CrimRxiv

Connecting Evidence-Based Policing and Cybercrime

Jacek Koziarski¹, Jin Ree Lee²

¹University of Western Ontario, ²Michigan State University

Published on: Mar 02, 2020

DOI: 10.21428/cb6ab371.40515372

License: [Creative Commons Attribution 4.0 International License \(CC-BY 4.0\)](https://creativecommons.org/licenses/by/4.0/)

ABSTRACT

Article Classification: Conceptual Paper. **Purpose:** This paper explores the various challenges associated with policing cybercrime, arguing that a failure to improve law enforcement responses to cybercrime may negatively impact their institutional legitimacy as reliable first responders. Further, the paper makes preliminary links between cybercrime and the paradigm of evidence-based policing (EBP), providing suggestions on how the paradigm can assist, develop, and improve a myriad of factors associated with policing cybercrime. **Methodology/Approach:** Three examples of prominent cybercrime incidents will be explored under the lens of institutional theory: the cyberextortion of Amanda Todd; the hacking of Ashley Madison; and the 2013 Target data breach. **Findings:** EBP approaches to cybercrime can improve the effectiveness of existing and future approaches to cybercrime training, recruitment, as well as officers' preparedness and awareness of cybercrime. **Research Implications:** Future research will benefit from determining what types of training work at the local, state/provincial, and federal level, as well as evaluating both current and new cybercrime policing programs and strategies. **Practical Implications:** EBP approaches to cybercrime have the potential to improve police responses to cybercrime calls for service, save police resources, improve police-public relations during calls for service, and improve police legitimacy. **Originality/Value:** This paper links cybercrime policing to the paradigm of EBP, highlighting the need for evaluating and implementing effective evidence-based approaches to policing cybercrime.

Keywords: Cybercrime; Police Legitimacy; Policing, Evidence-Based Policing; Institutional Theory

Corresponding Author: Jacek Koziarski – jkoziars@uwo.ca

This is a pre-copyedited, author-produced version of an article accepted for publication in *Policing: An International Journal*, following peer review. The version of record, Koziarski, J. & Lee, J.R. (2020). Connecting Evidence-Based Policing and Cybercrime. *Policing: An International Journal*, is available online at: <https://doi.org/10.1108/PIJPSM-07-2019-0107>. When citing, please cite the version of record.

Introduction

According to the Netcraft Web Server Survey (2019), the Internet has over 1.3 billion websites across 237 million unique domain names. While only a fraction of these are active and publicly accessible, the Internet has reached over 3.5 billion people worldwide, or 47% of the world's population (United Nations Educational, Scientific and Cultural Organization, 2016). Though advancements in digital technology have allowed for increased global connectivity, its growth has also engendered opportunities for deviance and criminal activity (Hunton, 2010; Willits and Nowacki, 2016). In fact, cybercrimes have increased in both frequency and severity since the early 2000s¹, including online interpersonal violence (Bocij, 2004; Choi and Lee, 2017; Choi et al., 2017; Nobles et al., 2014; Reyns et al., 2012), child pornography (Clevenger et al., 2016; Holt et al., 2010; Jenkins, 2001; Krone, 2004), fraud (Cross, 2015; Wall, 2004), piracy (Burruss et al., 2013; Higgins and Marcum, 2011), and hacking offenses (Bossler and Burruss, 2011; Bossler and Holt, 2009; 2012; Holt et al., 2018; Jordan and Taylor, 1998).

Cybercrimes provide various complications for both domestic and international law enforcement due to its multi-jurisdictional and technical nature, often resulting in ineffective cybercrime responses and prevention strategies (Holt and Bossler, 2015; Holt and Lee, 2019; Holt et al., 2019; Lee et al., 2019; Willits and Nowacki, 2016). If law enforcement responses to cybercrime do not improve, their institutional legitimacy as effective first responders may be negatively affected (Willits and Nowacki, 2016; Holt and Lee, 2019). In fact, an assessment for the United Kingdom Home Office found that only 150 cybercrime incidents were reported to law enforcement for every 1 million occurrences, attributing low reporting to diminished public confidence in the police to resolve cybercrime inquiries (Wall, 2002).

An approach that could assist and improve cybercrime policing is the emerging paradigm of evidence-based policing (EBP). EBP is concerned with determining 'what works' within the context of policing through rigorous, clear, transparent, peer-reviewed, and replicated/reproduced scientific research (Sherman, 1998; 2013; 2015; UK College of Policing, n.d.). Extant policing scholarship has largely focused on updating and evaluating traditional approaches to policing, including developing new and more efficient ways of executing various police duties. In contrast, policing research exploring law enforcement responses to cybercrime has been scant (see Holt and Bossler, 2012; Holt et al., 2019; Lee et al., 2019 for exception), limiting the knowledge base around 'what works' in regard to cybercrime policing writ large.

The current paper proposes a link between cybercrime and the paradigm of EBP, providing suggestions on how the paradigm can assist, develop, and improve a myriad of factors associated with policing cybercrime. Further, the authors explore three prominent cybercrime cases through the lens of institutional theory to examine the various challenges associated with both domestic and international cybercrime policing, arguing that a failure to improve law enforcement responses to cybercrime may negatively impact their institutional legitimacy as reliable regulators of cybercrime. Research and practitioner implications for evidence-based cybercrime policing are discussed in detail.

Literature Review

Cybercrime

Cybercrime is generally defined as the use of the Internet or Internet-enabled devices to enact criminal and/or deviant behavior (Choi, 2015; Furnell, 2002; Wall, 2001). That is, cybercrime involves the use of virtual environments and networked computer systems for the commission of a crime (Holt, 2012; Wall, 2007). The ubiquity of the Internet has led to steady increases in the commission of cybercrimes overall (Marion, 2010). Between 2007 and 2012, the Federal Bureau of Investigation (FBI) reported a 40% increase in cybercrimes (Willits and Nowacki, 2016)¹, whereas the 2013 United Nations Office on Drugs and Crime (UNODC) survey suggested that individuals were more likely to become victims of cybercrime than traditional, physical crimes. Specifically, participants were upwards of five times more likely to experience hacking, deception, identity theft, and online credit card fraud, than burglary, robbery, and car theft (UNODC, 2013).

Law Enforcement Challenges

Cybercrimes pose unique challenges to both domestic and international law enforcement agencies. For one, cybercrimes have the ability to transcend spatial and temporal boundaries, widening the victim pool to include all individuals with access to the Internet (Choi, 2015; Holt and Bossler, 2016). This spatial and temporal transcendence makes it difficult to prosecute offenders, as they may reside in different countries from their victims (Holt and Bossler, 2016; Holt and Lee, 2019). Since different countries have their own set of laws and criminal procedures, apprehending offenders may prove difficult if the involved nations do not have extradition agreements in place (Brenner, 2011; Holt and Bossler, 2016; Holt and Lee, 2019).

The globalized nature of cybercrime has also created confusion both within and across law enforcement agencies as to who is responsible for responding to cybercrime calls for service (Bossler and Holt, 2012; Holt et al., 2019; Lee et al., 2019). Agencies who are at the crux of this confusion are local law enforcement agencies. These agencies struggle with addressing cybercrime because of their inability to acquire the necessary technology to conduct adequate police investigations, as well as insufficient training and difficulties retaining officers who possess the appropriate skills to combat cybercrime (Bossler and Holt, 2012; Holt and Lee, 2019; Holt et al., 2019; Lee et al., 2019). Additionally, some local law enforcement agencies place lower priority on cybercrimes unless they are related to child pornography or pedophilia, arguing that cybercrimes should be assigned to cybercrime-specific task forces (Bossler and Holt, 2012; Holt and Lee, 2019; Holt et al., 2019; Lee et al., 2019). In some cases, these issues are exacerbated by the lack of managerial support and public outcry for adequate cybercrime enforcement (Bossler and Holt, 2012).

Evidence-Based Policing

Adapted from evidence-based medicine, EBP is a paradigm introduced by Sherman (1998, p. 3) whereby, "...police officers and staff work together with academics and other partners to create, review, and use the best available evidence to inform and challenge policing policies, practices, and decisions" (UK College of Policing, n.d.). In other words, EBP is concerned with determining 'what works' within policing through rigorous, clear, transparent, peer-reviewed, and reproduced/replicated research (Sherman, 1998; 2013; 2015; UK College of Policing, n.d.). EBP encourages both police practitioners and researchers to utilize the 'triple-T' strategy in their approach—that is, the *targeting* of problems; *testing* of solutions through rigorous scientific methods; and *tracking* of solutions over time to ensure desired outcomes are achieved (Sherman, 2013).

Although the adoption of and receptivity towards EBP is mixed across various jurisdictions (Telep and Lum, 2014; Lumsden, 2017; Huey et al., 2017; Kalyal, 2019), the demand and growth of EBP has been substantial within the past two decades. This is evident through the development of programs and agencies such as the National Institute of Justice (NIJ) Law Enforcement Advancing Data and Science (LEADS) program and BetaGov (n.d.), enabling agencies and pracademics² to develop their own capacity to conduct evaluations (Cordner, 2018). Growth is also witnessed through the establishment of various international EBP societies (e.g., United Kingdom, United States, Canada, Australia/New Zealand, and Spain) who work to build relationships

(i.e., host conferences and share EBP-related knowledge) among those interested in the paradigm (Mitchell, 2019). Numerous tools have also been constructed to help translate knowledge (i.e., research findings) into easily consumable information for police practitioners, such as the Evidence-Based Policing Matrix (Lum et al., 2011), the UK College of Policing Crime Reduction Toolkit (n.d.), or Square One by the Canadian Society of Evidence-Based Policing (CAN-SEBP, n.d.).

To-date, several rigorous evidence bases have been established on widely used law enforcement approaches, strategies, and programs (Telep and Weisburd, 2012; Sherman 2013). The practice of hot spots policing, for instance, is understood as having the most rigorous evidence base in contrast to any other policing strategy, widely recognized as an approach that ‘works’ (National Research Council, 2004). In fact, several experimental and quasi-experimental studies found that having a short, random, intermittent police presence within crime hot spots can significantly lower crime and disorder both within and around the area (Braga, 2005; Braga, Papachristos, and Hureau, 2014; Braga, Welsh, and Schnell, 2015; Braga, Turchan, Papachristos, and Hureau, 2019; Koper, 1995; Telep, Mitchell, and Weisburd, 2014). However, numerous studies also found variation in effectiveness between different approaches to hot spots policing. For instance, while increasing police presence within a hot spot is effective, problem-oriented approaches have been found even more efficacious in certain situations (Braga, 2005; Braga et al., 2014; Braga et al., 2015; Braga et al., 2019). This is because such strategies possess wider degrees of flexibility that allow agencies to tailor their approach to specific problems that are known within the hot spot, targeting the origin of the issue(s) at hand (Goldstein, 1990; Braga, 2008)

EBP has also revealed various ineffective approaches in the process of identifying ‘what works’ within policing—Drug Abuse Resistance Education (D.A.R.E.) is one such example. D.A.R.E., a substance-abuse education program formed in the early 1980s by the Los Angeles Police Department and the Los Angeles School District, largely focused on informing students on drugs and the consequences of drug use (D.A.R.E., 2019). Numerous studies found the program to have little-to-no effect on lowering drug use (West and O’Neal, 2004; Rosenbaum, 2007), with some showing a backfire effect where the program was associated with increases in alcohol and cigarette use (Sloboda et al., 2009). The D.A.R.E. curriculum was subsequently renamed (*keepin’ it REAL*) and altered in the late 2000s, focusing instead on improving participants’ decision-making in interactive learning environments (DARE, 2019).

Despite the growth of EBP within the two decades since the paradigm was formed, many areas of policing (e.g., cybercrime policing) remain untested to the levels of hot spot policing or D.A.R.E. That is, while various studies have examined issues around cybercrime policing, training, and institutional legitimacy (see Bossler & Holt, 2012; Holt & Bossler, 2012; Holt, Burruss, and Bossler, 2015; Wall and Williams, 2013; Willits and Nowacki, 2016), these studies are few in quantity and lack the replication and reproduction of findings necessary to qualify for an evidence base. In other words, despite the rigor, transparency, and peer-reviewed nature of these studies, they are too few in number to determine what works in the context of cybercrime policing. The extant literature on cybercrime policing approaches are great starting point towards building an evidence base, but do not yet possess the replicability of results necessary to constitute a robust understanding of what works.

Another important distinction to note is that while the *approaches* (i.e., strategies, tactics, actions) taken to address cybercrime may differ from those used in traditional crime, the *application* of EBP (i.e., generating rigorous, clear, transparent, peer-reviewed, and reproduced/replicated research) is identical for both cybercrimes and traditional crimes. In other words, the application of EBP to cybercrime does not differ from its application to traditional crime simply because cybercrimes are different and/or non-traditional. The *approaches* generated to address cybercrime must not be confused with the *application* of the paradigm to cybercrime—the former acknowledges differences in offending characteristics and behavioral traits, whereas the latter requires the same standard of rigor to all phenomena under its scope.

Methodology and Theoretical Framework

A potential consequence associated with inadequate and ineffective cybercrime policing is the deterioration of police legitimacy (Holt and Lee, 2019). Crank and Langworthy (1992) suggest that police legitimacy is dependent on establishing structures and policies that are consistent with constituents' expectations. In this context, simply *appearing* to address cybercrime is an inadequate response to increasing institutional legitimacy (Willits and Nowacki, 2016). Instead, law enforcement must structure themselves in a manner that meets the accepted norms and standards of its constituents—namely, the effective criminalization and prosecution of cybercrime and its offenders (Crank, 2003; Willits and Nowacki, 2016). A deterioration of public trust in police and police legitimacy may result if inadequate policies and ineffective prosecution of cybercrimes are enforced (Willits and Nowacki, 2016). Stated differently, if law enforcement do not improve their responses to

cybercrime incidents, they risk damaging their institutional legitimacy as both reliable and effective first responders.

In order to illustrate the real-life complexities associated with cybercrime policing, three examples of prominent cybercrime incidents will be explored: (1) the cyberextortion of Amanda Todd; (2) the hacking of Ashley Madison, an adultery facilitating website; and (3) the 2013 Target data breach. Although these cases are not exhaustive or representative of how all police services approach, address, or prevent cybercrime, they were selected for their pervasive media attention, emotional charge, and wide net of victims. In particular, institutional theory—which posits that organizations/institutions must make alterations to their operations over time in order to create and maintain legitimacy (Meyer and Rowan, 1977)—will be used to suggest that police legitimacy may be damaged if inadequate changes are made to address the challenges associated with regulating cybercrime. EBP is subsequently introduced as a possible avenue through which law enforcement can both enhance their responses to cybercrimes, as well as create, strengthen, and maintain legitimacy.

Case Studies: Online Threats, Hacks, and Data Breaches

Amanda Todd

In 2010, 14-year-old Amanda Todd was captured revealing her breasts while broadcasting herself on a livestream (CBC, 2013; 2017). A year later, Amanda received a message from a man threatening that if she did not give him a “show,” the screenshot would be sent to all of her peers. Amanda refused, resulting in the circulation of these photos.

Amanda was bullied by her schoolmates which forced her to change schools (CBC, 2013; 2017). However, the individual who captured and disseminated the screenshot of Amanda continuously attempted to extort and blackmail her for more images and online sex shows (CBC, 2013; 2017). In September 2012, two years after the initial screenshot was captured, and one year after the screenshot was circulated, Amanda attempted to provide some clarity about her victimization (CBC, 2013). She did this by sharing a video of herself explaining the extortion and how she became a victim that resulted in anxiety, depression, and drug/alcohol use (CBC, 2013; 2017). A month later, Amanda committed suicide.

The police were significantly criticized by Amanda’s parents for not doing enough to help her (CBC, 2013; 2017). Amanda’s mother allegedly contacted the police

subsequent to every incident of extortion and blackmail Amanda experienced. Despite the many attempts, the police indicated that they could not do much to help her. In fact, an officer wrote to Amanda's mother in one email: "I would highly recommend that Amanda close all her Facebook and email accounts at this time. If Amanda does not stay off the Internet and/or take steps to protect herself online... there is only so much we as the police can do" (CBC, 2013). This recommendation was contrary to protocols employed by other police services in similar situations. Detective-Sergeant Frank Goldschmidt of the Ontario Provincial Police (OPP) Child Exploitation Unit (CEU) indicated that in cases such as Amanda's, the CEU would take over the victim's social media account(s) in an attempt to lure and/or identify the offender (CBC, 2013; 2017).

In January 2014, with the assistance of Facebook, the Dutch police were able to arrest the individual responsible for harassing, extorting, and blackmailing Amanda—Aydin Coban (CBC, 2017). Coban was charged with blackmail, co-perpetration of rape, attempted rape, and several charges related to child pornography for the online abuse of 35 young girls and five gay men (CBC, 2014; 2017). He was sentenced to 10 years and eight months in prison (Corder, 2017).

This case, although extreme in nature and resulting in the loss of life, reveals the limited ability of law enforcement in some circumstances to respond to cybercrime. This shortcoming, which may have been the result of limited resources and skills, led law enforcement to place the onus on the victim to prevent her own victimization. While instructing victims to deactivate their social media account(s) may be an adequate approach in certain circumstances, a simple shut down may not be an effective strategy across equally similar circumstances. A failure to demonstrate an adequate ability to respond to cybercrime calls for service may leave the public with a negative perception of police legitimacy in the context of cybercrime.

Ashley Madison

In July 2015, a hacker group known as "Impact Team" breached the customer data of Ashley Madison, an online dating platform where married individuals find others willing to have an affair (Baraniuk, 2015; Cox, 2015; Gilbert, 2015; Pearson, 2015). The breach resulted in personal information being stolen from 36 million accounts. Impact Team accused Ashley Madison customers of fraud, deceit, and stupidity for committing adultery. They gave Avid Life Media, the Canadian company who owns Ashley Madison, a 30-day ultimatum: either they took the website offline, or they would publicly post the information of all 36 million accounts. Avid Life Media did not

comply with the demands, resulting in the public dissemination of all 36 million accounts (Baraniuk, 2015; Cox, 2015; Gilbert, 2015; Pearson, 2015).

Following the data breach, Toronto Police confirmed that two individuals associated with the leaked information committed suicide (Baraniuk, 2015). Despite seeking assistance from domestic and international partners, the Toronto Police had limited success locating and apprehending the Impact Team hackers (Pearson, 2015). In particular, the Toronto Police sought assistance from ethical hackers (i.e., white-hat hackers), while Avid Life Media announced a reward of \$500,000 for anyone who can identify the hackers (Pearson, 2015).

Building upon the Amanda Todd case, the Ashley Madison incident—which also resulted in the loss of life—reveals the complexities inherent within policing cybercrime. Specifically, this example illustrates the sheer challenge of identifying individuals responsible for more complex, technical cybercrimes. Although law enforcement was aware of the group involved in this case, they struggled to identify the exact individuals associated with the incident. The decision to involve white-hat hackers and other members of the public suggests that both the attack and the skills needed to identify the individuals involved may be beyond law enforcement capabilities. While inviting the public to assist in investigations is not uncommon for the police, the lack of skills within the institution to effectively respond to technical cybercrimes may leave the public with a negatively impacted perception of both police competency and legitimacy.

Target Breach

In December 2013, discount retailer Target experienced one of the largest data breaches in history, affecting 110 million customers (CNN Money, 2013; Garcia, 2015; Hsu, 2014; Kirk, 2014; Sheridan, 2014). During the breach, malicious software was used to infect Target's debit and credit point-of-sale (POS) machines, instantly transferring customer information to a server in Russia (Kirk, 2014). The retail giant experienced significant financial settlements despite few reports of customers' information being fraudulently used after this incident (CNN Money, 2013; Garcia, 2015; Hsu, 2014; Kirk, 2014; Sheridan, 2014). To-date, no progress has been made with respect to apprehending those responsible for this breach.

Similar to the Ashley Madison incident, the Target breach highlights the challenges associated with identifying those responsible, especially international offenders. Even if law enforcement successfully identifies the involved individual(s), there is low

chance of prosecution without cooperation from the Russian government. While largely out of law enforcement control, the availability of spatial safe havens may impact police legitimacy as there is little that can be done to prosecute these individuals in the absence of extradition agreements.

Evidence-Based Policing and Cybercrime

Adopting an EBP approach to cybercrime can significantly improve law enforcement responses to cybercrime inquiries, providing evidence and clarity as to what programs and strategies work best in various situations. In particular, EBP will make law enforcement both more effective and efficient in their response to cybercrime calls for service, leading to a more intentional utilization of resources for an already-difficult crime to regulate. By understanding the precise elements involved in the commission of a crime, police are able to target their time and resources more effectively, resulting in better outcomes for both the institution and those directly involved (e.g., victims). If police agencies adopt empirically driven approaches to cybercrime, their utilization may be less scrutinized by those responsible for approving police budgets as well as members of the public. Implementing such approaches could also enable the police to have increased institutional legitimacy in the policing of cybercrime.

There are various avenues that research may want to explore to begin developing evidence bases. One approach is to evaluate already-implemented cybercrime programs and strategies. Approaches that appear promising would move on to further examinations to develop a robust evidence base, while those that fail to work would cease to be used. Relatedly, evidence could also confirm and identify challenges within existing approaches, leading to further inquiry on how to effectively address these complications.

EBP also assists in further demarcating effective programs and strategies by various contextual factors. One avenue of inquiry would be to determine what approaches are effective for different cybercrimes, as well as what procedural characteristics could be uniform across different offenses. This would allow law enforcement to be more effective across various cybercrimes while attaining some form of uniformity across approaches to simplify training and execution. This uniformity would depend on the evidence presented. If a uniform approach with slight-to-major differences between different cybercrimes makes any approach less effective, then the trade-off for simplicity may be unwarranted.

Another contextually-based example would be an approach that is deemed effective within the context of a large, urban police agency but not within a contrastingly small, rural police agency, a medium-sized agency, or agencies tasked with policing international cybercrime. This is likely the result of many factors, though differences in required resourcing and skill to effectively address cybercrime are chief among them. A further line of inquiry would be determining what approaches are most effective at different levels of policing, including specialized cybercrime units and the hyper-specializations found within them. Even if a lack of skill and resourcing lead smaller agencies to transfer their cybercrime responsibilities to larger counterparts, research related to the characteristics and obligations found within this process may reveal what is effective in various contexts and situations. The same research focus can be applied to private-public partnerships that may be deployed in policing cybercrime (see Leppänen, Kiravuo, and Kajantie, 2016).

EBP can also contribute to the creation and identification of new and effective approaches to policing cybercrime. This can be formed through identifying and addressing limitations within existing approaches. New approaches can also be developed within the context of emerging cyber threats that may require its own specific approach. By employing an EBP approach from the beginning of new developments, identifying ‘what works’ can be determined earlier on, ensuring law enforcement are approaching cybercrimes using the most effective method. Understanding what strategies and practices are effective and deploying these into practice will make law enforcement more proficient at responding to cybercrime incidents.

Training, Recruitment, Preparedness, & Awareness

Effective cybercrime training is paramount in ensuring that any police-led approach to cybercrime is properly executed. With certain jurisdictions experiencing more cybercrime than others, evidence determining most effective training approaches across these varying districts is needed. In smaller jurisdictions, training may include how to effectively and efficiently delegate cybercrime responsibilities to larger agencies; whereas in medium-to-large agencies that experience more cybercrime calls for service, determining what works may require a more nuanced approach, including training on how to select the most capable individuals, as well as how to effectively deliver and retain training content.

An EBP approach to cybercrime could also increase the prioritization of the behavior. Previous research has found that law enforcement agencies place lower priority on

cybercrimes due to its complexity and demanding resources (Holt and Bossler, 2012; Holt et al., 2019; Lee et al., 2019). If police are given training on how they can effectively contribute to the enforcement of cybercrime given their local jurisdictional circumstances, they may place cybercrimes at a higher priority. Another training-related element that would benefit from EBP is raising public awareness and knowledge of cybercrime. Public awareness campaigns are an important component in policing cybercrime as they inform the public on existing threats, while providing knowledge on how they can protect themselves online. Determining what works in this regard would be instrumental in the prevention of online victimization, resulting in the decreased need for police intervention (i.e., lowering the demand for law enforcement resources).

Knowledge regarding police perceptions of cybercrime would also benefit cybercrime policing efforts. Extant literature suggests law enforcement officers do not have positive perceptions of cybercrime, chief among them are the complexities and resourcing demands that are associated with responding to and investigating online crimes (Holt et al., 2019; Lee et al., 2019). Despite such perceptions, the current progression of technological innovation suggests that cybercrime will only become more common with time. It is quintessential for law enforcement to be effectively trained on what they have the capacity to do given their contextual circumstances, as it may have the capacity to improve officers' perceptions. For agencies that have limited resources allocated for cybercrime, this may include speaking to victims, taking reports, and passing along information to other agencies that have greater cybercrime resourcing.

Improving officers' coping mechanisms to job stressors are also imperative within the training context. Police practitioners who deal with certain cybercrimes may be exposed to large amounts of disturbing content (e.g., child pornography) that negatively impact their overall health and well-being. An EBP approach could identify effective methods pertaining to personal coping mechanisms, as well as determine effective strategies to improve officers' health and well-being within policing institutions (e.g., increasing access to counselling and increased leaves).

Law enforcement recruitment is another area in which EBP can be particularly fruitful. Given the hiring requirements for many police agencies, the difficulty in recruiting officers, and the age of more tenured personnel, questions may arise as to whether recruiting highly trained civilians to address more complex forms of cybercrime is more effective than providing advanced training to existing or new officers.

Evaluations could explore which cybercrimes and/or segments of an investigation are better suited for trained officers, which are better addressed by civilian specialists, and how his process of assignment could be conducted to enhance both effectiveness and efficiency. Such evaluations may reveal the benefit of confronting certain issues through recruitment over additional cybercrime training.

A potential response to this recruitment query could be to strengthen public and private sector partnerships so that there is greater involvement of the private sector in policing cybercrime (Holt & Lee, 2019). Given the private sector's ability to monitor online spaces, it is imperative for law enforcement agencies to build stronger relationships with private industry so that ongoing collaborations can be had (Holt & Lee, 2019). Strong public and private partnerships can provide the trust and security needed for private industries to support the goals of public sector agencies (Holt & Lee, 2019). In fact, if public sectors are able to gain access to the resources and techniques that private sectors have, efforts toward addressing cybercrime can be more effective and efficient for all involved parties (Holt & Lee, 2019).

Limitations of Evidence-Based Cybercrime Policing

While an EBP approach to cybercrime assists in determining what works, it should not be misinterpreted as a panacea that addresses *all* existing challenges in policing cybercrime. One particular challenge—and likely the reason why EBP has not made the transition to this area of policing yet—is the technological complexity associated with this form of crime. Many aspects of cybercrime policing can be complex, particularly programs and strategies utilized in both the investigation (e.g., digital forensic) and prevention of these crimes. That is, even if researchers interested in policing cybercrime employ rigorous research methodologies, they may not have the technical knowledge to understand how a particular strategy or approach is used in order to adequately evaluate it.

Relatedly, fostering strong collaborative relationships between researchers, police practitioners, and cybersecurity experts who possess the necessary skills to create and deploy effective strategies may be challenging given the various differences in individual and agency-level objectives. A main component of EBP are partnerships between researchers and police practitioners. In the context of evidence-based cybercrime policing, this may include fostering strong relationships between professionals who possess the necessary skills to ensure that all technical aspects of an approach are understood. The 'triangulation' of researchers, police practitioners, and

cybersecurity experts in the evaluation process has the potential to resolve various complexities inherent within cybercrime policing.

Another challenge that evidence-based cybercrime policing may not be able to address — which is particularly unique to online crimes—is the change and unpredictability of the behavior’s progression. In other words, an effective EBP approach to cybercrime today may not be effective tomorrow due to increasing technological sophistication and advancements in the characteristics of the behavior. This is where the EBP concept of *tracking* may become particularly important. By continuously tracking a program and/or strategy over time, one can document the point at which an effective strategy is no longer effective, signaling the need for readjustment.

Conclusion

It is crucial that scholars, police administrators, and policymakers determine the effectiveness of cybercrime strategies and identify key components that regulate these offenses without delegitimizing law enforcement. Despite its limitations, an EBP approach to cybercrime can inform current and future police policies, practices, and decisions. In particular, initiating an EBP approach to policing cybercrime will allow practitioners to assess both current and prospective cybercrime policing strategies, sparking important discussions on why a particular approach was established, what the objectives are, how the objectives are meant to be achieved, how the approach is currently being measured, and how success of the approach is currently being defined. By identifying best approaches and strategies that are grounded in empirically sound and replicated/reproduced evidence, practitioners involved in policing cybercrime are able to understand how best to utilize their time, effort, and resources to improve their performance and legitimacy as effective responders to cybercrime.

In addition, an EBP approach may reveal the need for increased funding in institutions across various levels of governance, as well as improvement in transnational bodies of enforcement. Given the challenges in forming comprehensive extralegal and transnational relationships, EBP may also reveal how to effectively regulate industry so that they are able to enforce behavior without adopting arrest powers. Relatedly, EBP approaches to cybercrime may generate an evidence base that suggests the need to invest in creative technical solutions. Given the numerous limitations in law enforcement responses to cybercrime, innovative solutions to cybercrime should be encouraged. Though complications are inevitable, an EBP approach to cybercrime will introduce a tailored focus to law enforcement solutions and strategies to online crime,

while simultaneously enhancing police and practitioner legitimacy in the regulation and prevention of cybercrime.

References

- Baraniuk, C. (2015), "*Ashley Madison: 'Suicides' Over Website Hack*", available at: <http://www.bbc.com/news/technology-34044506> (accessed 16 May 2019).
- BetaGov (n.d.), "*About*", available at: <http://www.betagov.org/html/about-betagov.html> (accessed 27 May 2019).
- Bocij, P. (2004), *Cyberstalking: Harassment in the Internet age and how to protect your family*, Praeger Publishers, Westport, CT.
- Bossler, A.M. and Burruss, G.W. (2011), "The general theory of crime and computer hacking: Low self-control hackers?", in *Cyber Crime: Concepts, Methodologies, Tools and Applications*, IGI Global, pp. 1499-1527.
- Bossler, A. M. and Holt, T. J. (2009), "On-line activities, guardianship, and malware infection: An examination of routine activities theory", *International Journal of Cyber Criminology*, Vol. 3, pp. 400-420.
- Bossler, A.M. and Holt, T. J. (2012), "Patrol officers' perceived role in responding to cybercrime", *Policing: An International Journal of Police Strategies & Management*, Vol. 35 No. 1, pp. 165-181.
- Braga, A. A. (2005), "Hot Spots Policing and Crime Prevention: A Systematic Review of Randomized Controlled Trials", *Journal of Experimental Criminology*, Vol. 1 No.3, pp. 317-342.
- Braga, A.A. (2008), *Problem-oriented policing and crime prevention* (2nd ed.), Criminal Justice Press, Monsey, NY.
- Braga, A. A., Papachristos, A. V., and Hureau, D. M. (2014), "The Effects of Hot Spots Policing on Crime: An Updated Systematic Review and Meta-Analysis", *Justice Quarterly*, Vol. 31 No. 4, pp. 633-663.
- Braga, A. A., Turchan, B. S., Papachristos, A. V., and Hureau, D. M. (2019), "Hot Spots Policing and Crime Reduction: An Update of an Ongoing Systematic Review and Meta-Analysis", *Journal of Experimental Criminology*.

Braga, A. A., Welsh, B. C., and Schnell, C. (2015), "Can Policing Disorder Reduce Crime? A Systematic Review and Meta-Analysis", *Journal of Research in Crime and Delinquency*, Vol. 52 No. 4, pp. 567-588.

Burruss, G.W., Bossler, A.M. and Holt, T.J. (2013), "Assessing the mediation of a fuller social learning model on low self-control's influence on software piracy", *Crime & Delinquency*, Vol. 59 No. 8, pp. 1157-1184.

Canadian Society of Evidence-Based Policing (n.d.), "Square One", available at: <https://www.can-sebp.net/squareone> (accessed 27 May 2019).

CBC. (2013), "Amanda Todd Suicide: RCMP Repeatedly Told of Blackmailer's Attempts", available at: <http://www.cbc.ca/news/canada/amanda-todd-suicide-rcmp-repeatedly-told-of-blackmailer-s-attempts-1.2427097> (accessed 16 May 2019).

CBC. (2013), "The Sextortion of Amanda Todd", available at: <http://www.cbc.ca/fifth/episodes/2013-2014/the-sextortion-of-amanda-todd> (accessed 16 May 2019).

CBC. (2014), "Dutch Man Suspected of Tormenting Amanda Todd had 75 Other Victims, Facebook Report Says", available at: <http://www.cbc.ca/news/canada/dutch-man-suspected-of-tormenting-amanda-todd-had-75-other-victims-facebook-report-says-1.2857281> (accessed 16 May 2019).

CBC. (2017), "Dutch Man Charged in Amanda Todd Case Allegedly Targeted 2nd Canadian Child", available at: <http://www.cbc.ca/news/canada/british-columbia/amanda-todd-aydin-coban-1.3951334> (accessed 16 May 2019).

Choi, K.S. (2015), *Cybercriminology and digital investigation*, LFB Scholarly Publishing.

Choi, K.S. and Lee, J.R. (2017), "Theoretical analysis of cyber-interpersonal violence victimization and offending using cyber-routine activities theory", *Computers in Human Behavior*, Vol. 73, pp. 394-402.

Choi, K.S., Lee, S.S. and Lee, J.R. (2017), "Mobile phone technology and online sexual harassment among juveniles in South Korea: Effects of self-control and social learning", *International Journal of Cyber Criminology*, Vol. 11 No. 1, pp. 110-127.

Clevenger, S.L., Navarro, J.N. and Jasinski, J.L. (2016), "A matter of low self-control? Exploring differences between child pornography possessors and child pornography

producers/distributors using self-control theory", *Sexual Abuse*, Vol. 28 No. 6, pp.555-571.

CNN Money. (2013), "*Target: 40 Million Credit Cards Compromised*", available at: <http://money.cnn.com/2013/12/18/news/companies/target-credit-card/> (accessed 16 May 2019).

Cordner, G. (2019), "A practical approach to evidence based policing", in Mitchell, R.J. & Huey, L. (Eds.), *Evidence Based Policing: An Introduction*, Policy Press, Bristol, UK, pp. 231-242.

Corder, M. (2017), "*Amanda Todd's Accused Cyberbully Facing 11 Years in Dutch Prison*", available at: <https://globalnews.ca/news/3240975/amanda-todd-cyberbullying-aydin-coban/> (accessed 16 May 2019).

Cox, J. (2015), "*Ashley Madison Hackers Speak Out: 'Nobody Was Watching'*", available at: https://motherboard.vice.com/en_us/article/ashley-madison-hackers-speak-out-nobody-was-watching (accessed 16 May 2019).

Crank, J. P. (2003), "Institutional theory of police: A review of the state of the art", *Policing: An International Journal of Police Strategies & Management*, Vol. 26 No. 2, pp. 186-207.

Crank, J. P. and Langworthy, R. (1992), "An institutional perspective of policing", *The Journal of Criminal Law and Criminology*, Vol. 83 No. 2, pp. 338-363.

Cross, C. (2015), "No laughing matter: Blaming the victim of online fraud", *International Review of Victimology*, Vol. 21 No. 2, pp. 187-204.

D.A.R.E. (2019), "*The History of D.A.R.E.*", available at: <https://dare.org/history/> (accessed 28 August 2019).

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

Garcia, A. (2015), "*Target Settles for \$39 Million Over Data Breach*", available at: <http://money.cnn.com/2015/12/02/news/companies/target-data-breach-settlement/> (accessed 16 May 2019).

Gilbert, D. (2015), "*Ashley Madison hack: Who are Impact Team, and why did they leak website data and will they be caught?*", available at: <http://www.ibtimes.co.uk/ashley->

[madison-hack-who-are-impact-team-why-did-they-leak-website-data-will-they-be-caught-1516328](#) (accessed 16 May 2019).

Goldstein, H. (1990), *Problem-oriented policing*, Temple University Press, Philadelphia, PA.

Higgins, G. E. and Marcum, C. D. (2011), *Digital Piracy: An Integrated Theoretical Approach*, Carolina Academic Press, Raleigh, NC.

Holt, T. J. (2012), "Exploring the intersections of technology, crime, and terror", *Terrorism and Political Violence*, Vol. 24, pp. 337-354.

Holt, T. J., Blevins, K. R. and Burkert, N. (2010), "Considering the pedophile subculture online. *Sexual Abuse*", Vol. 22 No. 1, pp. 3-24.

Holt, T. J. and Bossler, A. M. (2012), "Predictors of patrol officer interest in cybercrime training and investigation in selected United States police departments", *Cyberpsychology, Behavior, and Social Networking*, Vol. 15 No. 9, pp. 464-472.

Holt, T. J. and Bossler, A. M. (2015), *Cybercrime in progress: Theory and prevention of technology-enabled offenses*, Routledge.

Holt, T. J., Burruss, G. W. and Bossler, A. M. (2018), "An examination of English and Welsh constables' perceptions of the seriousness and frequency of online incidents", *Policing and Society*, pp. 1-16.

Holt, T.J. and Lee, J.R. (2019), "Policing Cybercrime through Law Enforcement and Industry Mechanisms", in *The Oxford Handbook of Cyberpsychology*.

Holt, T.J., Lee, J.R., Liggett, R., Holt, K.M. and Bossler, A. (2019), "Examining perceptions of online harassment among constables in England and Wales", *International Journal of Cybersecurity Intelligence & Cybercrime*, Vol. 2 No. 1, pp. 24-39.

Hsu, T. (2014), "2 Arrested in Connection with Target Hack", available at: <http://www.latimes.com/business/la-fi-target-arrests-20140121-story.html> (accessed 16 May 2019).

Huey, L. and Mitchell, R. J. (2016), "Unearthing hidden keys: Why academics are an invaluable (if underutilized) resource in policing research", *Policing*, Vol. 10 No. 3, pp. 300-307.

Huey, L., Blaskovits, B., Bennell, C., Kalyal, H. J. and Walker, T. (2017), "To what extent do Canadian police professionals believe that their agencies are 'Targeting, Testing, and Tracking' new policing strategies and programs?", *Police Practice and Research*, Vol. 18 No. 6, pp. 544-555

Hunton, P. (2010), "Cybercrime and security: A new model of law enforcement investigation", *Policing*, Vol. 4 No. 4, pp. 385-394.

Jenkins, P. (2001), *Beyond tolerance: Child pornography on the Internet*, New York University Press, New York: NY.

Jordan, T. and Taylor, P. (1998), "A sociology of hackers", *The Sociological Review*, Vol. 46 No. 4, pp.757-780.

Kalyal, H. (2019), "'One Person's Evidence Is Another Person's Nonsense': Why Police Organizations Resist Evidence-Based Practices", *Policing: A Journal of Policy and Practice*, pp. 1-15.

Kirk, J. (2014), "Target Credit Card Data Was Sent to Server in Russia", available at: <http://www.pcworld.com/article/2088920/target-credit-card-data-was-sent-to-server-in-russia.html> (accessed 16 May 2019).

Krone, T. (2004), "A typology and online child pornography offending", *Trends & Issues in crime and criminal justice*, Vol. 279, pp. 2-6.

Lee, J.R., Holt, T.J., Burruss, G.W. and Bossler, A.M. (2019), "Examining English and Welsh Detectives' Views of Online Crime", *International Criminal Justice Review*, pp. 1-20.

Leppänen, A., Kiravuo, T. and Kajantie, S. (2016), "Policing the cyber-physical space", *The Police Journal: Theory, Practice, and Principles*, Vol. 89 No. 4, pp. 290-310.

Lum, C., Koper, C. S. and Telep, C. W. (2010), "The Evidence-Based Policing Matrix", *Journal of Experimental Criminology*, Vol. 7 No. 1, pp. 3-26.

Lumsden, K. (2017), "Police officer and civilian staff receptivity to research and evidence-based policing in the UK: Providing a contextual understanding through qualitative interviews", *Policing*, Vol. 11 No. 2, pp. 157-167.

Marion, N. E. (2010), "The Council of Europe's Cybercrime Treaty: An exercise in symbolic legislation", *International Journal of Cyber Criminology*, Vol. 4 No. 1-2, pp.

699-712.

Meyer, J. W. and Rowan, B. (1977), "Institutionalized organizations: Formal structure as myth and ceremony", *American Journal of Sociology*, Vol. 83 No. 2, pp. 340-363.

Mitchell, R.J. (2019), "A light introduction to evidence based policing", in Mitchell, R.J. & Huey, L. (Eds.), *Evidence Based Policing: An Introduction*, Policy Press, Bristol, UK, pp. 3-14.

National Research Council (2004), "Fairness and Effectiveness in Policing: The Evidence", available at: <https://www.nap.edu/read/10419/chapter/1> (accessed 25 May 2019).

Netcraft Web Server Survey. (2019), "June 2019 Web Server Survey", available at: <https://news.netcraft.com/archives/category/web-server-survey/> (accessed 13 June 2019).

Nobles, M.R., Reyns, B.W., Fox, K.A. and Fisher, B.S. (2014), "Protection against pursuit: A conceptual and empirical comparison of cyberstalking and stalking victimization among a national sample", *Justice Quarterly*, Vol. 31 No. 6, pp. 986-1014.

Panda, A. (2014), "Bringing academic and corporate worlds closer: We need pracademics", *Management and Labour Studies*, Vol. 39 No. 2, pp. 140-159.

Pearson, J. (2015), "Cops Investigating Ashley Madison Breach: We Need 'White Hat Hackers' to Help", available at: https://motherboard.vice.com/en_us/article/cops-investigating-ashley-madison-breach-we-need-white-hat-hackers-to-help (accessed 16 May 2019).

Reyns, B.W., Henson, B. and Fisher, B.S. (2012), "Stalking in the twilight zone: Extent of cyberstalking victimization and offending among college students", *Deviant Behavior*, Vol. 33 No. 1, pp.1-25.

Rosenbaum, D.P. (2007), "Just say no to D.A.R.E.", *Criminology & Public Policy*, Vol. 6, pp. 815-824.

Sherman, L.W. (1998), "Evidence based policing: Ideas in American Policing", available at: <https://www.policefoundation.org/publication/evidence-based-policing/> (accessed 25 May 2019).

Sherman, L.W. (2013), "The Rise of Evidence-Based Policing : Targeting , Testing , and Tracking", *Crime and Justice*, Vol. 42 No. 1, pp. 377-451.

Sherman, L.W. (2015), "A Tipping Point for "Totally Evidenced Policing": Ten Ideas for Building an Evidence-Based Police Agency", *International Criminal Justice Review*, Vol. 25 No. 1, pp. 11-29.

Sheridan, P. M. (2014), "*Target Breach: How Things Stand*", available at: <http://money.cnn.com/2014/05/05/news/companies/target-breach/> (accessed 16 May 2019).

Sloboda, Z., Stephens, R. C., Stephens, P. C., Grey, S. F., Teasdale, B., Hawthorne, R. D., Williams, J., and Marquette, J. F. (2009), "The Adolescent Substance Abuse Prevention Study: A randomized field trial of a universal substance abuse prevention program", *Drug and Alcohol Dependence*, Vol. 102, pp. 1-10.

Telep, C. and Weisburd, D. (2012), "What is known about the effectiveness of police practices in reducing crime and disorder?", *Police Quarterly*, Vol. 15 No. 4, pp. 331-357.

Telep, C. W. and Lum, C. (2014), "The Receptivity of Officers to Empirical Research and Evidence-Based Policing: An Examination of Survey Data From Three Agencies", *Police Quarterly*, Vol. 17 No. 4, pp. 359-385.

Telep, C. W., Mitchell, R. J., and Weisburd, D. (2014), "How Much Time Should the Police Spend at Crime Hot Spots? Answers from a Police Agency Directed Randomized Field Trial in Sacramento, California", *Justice Quarterly*, Vol. 31 No. 1, pp. 165-193.

UK College of Policing (n.d.), "Crime Reduction Toolkit", available at: <https://whatworks.college.police.uk/toolkit/Pages/Toolkit.aspx> (accessed 27 May 2019).

UK College of Policing (n.d.), "*What is evidence-based policing?*", available at: <https://whatworks.college.police.uk/About/Pages/What-is-EBP.aspx> (accessed 27 May 2019).

United Nations Educational, Scientific and Cultural Organization. (2016), "*The State of Broadband: Broadband catalyzing sustainable development*", available at: https://www.itu.int/dms_pub/itu-s/opb/pol/S-POL-BROADBAND.19-2018-PDF-E.pdf (accessed 28 May 2019).

United Nations Office on Drugs and Crime. (2013), "*Comprehensive study on cybercrime*", available at: <https://www.unodc.org/documents/organized->

crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf (accessed 28 May 2019).

Wall, D. S. (2001), "Cybercrimes and the Internet", in D. S. Wall (Ed.), *Crime and the Internet*, Routledge, New York, NY, pp. 1-17.

Wall, D. S. (2002). *"DOT.CON: Internet Related Frauds and Deceptions Upon Individuals within the UK"*, Final Report to the Home Office.

Wall, D. (2004), "Digital realism and the governance of spam as cybercrime", *European Journal of Criminal Policy and Research*, Vol. 10, pp. 309-335.

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*, Polity, Cambridge, UK.

West, S.L., and O'Neal, K.K. (2004), "Project D.A.R.E. outcome effectiveness revisited", *American Journal of Public Health*, Vol. 94 No. 6, pp. 1027-1029.

Willits, D. and Nowacki, J. (2016), "The use of specialized cybercrime policing units: An organization analysis", *Criminal Justice Studies*, Vol. 29 No. 2, pp. 105-124.

Footnotes

1. Extant cybercrime research has found that both increased access and more frequent use of technology has contributed to the proliferation of cybercrime—both offending and victimization (see Holt, Bossler, & Seigfried-Spellar, 2018 for review). While it is uncertain what proportion of the increase in cybercrimes is attributed to the heightened use of the Internet and how much is an actual increase beyond usage rates, extant criminological literature supports the argument that greater and easier access to technology, coupled with higher usage rates, increases cybercrime offending and individuals' likelihood of experiencing cybercrime victimization (see Holt & Bossler, 2015). [↵](#)

2. "... any individual who is dually recognized as expert in both academia and within a community of practice" (Huey & Mitchell, 2016, p. 301; Panda, 2014). [↵](#)