal of Criminology, 8,* 115–127.

Wahl-Jorgensen, K. (2015). The Chicago School and ecology: A reappraisal for the digital era. *American Behavioral Scientist*. doi: 0002764215601709

Warner, B. D., & Sampson, R. J. (2015). Social disorganization, collective efficacy, and macro-level theories of social control. In F. T. Cullen, P. Wilcox, R. J. Sampson, & B. Dooley (Eds.), *Challenging criminological theory: The legacy of Ruth Rosner Kornhauser* (pp. 215–236). New Brunswick, NJ: Transaction.

Weimann, G. (2006). Virtual disputes: The use of the Internet for terrorist debates. *Studies in Conflict & Terrorism, 29,* 623–639.

Westlake, B., & Bouchard, M. (2015). Criminal careers in cyberspace: Examining website failure within child exploitation networks. *Justice Quarterly*. doi: 10.1080/07418825.2015.1046393

Wijeratne, S., Doran, D., Sheth, A., & Dustin, J. L. (2015). Analyzing the social media footprint of street gangs. *Intelligence and Security Informatics, 1,* 91–96. doi:10.1109/ISI.2015.7165945

Wolfe, S. E., Higgins, G. E., & Marcum, C. A. (2007). Deterrence and digital piracy: A preliminary examination of the role of viruses. *Social Science Computer Review, 26,* 317–333.

Womer, S., & Bunker, R. J. 2010. Sureños gangs and Mexican cartel use of social networking sites. *Small Wars & Insurgencies, 21*(1), 81–94.

Zhou, Y., Reid, E., Qin, J., Chen, H., & Lai, G. (2005). U.S. domestic extremist groups on the web: Link and content analysis. *IEEE Intelligent Systems, 20,* 44–51.

***David Pyrooz** is Assistant Professor of Sociology at the University of Colorado at Boulder. His research focuses on gangs and criminal networks, crime trends and life-course criminology, violent offending and victimization, and incarceration and offender reentry.*

****Richard K. Moule, Jr.** is a doctoral candidate in the School of Criminology and Criminal Justice whose research interests include gangs and other deviant networks, criminological theory, and the intersection of technology and crime. His dissertation explores the negative influence of adolescent gang membership on a number of social, economic, and health outcomes among a sample of juvenile delinquents from the 1930s.*

*****Scott H. Decker** is a Foundation Professor of Criminology and Criminal Justice at Arizona State University. Professor Decker's primary research focus has been on criminal justice policy, gangs, violence, and the offender's perspective.*

On the Need for Policing Cybercrime Research

Adam M. Bossler, Georgia Southern University*
Thomas J. Holt, Michigan State University**

Over the last three decades, criminologists have examined issues related to cybercrime—or the use of technology and the Internet in order to engage in various forms of crime. The body of scholarship in this area has transitioned from definitional debates to empirical assessments, which has improved our understanding of the factors associated with both cyber-victimization and cyber-offending (Holt & Bossler, 2014). There has been less research, however, on the criminal justice system's response to cybercrime during this time. In fact, only a handful of published studies have examined issues related to policing or the prosecution of cybercrime with empirical data (Holt, Burruss, & Bossler, 2015). Instead, the vast majority of works that discuss criminal justice system issues pertaining to cybercrime consist of opinion pieces or theoretical discussions on the reasons why cybercrimes are largely not processed through the justice system.

The dark figure of cybercrime presents a major challenge in examining the criminal justice system's response to cybercrime. There are few official data sources that provide metrics for offenses involving computer systems. This information is absent in the Uniform Crime Report, though there is some detail available in the National Incident Based Reporting System (NIBRS), which would allow for the identification of computers involved in the course of an offense. NIBRS data, however, are not yet representative of the U.S., making its utility limited. The Internet Crime Complaint Center (IC3), a joint venture by the FBI, National White Collar Crime Center (NW3C), and the Bureau of Justice Assistance, receives complaints from individuals who have been victimized by crime through the Internet. The IC3 data indicates that the number of complaints increased from 16,838 in 2000 to 262,831 in 2013, but much of this could be the result of the center's success in promoting its reporting website, rather than an accurate depiction of Internet crime trends (Holt & Bossler, 2016).

This lack of reporting would suggest that police agencies may have limited experience with, or awareness of, how to respond to cybercrime calls for service. Certainly the mechanics of a cybercrime incident are somewhat different from those of traditional offenses. In the event an individual is stalked or harassed online, the individual would have to provide e-mail or social media posts that demonstrate the offense in action. Some victims may delete this information, which would require internet service providers to be contacted in the hopes that this information may be recovered. For other offenses, it may be difficult to find proof to support the case, as with identity theft in which an offender resides in another nation. The original incident that led victims to lose their credit or debit card information may have occurred months ago, and the victims may only know that something has occurred because

because they monitor their account statements.

Despite these data issues, there is a need for researchers to examine how criminal justice system actors recognize and deal with cybercrime cases. There is a particular need for research examining the local-level response to cybercrime. Both police scholars and administrators have called for local law enforcement to improve their response capabilities for cybercrime calls for service, including having better-trained first responders (e.g., Police Executive Research Forum, 2014; Stambaugh et al., 2001). Line officers in police agencies are likely to receive calls for service at some point in the field, as they are the primary point of contact for citizens in the event of an emergency (Police Executive Research Forum, 2014). Local police agencies, however, are limited by their jurisdictional boundaries and do not have the same resources as federal law enforcement agencies such as the Federal Bureau of Investigation and the Secret Service. As a consequence, local officers may be unable to properly respond to incidents to the satisfaction of either victims or prosecutors. This may also bias their experiences when dealing with cybercrime calls for service, leading officers to perceive them to be low priority.

Examining Local Police Officers' Attitudes and Beliefs Regarding Cybercrime

A small body of research has emerged that examines the perceptions of cybercrime among either administrators or representatives of local law enforcement agencies (e.g., Hinduja, 2004; Marcum, Higgins, Freiburger, & Ricketts, 2010; Police Executive Research Foundation, 2014; Stambaugh et al., 2001). There have been only a small number of studies, however, that have examined the perceptions and experiences of patrol officers regarding cybercrime (e.g., Senjo, 2004; Bossler & Holt, 2012; Holt & Bossler, 2012a; Holt et al., 2015). This line of research is vital, considering that patrol officers are being asked to be more effective first responders to digital forensic crime scenes as a crucial step in combatting online crime at the local level.

In an attempt to understand what line officers thought about cybercrime, we surveyed patrol officers in the Charlotte-Mecklenburg, NC police department (CMPD) and Savannah-Chatham, GA metropolitan police department (SCMPD) to examine their perceptions of, interest in, and preparation for cybercrime (Bossler & Holt, 2012; Holt & Bossler, 2012a). Despite being in the same geographic region, the cities differ in terms of population, racial composition, and industrial base. Charlotte is a large city with approximately 687,456 residents in the city limits and more than two million in the combined statistical area, while Savannah has a smaller population of 134,669 residents. Savannah is largely African American (57%), while Charlotte is predominantly white (55%). Charlotte is also a key banking and financial hub, while Savannah's economy is driven by tourism, shipping, and the military. The city police forces differed in size, as the CMPD had more than 1,400 patrol officers compared to just under 400 patrol officers in the SCMPD. Savannah also had no specialized cybercrime unit, while Charlotte had a burgeoning cybercrime task force.

Officers in both cities reported having minimal cybercrime investigation training and experience with previous computer crime cases. Only 11.6% of the respondents had cybercrime investigation training, with 16.1% of Charlotte officers reporting training compared to 7.6% of Savannah officers. Younger officers and those with some college experience were more likely to have completed cybercrime training. It is not surprising that 61.5% of all officers had no experience with cybercrime cases, given that anecdotal evidence suggests individuals do not contact law enforcement if they have been victims of a cybercrime. There were no demographic correlates associated with prior case experience, most likely reflecting the random assignment of most calls for service based on available patrol officers. As a result, many officers who responded to calls for service may not have had any cybercrime training.

Understanding patrol officer perceptions regarding the uniqueness, frequency, and seriousness of cybercrime helps us better understand the importance that officers place on addressing cybercrime (Holt & Bossler, 2012a; Senjo, 2004). Officers in our two city samples (Holt & Bossler, 2012a) were mixed regarding whether they agreed that "cybercrime is mostly traditional crime using a computer"; 39% of the officers agreed, one-quarter disagreed, but 37.9% were unsure. The mixed response is in line with findings regarding confusion among the general public over the nature of cybercrimes in general (Furnell, 2002). Officers with cybercrime training, however, were more likely to conceive of these offenses as traditional crimes enabled by a computer. Thus, training may aid in adjusting officer perceptions of cybercrime by allowing them to see the similarities across the cyber divide.

An area of policing cybercrime research that has been studied in a little more depth than other areas is how law enforcement perceives the seriousness of cybercrime (e.g., Burns et al., 2004; Holt & Bossler, 2012a; Senjo, 2004). Local law enforcement agencies have generally placed a lower priority on computer crimes, with the exception of child pornography or child exploitation cases (e.g., Hinduja, 2004; Stambaugh et al., 2001). Our analysis of patrol officers' responses, however, indicated that patrol officers may categorize crimes similarly based on their impact rather than their setting (online vs. offline; Holt & Bossler, 2012a). Officers were asked to rank the seriousness (1 = not serious; 2 = a little serious; 3 = somewhat serious; 4 = serious; 5 = very serious) of 12 forms of crime: five traditional offenses (armed robbery, burglary, selling cocaine, shoplifting, and vandalism) and seven computer crimes (copyright infringement, credit card fraud, electronic theft of money from accounts, harassment over the Internet, identity theft, pedophilia on the Internet, and malicious software infections). Their scores indicated that the crimes could be categorized into three groups: (1) serious offenses, including armed robbery, pedophilia, burglary, electronic theft, identity theft, selling cocaine, and credit card fraud; (2) moderately serious offenses, which included malicious software infection and online harassment; and (3) less serious offenses, which included vandalism, copyright infringement, and shoplifting. Although armed robbery was ranked as the most serious offense, probably due to its emotional impact on victims and potential role in homicides, these officers viewed online pedophilia as the most serious form of cybercrime, as a result of its violent and emotional harm caused to young victims,

congruent with previous research (e.g., Hinduja, 2004; Senjo, 2004; Stambaugh et al., 2001). In addition, property offenses that occur more often to businesses, public buildings, and large corporations than individuals, such as vandalism, shoplifting, and copyright infringement, were seen as relatively similar.

Finally, little has been examined regarding officer perceptions of the frequency of various forms of cybercrime. It should be noted that surveying officers about their perceptions of the frequency with which cybercrime occurs should never be utilized as a measure of how often these forms of crime actually occur, even in relation to other crimes, but rather as information that provides insight into how officers view these problems. When officers were asked to assess the frequency (1 = rare; 2 = somewhat rare; 3 = somewhat frequent; 4 = frequent; 5 = very frequent) of the same 12 offenses discussed earlier, we found that the top five offenses perceived as most frequent were all traditional offenses. Since some online incidents, such as online harassment and copyright infringement, occur more often than traditional crimes, their views are not congruent with reality. This misperception could be the result of several factors, including the underreporting of cybercrime to the police and their lack of personal and vicarious experiences with cybercrime calls for service.

Law Enforcement Response to Cybercrime

Over the last 10 to 20 years, a small number of scholars and police administrators have concluded that local law enforcement needs to have a larger role in combatting various forms of cybercrime (e.g., Stambaugh et al., 2001); however, this call for an increased role by local law enforcement may not match the interests of the rank and file. In our research, we found that patrol officers seemed either ambivalent or unsure about who should have primary responsibilities for cybercrime investigations (Bossler & Holt, 2012). Half of the officers neither agreed nor disagreed with the notion that federal and state law enforcement agencies had the primary responsibility for controlling local cybercrime. The remainder were equally split in terms of agreement and disagreement with this statement. Only 18% of respondents, however, agreed that controlling cybercrime in the local area was the primary responsibility of local law enforcement. Taken as a whole, officers were either unsure or did not believe that local law enforcement should have primary duties to investigate cybercrimes generally.

If local enforcement was going to be required or encouraged to handle an increase in cybercrime calls, a majority of the officers (73%) believed that cybercrime calls should be responded to directly by a specialized cybercrime unit, rather than by a patrol officer. Considering the challenges of cybercrime cases, including the collection and analyzing of digital evidence, it is not surprising that many local agencies, and particularly their officers, may want specialized task forces, such as an Internet Crimes Against Children (ICAC) taskforce, to hold the primary responsibility for investigating cybercrime cases. Recent research has shown that the increased presence of ICAC taskforces has increased the number of arrests for child exploitation crimes across the country (Marcum & Higgins, 2011; Wolak, Finkelhor, & Mitchell, 2012). However, patrol officers will continue to be the first responders to scenes that may have digital evidence. Therefore, although they may not be tasked with further investigation tasks, they, and not just special task forces, still need to be properly trained to respond to these

scenes. In fact, we have found that officers who had recently handled a cybercrime call for service were less likely to believe that specialized cybercrime units should directly respond to cybercrime calls (Bossler & Holt, 2012). Thus, actual case experience may generally increase officer confidence and efficacy in responding to cybercrime calls, which could inspire confidence that local officers can effectively respond to these cases.

One of the more troubling findings from this line of research was not their overall uncertainty about whether law enforcement in general takes cybercrime seriously enough, but their lack of knowledge of how their own agency was responding to cybercrime. We found that two-thirds of the officers did not know whether their departmental administrators took cybercrime seriously enough. Even more officers (71%) were unsure whether their agency was taking the proper steps to deal with cybercrime in their areas. These findings indicate that patrol officers were not informed about these issues during their roll call or through other means and that all agencies should examine how they are disseminating this information to their officers.

Considering that local law enforcement officers did not strongly support their agency taking a larger role in combatting cybercrime, we asked them to rank the importance (1 = not important; 5 = very important) of a series of 15 strategies, in order to assess their attitudes regarding how we as a society could better improve our responses to cybercrime (Bossler & Holt, 2012). The strategies were derived from well-known studies on police responses to cybercrime as well as recent suggestions from researchers and policy-making bodies. The findings suggested that these patrol officers did not dismiss any reasonable idea as being unimportant. The four strategies that ranked as the most important, however, did not require more responsibility for the police but rather asked for changes from online citizens, the courts, and legislation. According to these officers, the most effective strategy for improving our response to cybercrime was for citizens to be more careful when on the Internet. One way to encourage greater care while online would be through education programs for the public regarding cybercrime and cybersecurity. While law enforcement plays a role in communicating threats to citizen safety, officers in this sample felt that educating the public on the threat of cybercrime was a generally low priority (ranked ninth overall). The other three top recommendations required changes to the legal system to clarify existing laws, make prosecutions more effective, and to increase penalties for the commission of cybercrime.

In general, patrol officers ranked strategies that involved them or their agencies, such as staffing local cybercrime units (#11), providing more training to line officers (#13), and working with citizens (#15), as relatively lower priorities than the other strategies listed. In fact, respondents felt that working with citizens online to "police" the Internet was the least important strategy overall, with a mean score of 3.56, between "somewhat important" and "important." If the results of this study are indicative of the views of local patrol officers in other agencies throughout the U.S., there may be difficulties in winning their hearts and minds in becoming a more integral component of our response to cybercrime.

Officer Interest in Additional Training

Although officers may not view their role in combatting cybercrime as important as improvements to other strategies, it is clear that patrol officers will continue to be first responders to incidents that may involve digital evidence. Thus, they will need to be as well trained to respond to incidents involving digital evidence as they are to "traditional" cases, including securing evidence, interviewing witnesses, and developing information and leads (Holt et al., 2015; Stambaugh et al., 2001; NIJ, 2008). Our analyses of survey data collected from law enforcement officers who completed a digital forensic course from the NW3C indicated that younger, white officers from larger police departments with more years of experience handling digital evidence received more weeks of training than other officers (Holt et al., 2015).

Within our two-city sample, we surprisingly found that 40% of officers expressed an interest in conducting cybercrime investigations, and 57.7% were interested in cybercrime investigation training (Holt & Bossler, 2012b). There were several factors associated with an interest in training and investigation. Older officers with greater computer proficiency and no prior computer training were more likely to be interested in the training. Those officers who felt cybercrime investigation was valuable and believed that cybercrimes would change the nature of policing were more likely to desire training and investigative roles. There was no relationship between desire for training and participating in digital investigative roles and an officer's experience with cybercrime calls for service, suggesting that field work may not be the most important factor when selecting the individuals who should receive cybercrime training. Thus, the abilities of the officer and his or her attitudes toward the value of cybercrime investigations, and an awareness of how the Internet is affecting policing, could be better indicators for the selection of officers for further training and investigative roles. A better understanding of the factors that increase officer interest in this field would be valuable, to develop effective recruitment and retention strategies to fill these positions.

The Stress of Digital Forensic Examiners

Local law enforcement will continue to handle large numbers of digital evidence cases, including those that involve children. The investigation of cybercrimes, particularly child exploitation cases, is particularly stressful and traumatic for officers and investigators of these crimes. In fact, quantitative and qualitative research has found that between 25% and 50% of forensic investigators who deal with child pornography experience psychological harm (Burns et al., 2008; Perez et al., 2010). With the increased movement toward specialized units and personnel to investigate cybercrime, particularly child exploitation, it is necessary to know how these roles and experiences impact these particular officers. Unfortunately, few studies have focused on the stress and trauma that is reported by digital investigators (e.g., Holt & Blevins, 2012).

Surveying a sample of law enforcement officers who had received computer training through the NW3C, we found that specific investigators were more likely to indicate that they experienced work stress, including those investigators who had longer law enforcement careers (possibly because of exposure to more

violent images), felt role conflict within their working environment, perceived that they received less supervisory support, and reported less job satisfaction (Holt et al., 2015). Police administrators who fail to recognize the unique contributions of digital forensic investigators, the challenges they face, and the traumatic impact that viewing abusive images can have on an individual's emotional and psychological health can create stressful working environments in which examiners' hard work and stress may be underestimated.

Not surprisingly, examiners who viewed abusive images suffered both emotional and psychological harm. Although it was not surprising that we found that a small proportion of these investigators dealt with their experiences with negative coping mechanisms, such as drinking or abusing prescription pills, we also found that even fewer respondents sought professional help from either counselors or clergy. Rather, they chose to talk with spouses or colleagues about their traumatic experiences.

In summary, this limited body of research indicates that (1) digital examiners' unique experiences with images and files significantly impacts their working and personal environments, and (2) additional research is sorely needed. This additional research could include samples of officers with broader ranges of experiences with these cases. In addition, more in-depth interviews and ethnographic research with officers and task forces assigned to these cases would be invaluable in better understanding the daily activities of these officers, how it impacts their satisfaction with their jobs and burnout, how they cope with their effectively perform their jobs but decrease the impact that it has on them both professionally and personally.

trauma, and how we can better help them effectively perform their jobs but decrease the impact that it has on them both professionally and personally.

Support for Online Community Policing

As the above sections allude, law enforcement has typically responded to the various threats of cybercrime through traditional methods but in a virtual manner, such as improving our digital evidence collection and analysis, conducting online stakeouts and stings, and reducing criminal opportunities via a situational crime prevention framework (e.g., Newman & Clarke, 2003; Hinduja, 2007; Stambaugh et al., 2001). These methods, however, do not appropriately utilize the vast number of possible interactions and collaborations with citizens who "police" the Internet, non-law enforcement agencies, and business entities that spend significant time online and have vast wealth of knowledge regarding cyber-deviance and cybersecurity (Brenner, 2008; Wall, 2007). The success of community policing in certain contexts has encouraged some scholars and police administrators to therefore advocate for the adoption of similar programs in online environments, in order to incorporate these groups (e.g., Bossler & Holt, 2013; Holt et al., 2015; Wall & Williams, 2007), what one may term as "online community policing." Although there are few examples of fully operating programs in action, agencies in various countries, including the U.S., use social media to request information from the online community in order to both generate leads and provide alerts to the public on crimes in progress (e.g., Wang & Doong, 2010). The creation of strong collaborations with citizens, groups, and businesses that is required for fuller online community policing programs to take root

requires great effort, resources, and time, thus making it a challenging innovative strategy.

Some of our recent research has begun to examine officer interest and support for local law enforcement to work with these non-law enforcement individuals, groups, and business entities (Bossler & Holt, 2013, 2014; Holt et al., 2015). In our two cities, 40% of the officers agreed that the principles of community policing could be applied to an online environment; most, however, were unsure. Almost two-thirds felt that their departments should hold information workshops regarding cybercrime risks and prevention efforts in order to help educate the public. In addition, 60% thought it was important to work with netizens to police the Internet (Bossler & Holt, 2013).

One of the strongest and most consistent predictors of support for working with online citizens in a spirit of online community policing and collaborating with high-tech industries and service providers was the officers' support for traditional community policing. Officers who also perceived that cybercrimes often go unreported to the police were also likely to believe that online community policing would be a positive initiative. Those who perceived that cybercrime was both serious and drastically altering law enforcement realized that law enforcement could not combat cybercrime alone and needed to work more cooperatively with the business community and high-tech industries. If officers believed, however, that upper management was taking cybercrime seriously enough and responding appropriately, they were less likely to support engaging the community (Bossler & Holt, 2014). Finally, support for online community policing or working with non-law enforcement entities was not related to officer computer proficiency, whether measured by self-reported computer skill, the number of hours one spends online per week, or whether they had used the Internet to help with a case (Bossler & Holt, 2013; Holt et al., 2015).

The current research has only scratched the surface on what is needed to better understand support for online community policing strategies. First, process and outcome evaluations of these types of programs are necessary to understand how they operate, the factors affecting their successes, and their impact on citizens' perceptions of and willingness to report cybercrimes to legal authorities. In addition, scholars and police administrators need to continue to examine officer support for online community policing and the use of social media in order to improve officer willingness to engage with online communities.

Conclusion

As technology is transforming the world in which we live, there is a need for law enforcement agencies to understand both how computers and the Internet may be misused and how to best combat these offenses. Local police agencies are increasingly tasked with calls for service related to cybercrime, though it is not clear how well-prepared they may be to handle these cases. Without adequate national statistical measures for cybercrime offending and victimization, however, it is challenging at best to determine how rates of cybercrime are changing and whether law enforcement responses have had any significant impact. Clearly, our data collection efforts need to be greatly improved. In addition, the lack of research on policing cybercrime has created a situation in which even the most preliminary research would help to fill this void.

Our research has found that officers had some experience with cybercrime training and investigation. We also found that many officers had no opinions or solid perceptions of various aspects of computer crime. In general, they would rather not become directly involved in cybercrime cases and would prefer they be handled via other means. Particularly, they place greater emphasis on citizens changing their online behavior and changes to our legal system. Officers considered working with the public to understand cybercrime as one of the least important strategies to help deal with these crimes, although some scholars have argued that the use of social media and online community policing principles may help the police improve their response to cybercrime by tapping into one of the greatest untapped resources: online citizens. When selecting officers to participate in innovative online strategies, whether through social media or public workshops, the evidence suggests that police administrators may find greater success choosing officers who support working with citizens, high-tech industries, and service providers than basing decisions on computer proficiency.

Our overall findings also suggest there is a need for police administrators to expose line officers to the concept of cybercrime in departmental meetings, as well as early on in academy training programs. Increasing officer awareness could help sharpen officer perceptions of these crimes and improve their response to calls for service and victim interactions in the field. Additionally, there is a need for substantial research using samples of line officers from across the U.S. to better document the state of the field. Almost all studies in this field are geographically limited, raising questions about generalizability. Research is therefore sorely needed that samples small, medium, and large agencies across the nation to better understand officers' experiences, perceptions, interests, and insights. In addition, qualitative work that dives into the experiences of patrol officers and specialized units would be additionally beneficial to better understand these individuals' working environment, including the cultural support they receive, the impact that these cases have on their lives, and how they cope with it. Without such information, we may never be able to develop a coherent roadmap for local agencies to aid in combating cybercrime in the future.

References

Bossler, A. M., & Holt, T. J. (2012). Patrol officers' perceived role in responding to cybercrime. *Policing: An International Journal of Police Strategies and Management, 35*(1), 165–181.

Bossler, A. M., & Holt, T. J. (2013). Assessing officer perceptions and support for online community policing. *Security Journal, 26*(4), 349–366.

Bossler, A. M., & Holt, T. J. (2014). Further examining officer perceptions and support for online community policing. In C. D. Marcum & G. E. Higgins (Eds.), *Social networking as a criminal enterprise* (pp. 167–196). Boca Raton, FL: CRC Press.

Brenner, S. W. (2008). *Cyberthreats: The emerging fault lines of the nation state.* New York: Oxford University Press.

Burns, C. M., Morley, J., Bradshaw, R., & Domene, J. (2008). The emotional impact on and coping strategies employed by police teams investigating Internet child exploitation. *Traumatology, 14,* 20–31.

Burns, R. G., Whitworth, K. H., & Thompson, C. Y. (2004). Assessing law enforcement preparedness to address Internet fraud. *Journal of Criminal Justice, 32*, 477–493.

Furnell, S. (2002). *Cybercrime: Vandalizing the information society*. London: Addison-Wesley.

Hinduja, S. (2004). Perceptions of local and state local law enforcement concerning the role of computer crime investigative teams. *Policing: An International Journal of Police Strategies and Management, 3,* 341–357.

Hinduja, S. (2007). Computer crime investigations in the United States: Leveraging knowledge from the past to address the future. *International Journal of Cyber Criminology, 1,* 1–26.

Holt, T. J., & Blevins, K. R. (2012). Examining job stress and satisfaction among digital forensic examiners. *Journal of Contemporary Criminal Justice, 27*, 230–250.

Holt, T. J., & Bossler, A. M. (2012a). Police perceptions of computer crimes in two southeastern cities: An examination from the viewpoint of patrol officers. *American Journal of Criminal Justice, 37*(3), 396–412.

Holt, T. J., & Bossler, A. M. (2012b). Predictors of patrol officer interest in cybercrime training and investigation in selected United States police departments. *Cyberpsychology, Behavior, and Social Networking, 15*(9), 464–472.

Holt, T. J., & Bossler, A. M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behavior, 35*(1), 20–40.

Holt, T. J., & Bossler, A. M. (2016). *Cybercrime in progress: Theory and prevention of technology-enabled offenses.* London: Routledge.

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2015). *Policing cybercrime and cyberterror.* Durham, NC: Carolina Academic Press.

Marcum, C., & Higgins, G. E. (2011). Combating child exploitation online: Predictors of successful ICAC task forces. *Policing: A Journal of Policy and Practice, 5,* 310–316.

Marcum, C., Higgins, G. E., Freiburger, T. L., & Ricketts, M. L. (2010). Policing possession of child pornography online: Investigating the training and resources dedicated to the investigation of cybercrime. *International Journal of Police Science and Management, 12*, 516–525.

National Institute of Justice. (2008). *Electronic crime scene investigations: A guide for first responders* (2nd ed.) NCJ 219941. Washington, DC: Author.

Newman, G., & Clarke, R. (2003). *Superhighway robbery: Preventing e-commerce crime.* Cullompton, NJ: Willan Press.

Perez, L. M., Jones, J., Engler, D. R., & Sachau, D. (2010). Secondary traumatic stress and burnout among law enforcement investigators exposed to disturbing media images. *Journal of Police and Criminal Psychology, 25*, 113–124.

Police Executive Research Forum. (2014). *The role of local law enforcement agencies in preventing and investigating cybercrime.* Washington, DC: Author.

Senjo, S. R. (2004). An analysis of computer-related crime: Comparing police officer perceptions with empirical data. *Security Journal, 17,* 55–71.

Stambaugh, H., Beaupre, D. S., Icove, D. J., Baker, R., Cassady, W., & Williams, W. P. (2001). *Electronic crime needs assessment for state and local law enforcement.* Washington, DC: National Institute of Justice. Retrieved August 3, 2010, from http://www.ncjrs.gov/pdffiles1/nij/186276.pdf.

Wall, D. S. (2007). *Cybercrime: The transformation of crime in the information age.* Cambridge, UK: Polity Press.

Wall, D. S., & Williams, M. (2007). Policing diversity in the digital age: Maintaining order in virtual communities. *Criminology and Criminal Justice, 7,* 391–415.

Wang, H. C., & Doong, H. S. (2010). Does government effort or citizen word-of-mouth determine e-government service diffusion? *Behaviour and Information Technology, 29*(4), 415–422.

Wolak, J., Finkelhor, D., & Mitchell, K. (2012). *Trends in law enforcement responses to technology-facilitated child sexual exploitation crimes: The Third National Juvenile Online Victimization Study (NJOV-3).* Durham, NH: Crimes against Children Research Center.

***Dr. Adam Bossler** is an Associate Professor of Criminal Justice and Criminology. He earned his doctorate in criminology and criminal justice from the University of Missouri – St. Louis. His* most recent publications can be found in *Crime & Delinquency*, *Youth & Society*, *American Journal of Criminal Justice*, *Policing*, and *Journal of Criminal Justice*.

****Thomas J. Holt** is an Associate Professor in the School of Criminal Justice at Michigan State University whose research focuses on computer hacking, malware, and the role of the Internet in facilitating all manner of crime and deviance. His work has been published in various journals including Crime and Delinquency, Deviant Behavior, Journal of Criminal Justice, and Youth and Society.*

Special Issue: New Directions in Cybercrime Research

Guest Editor, Thomas J. Holt*

I was elated when Robert Worley approached me with the opportunity to edit a special issue of *ACJS Today* focusing on cybercrime—when offenders use the Internet and technology in order to offend. Having studied cybercrime for the last 12 years, I have seen this area of research grow from a topic at the margins of criminal justice and criminology to become a large body of study with interdisciplinary focus. Research on cybercrimes using empirical data have increased dramatically over the last decade, with tests of various theories to explain victimization and offending. The state of the literature has improved dramatically, though there are many questions that must still be addressed, from the role of on- and off-line experiences in offending to the criminal justice responses to cybercrime.

The works included in this issue by top scholars in the discipline highlight some of the most critical issues present in criminological and criminal justice research. Billy Henson and Brad Reyns provide an overview of the transformation of research regarding cybercrime victimization. They highlight the strengths and weaknesses of this literature and highlight ways that the field can improve its understanding of victimization generally.

The article by David Pyrooz, Richard Moule, and Scott Decker demonstrates the effect that access to technology has on real-world offending. Their research on gang members' use of technology has substantial value for our understanding of the ways that digital experiences are shaping the experiences of individuals and the challenges that this presents for researchers and practitioners alike.

My long-time colleague Adam Bossler and I consider the impact that the Internet and cybercrimes have for local law enforcement officers. Few have examined the ways that line officers think about cybercrime or how they feel these offenses should be dealt with. Thus, this article summarizes a number of studies on these issues and points to the need for improved research on the criminal justice system response to cybercrime.

Finally, my friend Special Agent Thomas Hyslip of the Department of Defense, Defense Criminal Investigative Service (DCIS) was kind enough to answer my questions regarding his experiences in investigating cybercrimes. He demonstrate how individuals become cybercrime investigators and the issues they face in the field.

In producing this issue, I must thank the authors whose work is on the cutting edge of the field for sharing their insights. Many thanks to Special Agent Tom Hyslip for his willingness to take time out to help us better understand the experiences of law enforcement. It is an area that few are exposed to, so his insights are invaluable. Finally, I must thank the regular editor, Robert Worley, for the opportunity to put this issue together. Cybercrime research is increasing in prominence, and the opportunity to share great research with the larger Academy is greatly appreciated.

***Thomas J. Holt** is an Associate Professor in the School of Criminal Justice at Michigan State University whose research focuses on computer hacking, malware, and the role of the Internet in facilitating all manner of crime and deviance. His work has been published in various journals including Crime and Delinquency, Deviant Behavior, the Journal of Criminal Justice, and Youth and Society.*

This Is Where We Leave You: The Current State of Cybercrime Victimization Methodology

Billy Henson, Shippensburg University*
Brad Reyns, Weber State University**

Our interest in studying online victimization began when we were first-year Ph.D. students. Back then, the cyber landscape looked very different than it does today. Facebook had just become open to the general public, phones were still stupid (relatively speaking), and many people were still using Netscape to browse the Internet. While there were a few cybercrime victimization studies, most were very basic and many were not very methodologically sound. Unfortunately, cybercrime was simply not a topic of interest among most criminologists. Like us, many of the now-notable cybercrime researchers had only just begun to explore the realm of online crime. Since that time, much has changed, however. In the last decade, cybercrime victimization has come into its own as a serious topic of research. There are currently dozens, if not hundreds, of cybercrime studies, focusing on a broad range of crime types, criminological theories, and outcomes. Such significant growth in a short period of time allows us to review the good, the bad, and the ugly with regard to cybercrime victimization research methods.

The Good

As with the technology that fuels it, we have seen an exponential growth in the numbers and quality of cybercrime victimization studies in the last decade. However, as with any new arena of research, there have been more than a few stumbling blocks along the way. One of the key challenges many researchers have encountered is the question of how to collect the necessary data. For years, secondary cybercrime victimization data simply did not exist. Even today, there are only a few large-scale datasets that include measures of cybercrime victimization. And, while some researchers are working with those datasets (see Reyns, Randa, & Henson, 2016, for an example), many more have turned to collecting primary data. It is in this area that we've seen some of the better improvements in cybercrime research.

Simply put, in the beginning, we did not know what we were doing. The online medium was entirely new, and we failed to utilize it effectively. Most researchers were still using pencil-and-paper surveys to collect data about cybercrime. That is the equivalent of calling someone's landline to ask him about his cell phone use. Technology, and more specifically the Internet, was the lifeline of the new generation—a generation that, quite frankly, was already forgetting how to use a pencil. We were using antiquated methods to examine a cutting-edge form of crime. Luckily, we quickly learned how to reach potential respondents on their own level. Online surveys became the norm for most cybercrime researchers. They allow us to interact with respondents in an environment

with which they find comfort and familiarity. However, while the tools for data collection improved, our methodology was slow to follow.

When online surveys were first used for cybercrime research, issues of generalizability of the resulting data and/or lack of consistency of sample demographics were often overlooked for the sake of getting enough cases to perform an analysis. For example, this issue was addressed in one of the first studies to examine cyberstalking victimization. With his work, Bocij (2003) noted that he utilized an online survey, which was essentially randomly e-mailed to friends of friends. As a result, he was unable to report any generalizable results. Other studies were based on similar lackluster techniques, with some posting their survey on a website for anyone to complete. This was simply the negative side effects of an otherwise improved approach to collecting data.

Fortunately, today, our ability to effectively use electronic surveys has improved dramatically. With practice, researchers are now better able to design and disseminate surveys in a manner that results in improved response rates and more detailed data. Cybercrime researchers can now target specific populations (e.g., college students), reach those populations more effectively, and obtain large amounts of information at a relatively low cost. Our research methods are finally catching up with our research topics.

The Bad

As stated before, there have been a large number of cybercrime studies published to date. Ordinarily, one could say that such a wealth of information about a given topic would be a great benefit to improving our understanding of said topic. Unfortunately, however, reviewing the whole of the published cybercrime literature reveals a fundamental flaw in the growth of the research. There is a serious lack of direction. One could review any given dozen cybercrime studies and easily read about at least half a dozen different topics/types of cybercrime. Very little effort has been made to establish and/or build upon a foundation. As a result, the growth of our knowledge of cybercrime has been somewhat stunted.

One of the central explanations for this flaw is a lack of focus on any given topic. This is driven partially by how quickly and frequently technology changes. It seems that the constant change has hypnotized many researchers, convincing them to chase the newest "buzz" topic (e.g., revenge porn, trolling). That's not to say that such topics don't deserve attention, but rather than continuing to cultivate research on a few, specific forms of cybercrime, we have elected to analyze anything and everything related to field. While this has produced an impressive breadth of knowledge, it has greatly restrained our depth of knowledge.

Because of our desire to be the first to examine a particular issue or topic, the field has become saturated with an array of cybercrime topics and measures. As a result, there are

literally hundreds of cybercrime measures within the literature, but there are no uniform, replicated measures. For example, Hinduja and Patchin (2008) defined cyberbullying as "bothering someone online, teasing in a mean way, calling someone hurtful names, intentionally leaving persons out of things, threatening someone, and saying unwanted sexually-related things to someone" (p. 138), while Rivers and Noret (2010) use 11 various items to define cyberbullying, including "threats to damage existing relationships" and "demands/instructions." While this creates more problems than can be discussed here, the dominant problem is our inability to compare results across studies. This goes beyond the desire to discuss predictors or outcomes of cybercrime victimization and gets at the very base of our understanding of cybercrime. How can we, with any level of scholarly responsibility, even provide an idea of the prevalence of cybercrime victimization when different studies report percentages that vary by more than 75%?

Unfortunately, our lack of focus has left a dark cloud over the cybercrime literature. Until there is more consistency in measures, it may be irresponsible to compare information across studies. We need to return to methodology fundamentals. In order to truly move the field forward, more attention must be given to basics of measurement and design.

The Ugly

As the study of cybercrime has matured, research has advanced beyond merely estimating its scope to also identifying In doing this, cybercrime scholars have turned to existing theories of offline crime and victimization. Many times this process has been messy and challenging, and the results have not always borne out the practice. We say this for three reasons.

First, applying current theories to a new social context such as cyberspace can introduce issues that were simply not foreseeable at the time the theories were developed. For example, within the field of victimology the lifestyle-exposure and routine activity theories are arguably the most popular perspectives used by researchers to understand victimization risk. They were also published in the late 1970s. Thus, the applicability of these theories to online types of victimization has been debated and is still somewhat unsettled. This is because the architects of these theories created them to explain personal victimization and direct-contact crime, respectively. Online experiences don't necessarily fit within either of these boundaries. Further, even if logical arguments can be (and have been) made for how the theories can be adapted to fit this new social context, that doesn't mean that the theories have proven their utility in explaining online forms of crime and victimization. These same growing pains also are evident when applying other criminological and victimological theoretical frameworks to online outcomes.

Second and relatedly, this may be due to the conceptualization, operationalization, and measurement choices of cybercrime scholars. As noted previously, there has been a distinct absence of uniformity of measurement across studies in the cybercrime research literature. The issue is no less serious or prevalent when it comes to theory testing. In some ways, this is a

reflection of the larger fields of criminology and victimology, but the newness of the study of cybercrime amplifies the difficulty. For instance, in continuing with the examples of lifestyle-exposure and routine activity theories, not only do cybercrime scholars need to explain *how* and *why* the theories apply to the social context, but they must also craft measures of theoretical concepts such as exposure, proximity, target suitability and guardianship—concepts that take on special meanings in this new social context (see Reyns, Henson, & Fisher, 2011).

Third, as previously noted, the results have not always been pretty. Despite researchers' assertions that the empirical evidence speaks to the utility of the theories in the online world of cyberspace, theoretical support for these traditional theories has often been modest at best. Again, we lay the blame for this squarely on measurement differences across studies. For example, an unscientific non-random sampling of the online routine activity literature yielded the following measures of guardianship: use of security software, use of firewalls, computer proficiency/skill of the user, risky information sharing, deleting e-mails, changing passwords, location of the computer or device, presence of others in the room while using the Internet, whom the individual lives with, social network privacy settings, personal online deviant behavior, and the online behaviors of peers. In some ways, it is therefore not surprising that support for this part of the theory is not very robust—we haven't decided how best to measure it yet. On a positive note, however, theories with established measures that make a straightforward transition from offline to online applications have fared better. A case in point is the usefulness of self-control as an indicator of both online offending and online victimization. A potential reason for the success of this theory in cybercrime studies may be that the field has coalesced around a more or less uniform measure of the concept (see Pratt, Turanovic, Fox, & Wright, 2014).

This Is Where We Leave You

With regard to cybercrime victimization methodology, there has been some good, there has been some bad, and there has been some ugly. So, where does this leave us? As we move forward, if we want to continue to advance the field of cybercrime victimization, there are three main areas that need further attention. First, in order to be able to effectively compare results across studies, we need to focus on creating more uniform measures of cybercrime victimization. At the very least, we need to identify central definitions of the types of cybercrime (e.g., cyberstalking, cyberbullying, hacking). This will help produce some cohesion within the field. Second, there needs to be considerable attention given to the development of uniform measures of theoretical concepts. Can traditional criminology and victimology theories be applied to cyberspace, or are completely autonomous theories necessary? Unless we can more effectively test these theories in the cyber realm, we may never truly know. Finally, we need to improve collaboration among cybercrime victimization researchers. Rather than competing with one another, more effort to solidify a research foundation and build upon others' work is necessary. With a little work, the good can easily overtake the bad and ugly.

References

Alexy, E. M., Burgess, A. W., Baker, T., & Smoyak, S. A. (2005). Perceptions of cyberstalking among college students. *Brief Treatment and Crisis Intervention, 5*(3), 279–289.

Bocij, P. (2003). Victims of cyberstalking: An exploratory study of harassment perpetrated via the Internet. *First Monday, 8*. Retrieved June 26, 2015, from http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1086/1006.

Hinduja, S., & Patchin, J. W. (2008). Cyberbullying: An exploratory analysis of factors related to offending and victimization. *Deviant Behavior, 29*(2), 1–29.

Pratt, T. C., Turanovic, J. J., Fox, K. A., & Wright, K. A. (2014). Self-control and victimization: A meta-analysis. *Criminology, 52*(1), 87–116.

Reyns, B. W., Henson, B., & Fisher, B. S. (2011). Being pursued online: An adaptation and application of lifestyle-routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, *38*(11), 1149–1169.

Reyns, B. W., Randa, R., & Henson, B. (2016). Preventing crime online: Identifying determinants of online preventive behaviors using structural equation modeling and canonical correlation analysis. *Crime Prevention and Community Safety, 19*(1).

Rivers, I., & Noret, N. (2010). 'I h 8 u': Findings from a five-year study of text and email bullying. *British Educational Research Journal, 36*(4), 643–671.

Combatting Crime On-Line: A Conversation With Special Agent Thomas Hyslip

Special Agent Thomas Hyslip

Recently, Guest Editor, Tom Holt caught up with Special Agent Thomas Hyslip, the Resident Agent in Charge of the Department of Defense, Defense Criminal Investigative Service (DCIS), Cyber Field Office, Eastern Resident Agency. Agent Hyslip has specialized in cybercrime investigations and computer forensic and has testified as an expert witness on computer forensics and network intrusions at numerous federal, state, and local courts. Agent Hyslip graciously answered several of Tom's questions and discussed highlights of his fascinating career.

TH: How did you start your career in law enforcement?

SATH: I started as a Special Agent with the Secret Service in 1998. After 5 years in the Army, I knew I wanted to work in law enforcement, but was limited to where I could apply because of my location. I was stationed at Rock Island Arsenal, IL, and all the state or local law enforcement jobs would have required me to travel to the location numerous times during the application process. So I concentrated on federal law enforcement, and thankfully the Secret Service was hiring. At that time I didn't have any preference as to what agency I worked for, so I applied to the Secret Service, ATF, and DEA and took the first offer I received.

TH: What drew you to the field?

SATH: I thought law enforcement in general would be rewarding, yet challenging. My undergraduate degree is in engineering, so I have always enjoyed solving problems, and the thought of conducting investigations was intriguing. So my goal was to become a detective with a state or local agency or an agent with a federal agency.

TH: How long have you worked for DOD OIG?

SATH: Eight years in May 2015.

TH: And, what led you to work on cybercrime?

SATH: After I was hired by the Secret Service in 1998, cybercrime began to significantly increase. America Online was in its prime, and high speed Internet through the cable companies was spreading fast. Also at that time, the Secret Service was the lead federal agency for investigating cybercrime, other than national security investigations, and those were done by the FBI. I was assigned to the Pittsburgh field office, and the Secret Service was training at least one agent per

office to investigate cybercrime and conduct computer forensics. When the Special Agent in Charge asked if anyone was interested in being trained, I volunteered. I was also interested in computers and thought the training would be fun. I had no idea at the time that it would lead to my entire career being in cybercrime.

TH: Can you explain the mission of your office/role?

SATH: The mission of the DOD IG is to fight fraud, waste, and abuse in the Department of Defense. The Defense Criminal Investigative Service (DCIS) is the criminal enforcement arm of the IG. Within the DCIS, there is the Cyber Field Office, and the mission is to investigate computer intrusions into the DoD and other cybercrimes that affect the DoD and its programs. So in addition to intrusions within the DoD, we also investigate intrusions into DoD contractors when DoD information is affected. We also provide computer forensics support to the entire DCIS for all the criminal investigations. We also provide support to other components of the IG such as admin investigations, whistleblower, hotline, etc. My role is the Resident Agent in Charge (RAC) of the Cyber Field Office, Eastern Resident Agency. So I supervise the cybercrime agents located in the eastern USA.

TH: Can you describe educational background?

SATH: Certainly. I have mix of postsecondary education and government/private industry training. Academically, I have a doctor of science degree in information assurance from Capitol College, a master of science degree in technology systems from East Carolina University, and a and a bachelor of science degree in mechanical engineering from Clarkson University.

TH: And, I would presume you have quite a bit of technical training.

SATH: I do. As part of my training with the Secret Service, I attended a 4-week class at the Federal Law Enforcement Training Center. The course was a mix of computer forensics, networking, and intrusion investigation and was put on by the Department of Treasury Enforcement Bureaus (Secret Service, IRS, ATF, and Customs). The forensic training was based on the FLETC Seized Computer Evidence Recovery Specialist (SCERS) training program, which some people may be familiar with.

TH: Impressive.

SATH: And, later, I attended the basic and advanced data recovery classes at the National White Collar Crime Center, Guidance Software's Encase training, and Access Data's FTK boot camp. And, finally, I have attended a network security and intrusion course at the National Security Agency and the Certified Ethical Hacker boot camp and certification.

TH: Walk us through an average day. What do you do?

SATH: Because I am supervisor, my day is pretty boring most of the time, at least when compared to my agents in the field. Typically I am on the phone, answering e-mail, and reading and approving reports all day. While I

stay engaged with all my agents' investigations, I am not actively conducting the investigations. Rather, I am providing guidance and assigning work to my agents. They, in turn, get to conduct the investigations through interviews, evidence collection, and forensic analysis.

TH: What is the most difficult case you've worked?

SATH: I was involved with the Mariposa/Butterfly botnet investigation. The FBI and foreign law enforcement were investigating the hackers who wrote and maintained the malware that operated the Mariposa botnet, and at the same time, I was actively investigating a hacker in the USA who was selling compromised computers (bots). It turned out my suspect was also operating a large Mariposa botnet, so we began to work together (the FBI and DCIS). It was difficult because during the course of the investigation I obtained control of the botnet from the suspect, and it consisted of over 50,000 compromised computers. Together we had to dismantle the botnet and also do our best to inform the owners of the victim computers.

TH: What is the most rewarding case?

SATH: There was a case where a hacker obtained access to numerous DoD and many other federal, state, and local government computers, and posted accounts and portions of SQL databases for sale. I was able to track the hacker back to an IP address in Kuwait, and working with Kuwaiti law enforcement, we were able to identify the hacker. The hacker was indicted for the crimes and is currently a fugitive. Although he hasn't been captured yet, the case was rewarding because the system worked as it should. Through MLAT requests and a good working relationship with foreign law enforcement, the hacker is now a known fugitive and published by Interpol for capture and extradition to the United States if he is identified while travelling internationally.

TH: What is the most important thing you think is needed to improve the law enforcement response to cybercrime?

SATH: The laws need to be updated to reflect the fast and ever-changing nature of cybercrime. By that I mean the laws related to obtaining account information, IP logs, and evidence from third parties. For example, if there is an intrusion at the DoD and the logs show the intrusion was from the IP address 1.2.3.4, we will determine who the IP address 1.2.3.4 is registered to and then obtain a subpoena for the account holder's information. The subpoena can take up to 30 days to receive the information. Once we receive the information, we then have to send an agent to interview whoever was assigned the IP address at the time of the intrusion. Usually the IP address was assigned to a home user from a large ISP, and she was a victim as well. The criminal hacked the home user's computer, then used her computer to hack the DoD. Now we have to analyze the computer to determine where the hacker came from when he hacked the home user's computer. This leads us to another IP address, and the cycle starts again. Smart criminals "hoop" through numerous computers on their way to the end target, knowing we (law enforcement) will have to try and trace the hoops back. The process can take many months waiting on subpoena responses, and often the IP address logs will be gone by the time we get there. So, requiring faster responses for subpoenas would definitely help.

TH: What else might help in the fight against cybercrime?

SATH: The prosecutors, both federal and state, need more resources to investigate cybercrime. There are only finite resources in every U.S. attorney's office and district attorney's office, so many cybercrimes do not get prosecuted. For example, intrusion attempts are rarely prosecuted. Only if the intrusion is successful is the crime investigated and prosecuted. This allows hackers to keep trying until they are successful. If the attempts were prosecuted, it could deter future hackers from trying. I liken the current situation to a criminal who takes a gun to the airport. Are you going to simply turn away a person who tries to take a gun through security at the airport or arrest him when he is caught trying? Obviously, you arrest him. Otherwise, he will keep coming back and trying to get the gun through security until he is successful. But with cybercrimes, we simply turn them away and let them try again another day. Eventually, they will be successful.

TH: In terms of international cases, what are some of the unique challenges that you have to deal with?

SATH: Take the challenge of a domestic case with subpoena response time and easily double or triple the time it takes to obtain records. With international cases, the U.S. government has to file a request under the Mutual Legal Assistance Treaty (MLAT) with the foreign government and request assistance to obtain the records, i.e., IP logs. The MLAT process is tedious, similar to obtaining a search warrant, and then you are dependent on the foreign government to obtain the records. Some will assist, but many will not, and even when they do provide assistance, it can take months to obtain a response. Criminals also know that certain countries will not cooperate with U.S. law enforcement, so they purposely try to hoop through a hacked computer in one of those countries. Then when we track the hacker back to that country, our investigation is effectively done.

TH: How can research improve the response to cybercrime?

SATH: Since much of cybercrime is now automated through the use of malware and botnets, research can significantly improve the ability of law enforcement and network defenders to respond to cybercrime. Furthermore, the anonymity of the Internet allows criminals to hide through the use of TOR, I2P, and payment systems such as bitcoin. Research into identifying criminals using these system would be very helpful to law enforcement.

TH: What would you tell students who want to enter this field in terms of necessary experience, training, education, expectations?

SATH: Historically most students obtained a degree in criminal justice to work in law enforcement, and that is still a good path to follow. However, I recommend students who wish to work in cybercrime to obtain a degree in CJ with a minor in computer science, or vice versa. It is much easier to teach a police recruit how to investigate and enforce laws than it is to teach a police recruit computer hardware, software, and networking. So if you already have experience and a background in computer science, information assurance, networking, or administration, you will have a leg up on those who do not. If you look at the FBI website, they are currently seeking

applicants with backgrounds and expertise in "IT network administrators, intrusions." Therefore, consider taking your electives or a few extra courses in computers and information technology. The more experience you have with computers and networking, coupled with a background in criminal justice, the easier it will be to obtain a career in cybercrime.

TH: Some people may not think of cybercrimes as having a physical demand on the responding officers/agents as do physical or real-world crimes. Do you think cybercrimes have more of an emotional or psychological impact, and if so, how?

SATH: The majority of cybercrimes and "real world" crimes are very similar and have the same effect on a responding officer/agent, with the exception of crimes that involved bodily injury or death. However, I see two types of cybercrimes that may have more of an emotional or psychological impact on the officers. The first and most obvious are the crimes against children that are often classified as cybercrime. The emotional impact on officers involved in these types of cases can be severe and overwhelming at times. As anyone can imagine, having to investigate any crime involving children is difficult, but when the crime involves sexual acts against defenseless children, the emotional and psychological impact is severe. The second classification of cybercrime that has a psychological impact is hacking cases. When investigating top-tier hackers, especially groups such as Anonymous, agents are always concerned about retaliation. The possibility of hackers targeting agents is real and includes identity theft, credit damage, and even public smear campaigns online.

TH: In your opinion, from an investigative standpoint, what is it that makes a cybercrime case different from a traditional crime that occurs outside the virtual world?

SATH: Well, cybercrime cases are similar to traditional, large white collar fraud cases in that both investigations involve lots of paper, i.e., subpoenas, search warrants, and the subsequent review and analysis of the records or computer logs and account information. But what makes them different is the fast nature of the Internet and the quick destruction of potential evidence in cybercrimes. While investigators are waiting for subpoena or search warrant returns, there is a good possibility the digital evidence in another location may be getting overwritten or unknowingly destroyed. So you are always in a rush to get the evidence before it is gone.

TH: How can criminological/criminal justice research help improve our knowledge of cybercriminal behavior?

SATH: It is difficult for investigators to stay on top of the latest communication practices of cybercriminals, so up-to-date research on how cybercriminals communicate is very helpful. As we have seen in recent years, the mode of communications for hackers changes quickly. ICQ, AIM/MSN, PMs on forums, IRC chat rooms, TOR forums, online gaming forums—there are so many possible locations to communicate from, and it is easy to hide in plain sight, such as communicating via gaming systems, that investigators may not be aware of the newest mode of communications. If we were able to see the patterns of how and when different types of hackers (hacktivists, carders) work together, this would also be helpful from an investigative standpoint.

Support Women's Rights Activists Around the World

The Everywoman, Everywhere Coalition is a global group that embraces the "belief in the right to a life free from all forms of violence for everywoman, everywhere." Last year, the Executive Board approved ACJS signing on in support of this position. The Coalition is now inviting individuals who have at least 10 years experience working in the area of violence against women to join in developing a global treaty on VAW. If you are interested in participating, please contact Maria Pachon at mariapachon@everywomaneverywhere.org.

Lorenzo Boyd Attends ANZSOC Conference on Behalf of ACJS

Lorenzo M. Boyd, 1st Vice President, ACJS

Greetings, ACJS colleagues! In continuing the work of past presidents, building and strengthening ties with affiliate organizations, I had the distinct honor of representing President Brandon Applegate and the Academy of Criminal Justice Sciences at the 28th Annual Australian and New Zealand Society of Criminology (ANZSOC) conference, November 25–27, 2015. The host institution for the conference was Flinders University Law School and the Centre for Crime Policy and Research. The ANZSOC conference was held in the beautiful and picturesque city of Adelaide, South Australia.

Founded in 1836, the city of Adelaide was named in honor of the wife of Britain's King William IV. This city has many majestic and palatial cathedrals and the "city of churches." With roughly 1.3 million residents, Adelaide is the capital city of the state of South Australia, is the fifth most populous city in Australia, and it boasts a Mediterranean climate.

The theme of the 2015 ANZSOC Conference was "*Security and rule of law: The changing face of criminal justice.*" This theme was very timely and included a wide range of interactive workshops, interesting plenary sessions, informative roundtables, presentations, and seminars, all geared toward enhancing and supporting this theme. There were several hundred presenters, speakers, and participants at this conference. They ranged from graduate students, practitioners, and educators to administrators and jurists.

The vast majority of the conference events were held at the 10+-story Flinders University School of Law building; however, the opening session of the conference was held across scenic Victoria Square at the historic Old Pilgrim Church. This Gothic-style cathedral, replete with stunning stained glass windows, interestingly sculpted columns, and an impressive pipe organ, was an awe-inspiring locale. The pre-conference reception was housed across the street in the iconic Sir Samuel Way Courthouse, which contains several court offices, including district and appellate courts, environmental court, the sheriff's office, and the Supreme Court of South Australia. Sir Samuel Way was a Supreme Court

Chief Justice and lieutenant governor of South Australia.

ANZSOC President Rick Sarre (professor of law, University of South Australia) was an amazingly hospitable and gracious host, introducing me to many of the conference attendees and constantly checking with participants and presenters to assure that things were progressing smoothly. Notable people on the program included the dean of the law school, a chief justice, the attorney general, deputy premier, assistant director of the state library, and a chief judge.

Lorenzo Boyd and ANZSOC President, Rick Sarre.

There were ample sub-thematic panels to choose from, but what stood out to me was the variety of presentations surrounding three primary themes: policing, restorative justice, and human rights/victims' issues. There were several presentations on sustainable justice and perceived justice. There were conversations and presentations about the indigenous populations and the efforts to preserve their rights in the criminal justice system.

One major issue that came up at the conference was the recent mass shootings in the U.S. and the associated proliferation of guns, especially compared to the lack of guns and thus lack of mass shootings in Australia. Several presenters pointed to the comparison, noting that the National Firearms Agreement in Australia basically prohibits automatic and semiautomatic assault rifles as well as pump-action shotguns. The agreement also tightened licensing rules, created a national gun registry, and established a 28-day waiting period for gun purchases. Australia then instituted a national buyback program (similar to ones used in American cities) that removed more than 20% of firearms from public circulation.

As noted by others at the conference, there has not been a mass shooting in Australia in nearly two decades, and the lack of available firearms is said to be an associated factor. In addition, the per capita rate of gun-related homicides and suicides in Australia has decreased significantly since 1996, the year in which gun ownership restrictions (National Firearms Agreement) went into effect. It is worth pointing out that

the land mass of Australia is slightly smaller than the contiguous U.S., and with almost 23 million residents, Australia has a population roughly equal to that of the state of Texas.

The annual conference dinner was held in the historic Mortlock Chambers at the State Library of South Australia. A spectacular building done in in the French Renaissance style, it was a memorable location to dine and mingle with the other conference attendees. I had a number of great conversations prior to and during the meal, with lots of discussion comparing U.S. criminal justice policies to those of Australia and New Zealand, with a particular focus on gun control, restorative justice, and incarceration practices. This conference dinner was both intellectually stimulating and quite filling.

The conference ended with an ice cream social, a fitting way to end any event! The social was co-sponsored by ACJS, featuring a local shop with excellent handmade ice cream and gelato. That was a big hit and provided more time to socialize with the attendees as we debriefed and further discussed the conference presentations.

All in all, the ANZSOC conference was an excellent display of the intriguing work and beguiling hospitality of our criminal justice colleagues from the lands down under. If you can swing it, I strongly encourage you to attend this meeting at least once in your career. The next conference, timed for late November 2016, will be held in the city of Hobart, on the Australian Island of Tasmania.

*__Lorenzo M. Boyd__ *is lecturer and Master's Program Coordinator at University of Massachusetts Lowell. He received his Ph.D. in sociology from Northeastern University. He is a former Deputy Sheriff in Suffolk County, Mass., and has served for several years as a police consultant. He also served as a Senior Researcher at the North Carolina Juvenile Justice Institute, where he conducted program evaluations on local community-based juvenile justice intervention programs. His doctoral research explored attitude differences between Black and White police officers regarding non-life threatening and quality of life issues, and he continues to have interests in that area. Dr. Boyd has also developed curricula for graduate and undergraduate programs, both online and on-campus. He is interested in exploring the effects of method of delivery and type of assessment on student outcomes. He has published articles in journals, such as, Race and Justice, Journal of Ethnicity in Criminal Justice, Criminal Justice Policy Review, and Criminal Justice Studies, among others.*

ACJS Today

Editor: **Robert M. Worley, Ph.D.**
Lamar University
Department of Sociology, Social Work, and Criminal Justice
P.O. Box 10026
Beaumont, Texas 77710
Phone: 409.880.7827
rworley@lamar.edu

Historian: Willard Oliver, Ph.D.
Sam Houston State University
College of Criminal Justice
P.O. Box 2296
Huntsville, TX 77341
Phone: 936.294.4173
woliver@shsu.edu

ACJS National Office

Mary K. Stohr: Executive Director
execdir@acjs.org

Mittie D. Southerland: Executive Director Emeritus
mittie.southerland@gmail.com

Cathy L. Barth: Association Manager
manager@acjs.org

Academy of Criminal Justice Sciences
P. O. Box 960
Greenbelt, Maryland 20770

Office Location:
7339 Hanover Parkway, Suite A
Greenbelt, MD 20768-0960
Tel.: (301) 446-6300; (800) 757-ACJS (2257)
Fax: (301) 446-2819
Website: http://www.acjs.org

ACJS Today Publication Dates

January
March
May
September
November

Submission Deadlines

December 15th
February 15th
April 15th
August 15th
October 15th

The editor will use his discretion to accept, reject or postpone manuscripts.

Article Guidelines

Articles may vary in writing style (i.e. tone) and length. Articles should be relevant to the field of criminal justice, criminology, law, sociology or related curriculum and interesting to our readership. Please include your name, affiliation and email address, which will be used as your biographical information. Submission of an article to *ACJS Today* implies that the article has not been published elsewhere nor is it currently under submission to another publication.
Photos: jpeg or gif
Text format: Microsoft Word, RTF, TXT, or ASCII
Citation Style: APA 5th Edition

ACJS 2015 – 2016 Executive Board

President
Brandon Applegate
University of South Carolina
Department of Criminology and Criminal Justice
1305 Greene Street
Columbia, SC 29208
803-777-7065
applegatep@sc.edu

First Vice President
Lorenzo Boyd
University of Massachusetts – Lowell
School of Criminology and Justice Studies
113 Wilder Street , HSSB Room 411
Lowell, MA 01854-3060
978-934-4160
lorenzo_boyd@uml.edu

Second Vice President
Nichole Leeper Piquero
University of Texas at Dallas
Program in Criminology
800 West Campbell Road
Richardson, TX 75080
972-883-2485
npiquero@utdallas..edu

Immediate Past President
Brian Payne
Old Dominion University
Graduate and Undergraduate Academic Programs
University 210E Koch Hall
Norfolk, VA 23529
757-683-4757
bpayne@odu..edu

Treasurer
L. Edward Day
Chapman University
One University Drive
Orange, CA 92866
714-997-6621
lday@chapman.edu

Secretary
Prabha Unnithan
Colorado State University
Department of Sociology
200 West Lake Street
Fort Collins, CO 80523
970-491-6615
prabha@lamar.colostate.edu

Trustees-at-Large
Bitna Kim
Indiana University of Pennsylvania
411 North Walk
Wilson Hall, Room 112
970-351-2107
bitna.kim@iup.edu

Barbara Sims
Mars Hill University
316 Cornwell
Mars Hill, NC 28754-0370
828-689-1276
bsims@mhu.edu

Heather L. Pfeifer
University of Baltimore
1420 North Charles Street
Baltimore, MD 21201
410-837-5292
hpfeifer@ubalt.edu

Regional Trustees

Region 1—Northeast
Denise Kindschi Gosselin
Western New England University
Herman 206A
1215 Wilbraham Road – BOX H5164
413-320-7576
denise.gosselin@wne.edu

Region 2—Southern
Dean Dabney
Georgia State University
140 Decatur Street
1201 Urban Life Building
Atlanta, GA 30303
404-413-1039
ddabney@gsu.edu

Region 3—Midwest
Joseph Schafer
Southern Illinois University Carbondale
4248 Faner Hall
Carbondale, IL 62901-4504
618-453-6376
jschafer@siu.edu

Region 4—Southwest
Camille Gibson
Prairie View A&M University
PO Box 519, MS 2600
Prairie View, TX 77446
936-261-5234
cbgibson@pvamu.edu

Region 5—Western/Pacific
Marlyn J. Jones
California State University, Sacramento
6000 J Street
Sacramento, CA 95819
916-278-7048
marlyn@csus.edu

Executive Director
Mary K. Stohr
Washington State University
Department of Criminal Justice and Criminology
P.O. Box 644872
Pullman, WA 99164
execdir@acjs.org

Executive Director Emeritus
Mittie D. Southerland
1525 State Route 2151
Melber, KY 42069
270-674-5697
270-674-6097 (fax)
mittie.southerland@gmail.com

Association Manager—Ex Officio
Cathy L. Barth
P.O. Box 960
Greenbelt, MD 20768-0960
301-446-6300
800-757-2257
301-446-2819 (fax)
manager@acjs.org

Academy of Criminal Justice Sciences
ACJS Today
P.O. Box 960
Greenbelt, Maryland 20768-0960