Volume 3 Issue 1 June 2021

International Journal of Criminal Justice

KIC Korean Institute of Criminology

JOURNAL DESCRIPTION

The primary research areas of the journal are change of human behaviors, community response, and social system in the field of criminal law, criminology, criminal justice and psychology. We welcome research contributions that achieve: (a) improving knowledge and understanding of the etiology and trends of crime (b) utilizing theoretical frameworks and research methodologies in evaluation of criminal legislations and policies in different jurisdictions and (c) undertaking analysis and research on enacting and amending the criminal codes and legislations in response to changing or evolving crime trends with an eye towards improving the effectiveness of the judicial system and criminal policies.

International Journal of Criminal Justice

Contents

Invitation Article

New Directions in Online Illicit Market Research

*Thomas J. Holt, Ph.D.**
Professor
School of Criminal Justice
Michigan State University

Abstract

Criminological scholarship has long examined the ways that illicit goods and services are traded through underground economies, such as narcotics and stolen goods. In the last two decades, researchers have explored the ways that online spaces, such as forums, are used by actors to engage in the sale of digital goods, including stolen personal information and malicious software. Additionally, research has begun to explore the ways that a global network for the sale of drugs has emerged in online markets operating on the so-called Dark Web. Though these studies improve our understanding of the basic social structures that drive online transactions for various criminal services, myriad questions remain as to what drives engagement in online markets and the ways that they persist and evolve over time. This work provides an overview of the various illicit markets operating on the Open and Dark Web, and their relationship to open and closed economically-motivated illicit goods and services markets in the real world. This work also explores the range of research questions that must be addressed to improve our understanding of the actors who shape the processes of online markets, inclusive of buyers, sellers, and website operators.

Keywords

Illicit Markets, Economic Crime, Cybercrime, Cryptomarkets, Dark Web, Drugs, Hacking, Rational Choice

---

* This article is based on Professor Holt's keynote lecture delivered to the International Forum of the Korean Institute of Criminology, Seoul, Korea, on December 3rd, 2020.
* http://dx.doi.org/10.36889/IJCJ.2021.005.
* Direct correspondence to Thomas J. Holt, Ph.D., Professor, School of Criminal Justice, Michigan State University; e-mail: holtt@msu.edu.
INTERNATIONAL JOURNAL OF CRIMINAL JUSTICE, Vol. 3 Issue 1, June 2021, 3-23

NEW DIRECTIONS IN ONLINE ILLICIT MARKET RESEARCH

Criminological scholarship has historically focused on the distribution of a variety of illicit goods and services, ranging from prostitution (e.g. Cunningham & Shah, 2016), drugs (Adler, 1993; Jacobs, 1996; Sterk, 1999; Turnbull, 2002), and weapons (Cook, Cukier, & Krause, 2009; Hureau & Braga, 2018), to more exotic items such as endangered wildlife (Lavorgna, 2014; Sollund, 2019). These studies provided rich insights into not only the practices of buyers, sellers, and market facilitators (Adler, 1993; Jacobs, 1996; Wright & Decker, 1994; 1996), but also into the social and economic factors that influence involvement in illicit exchanges (Cunningham & Shah, 2016; Jacobs, 2000). Scholars have also examined the efficacy of law enforcement efforts to dismantle illicit economies (Eck, 1995; May & Hough, 2004), and the ways that offender behaviors evolve to reduce the risk of arrest (Cross 2000; Jacobs 1996; 2010; Johnson et al. 2000; Johnson & Nataranjan 1995; Knowles 1999; Topalli et al. 2002; VanNostrand & Tewksbury 1999).

In recent years, offenders have seized upon the opportunities afforded by the Internet and mobile devices to expand the scope of illicit market operations (Holt & Bossler, 2015; Mann & Sutton, 1998). The communications, finance, and retail tools available through the World Wide Web and social media application made it possible for illicit markets that traditionally existed in physical spaces to move their operations into virtual spaces (Barratt, 2012; Franklin et al., 2007; Holt et al., 2016; Martin, 2014). In fact, there are now services selling access to sex (Cunningham & Kendall, 2010; Weitzer, 2012), narcotics (Barratt, 2012; Martin, 2014; Moeller et al., 2017; Tzanetakis et al., 2017), counterfeit documents (Holt & Lee, 2020), and even hitmen and contract violence providers (Roddy & Holt, 2020). These activities may be viewed by some as cybercrimes by virtue of the use of technology in the offense, though they may be defined more as cyber-enabled crimes as they can be performed without technology, but are made easier through this medium (Dowling & McGuire, 2013; Holt & Bossler, 2016).

There are also forms of cybercrime that may be referred to as cyber-dependent crimes, like computer hacking, as they cannot be performed without the use of computers and the Internet (Dowling & McGuire, 2013; Holt & Bossler, 2016). Individuals involved in these offenses have created underground economies where

malware, attack services, and access to sensitive data are available on a fee-for-service basis (Dupont et al., 2017; Franklin et al., 2007; Holt, 2012; Holt, 2013; Hutchings & Holt, 2015). Online markets selling email lists for spam campaigns, global distribution of malicious software, and access to stolen credit card numbers emerged in the early 2000s and have evolved in tandem with the applications and services on the Internet (Dupont et al., 2017; Holt & Dupont, 2019; Hutchings & Clayton, 2016; Smirnova & Holt, 2017).

Research exploring the online markets for physical and digital goods has increased dramatically over the last decade, examining aspects of market operations and the utility of some theories to account for these offenses (Holt & Bossler, 2015; Hutchings & Holt, 2017). Though valuable, there is a need for a systematic review of the literature related to online illicit markets to identify gaps in the literature that must be addressed. Such work is essential to improve our fundamental understanding of the participants of markets, whether as vendors, buyers, or facilitators, as well as their technical and social structure. This work will provide an analysis of the state of virtual market research and its operations on both the Open and Dark Web based on the existing body of empirical research. A series of recommendations are provided for future research in the hopes of improving the capacities of policy makers and practitioners in cybersecurity and law enforcement around the world.

DIFFERENTIATING PHYSICAL AND VIRTUAL MARKETS

Criminological and sociological inquiry into the nature of illicit goods markets has been particularly useful to understand the structural distribution models at play for different products and services (Adler, 1993; Jacobs, 1996; Klockars, 1974; Potter, 2009). The dynamics that shape the practices of markets are due in part to the visibility that their illicit exchanges may have to the general public. The most often examined illicit markets are those which occur in relatively public settings, whether in street corners, alleys, or the front porches of homes and apartment buildings as with drug sales (Jacobs 1996; 2000; Johnson, Dunlap, & Torginy 2000; Johnson & Nataranjan 1995; Knowles 1999; Topalli, Wright, & Fornango 2002; VanNostrand & Tewksbury 1999; Weitzer, 2012). Such exchanges are

typically referred to as open markets by virtue of the public visibility of the activities (Eck, 1995; May & Hough, 2004). Involvement in transactions in open markets creates risk for both buyers and sellers, as both parties can be observed by police and other informal agents of social control, such as neighbors or community watch groups (Jacobs, 2010; May & Hough, 2004). In addition, the presence of drugs, weapons, and cash creates a point of risk for market participants from other criminals who would target them for robbery or theft (Gibbs, 1997; Jacobs, 1996, 2010).

Due to the range of risks present in open illicit markets, a portion of actors shifted their practices to reduce the risk of detection (e.g. Gibbs, 1996; May & Hough, 2004). Specifically, sellers began to engage in transactions with only those individuals who they knew or trusted in some way (Johnson et al., 2000; May & Hough, 2004). They also began to operate in low visibility environments, such as in residences or other controlled and enclosed spaces (Hammid, 1998; Johnson et al., 2000; May & Hough, 2004). Some also continued to operate in public spaces, though they dramatically reduced their visibility and vending practices. Such markets came to be known as closed markets due to their restrictions and limited access to outsiders (May & Hough, 2004).

The organization and practices of actors involved in physical illicit markets are replicated to some degree in virtual spaces. Many of the advertisements for illicit products in online spaces operate in a quasi-open state in that they can be identified with relatively little difficulty through search engines or other publicly accessible means (Franklin et al., 2007; Holt & Lampke, 2010; Holt & Lee, 2020; Tzanetsakis et al., 2016; Yip et al., 2013). Additionally, the public statements made by vendors regarding their products and services are similar to open air illicit markets in that they are hawking their wares to any interested parties (Holt & Dupont, 2019; Odabas et al., 2017).

There are minor differences in the operating environments where buyers and sellers congregate online. First, illicit products can be identified for sale via online platforms that can be accessed using a traditional web browser, search engine, and appropriate key terms (Holt & Lampke, 2010; Hutchings & Holt, 2015; Odabas et al., 2017; Yip et al., 2013). This environment is often referred to as the Open Web, in that anyone can access website content through the use of any browser software, and this information may be indexed and retained by search engines and

historical web archives (Smirnova & Holt, 2017).

Various illegal products and services are also readily available on the so-called Dark Web, which is an encrypted portion of the Web that can only be accessed through the use of specialized browser software (Barratt, 2012; Decary-Hetu et al., 2016; Martin, 2014; Smirnova & Holt, 2017). There are various tools that can be used to access the Dark Web, though the most prominent software is called TOR, or The Onion Router, which is a free software program incorporating encryption software with a Firefox browser plugin (Martin, 2014). TOR functions by routing user web traffic through other TOR users' internet connections at multiple points to effectively hide the IP address and information of all within the network (Barratt, 2012). Websites hosted on servers connected to TOR utilize similar processes which makes it exceedingly difficult to identify the physical location of websites to shut down their operations (Decary-Hetu et al., 2016).

Regardless of platform, there are two primary modes of selling products. The first involves the use of single-operator e-commerce style platforms to facilitate transactions. These sites are typically referred to as "shops" as they provide access to various goods and services sold by one individual (Copeland et al., 2020; Holt & Lee, 2020; Smirnova & Holt, 2017). Customers can identify shops through various search engines or links posted on dark web indexes, though they may have to register with the site in order to complete a purchase or see their exact products for sale (Copeland et al., 2020; Holt & Lee, 2020; Smirnova & Holt, 2017). Registration systems vary based on the vendor, but typically require an individual to provide a username and password in order to create an account that can give them access to site content (Holt & Lampke, 2010; Smirnova & Holt, 2017).

The second model involves the use of forum software, which provides an asynchronous communications platform hosted on the websites designed to connect participants from around the world (Dupont et al., 2017; Holt, 2007; Hutchings & Holt, 2015; Mann & Sutton, 1998). Forums comprise an online discussion group with a specific topic focus, segmented by sub-topic (Holt, 2007; Holt & Bossler, 2015; Mann & Sutton, 1998). Conversations begin when an individual makes a post about a specific issue, which in the context of illicit markets involves the products or services they have for sale, or may be seeking. Responses to that

post are threaded together sequentially to provide an ongoing dialogue (Holt, 2007; Holt & Lampke, 2010; Mann & Sutton, 1998).

Forums used to sell illegal good and services have been observed since the early 2000s, and can operate in a similar fashion to a retail mall in physical space (Dupont et al., 2017; Holt & Lampke, 2010; Odabas et al., 2017). The site operators provide a communications space via the forums, and vendors can post ads directly next to their competitors. Customers can then review all advertisements and ask questions about the products, before selecting a vendor with whom to engage in a transaction (Odabas et al., 2017). The actual exchange takes place outside of the forum, though customers can provide reviews of the quality of the vendor and their services within their thread after a transaction is complete (Dupont et al., 2017; Holt & Lampke, 2010; Hutchings & Holt, 2015).

Variants of forums also exist on the Dark Web which are called cyrptomarkets, referencing the notion that the site is hosted on an encrypted portion of the Internet and utilizes encrypted payment methods to facilitate illicit commerce (Barratt, 2012; Decary-Hetu et al., 2017; Moeller et al., 2017). Cryptomarkets can provide a space for multiple vendors to sell products simultaneously, as with forums, though there are some that are single operator shops selling multiple products (Decary-Hetu et al., 2017; Moeller et al., 2017; Tzanetakis et al., 2017).

Forums and cryptomarkets typically require participants to register with the forum in order to post messages, and may also hide posted content from outsiders until they register. Such a practice still fits within the notion of a quasi-open market (Holt & Dupont, 2019), as these sites may be identified on the basis of their involvement in the sale of illicit goods, like stolen credit card data (Decary-Hetu & Leppanen, 2013; Holt & Lampke, 2010), hacking tools (Holt, 2013), or drugs (Decary-Hetu & Gommoni, 2017; Decary-Hetu et al., 2016).

To reduce the risk of registration by law enforcement and the research community, some forums and cryptomarkets have adopted strategies that mirror the characteristics of closed markets in physical space. For instance, some sites require potential participants to pay for access to the market in order to increase the likelihood that they will complete a transaction (Decary-Hetu et al., 2017; Dupont et al., 2017; Holt & Dupont, 2019). Others have adopted social vetting schemes, where anyone who attempts to register with the site are required to

provide details about their involvement in other online communities and illicitactivities (Dupont et al., 2017; Holt & Dupont, 2019; Meyer, 1989). The applications are then reviewed by the existing members who can provide feedback and essentially vouch for the individual's claims (Dupont et al., 2017; Holt & Dupont, 2019).

UNDERSTANDING THE PRACTICES OF PARTICIPANTS IN ONLINE ILLICIT MARKETS

The differences observed in the structure of the forums and shops operating on the Open and Dark Web call to question how participants engage in illicit exchanges online. Research indicates there are substantial similarities in the ways that vendors advertise and engage in transactions (Holt & Lee, 2020; Smirnova & Holt, 2017). The process of beginning a transaction are quite similar, regardless of whether the vendor offers physical goods, such as drugs, or virtual commodities like credit card numbers. Studies utilizing crime script analyses illustrate that vendors must first make their advertisement and provide an overall description of their products, pricing, and purchasing details (Copeland et al., 2020; Decary-Hetu et al., 2016; Holt & Lee, 2020; Hutchings & Holt, 2015; Roddy & Holt, 2020).

Advertisements that provide concise details as to the nature of their products are often seen as being more legitimate, particularly if they can provide photos of the items that are not taken from other websites or stock photos (Copeland et al., 2020; Tzanetakis et al., 2017). Variations in the nature of products also creates differences in the language included in advertisements. For instance, individuals offering stolen credit and debit card information often provide specific details as to the bank that issued the card, and the state and country of origin for the data (Franklin et al., 2007; Holt & Lampke, 2010; Smirnova & Holt, 2017). Vendors selling passports and identity documents often identify the exactpersonal information potential customers need to provide in order to create the document (Holt & Lee, 2020). Sellers may also provide information on their shipping procedures, particularly in the case of firearms and narcotics, so that customers understand how products may arrive (Copeland et al., 2020; Decary-Hetu et al., 2017).

Once an advertisement has been created, customers are then required to reach

out to the vendor to complete a transaction. In the case of forums and cryptomarkets, customers may contact the vendor via private messaging applications or email (Decary-Hetu et al., 2017; Martin et al., 2014). This is also true for some shops on both the open and dark web, which may use website-based contact forms or internal ticketing and communications tools that allow customers to connect with vendors (Copeland et al., 2020; Holt & Lee, 2020; Roddy & Holt, 2020). Vendors are also increasingly using encrypted email systems, like Protonmail, on both the open and dark web as they provide end-to-end protection for the contents of emails in transit (Decary-Hetu et al., 2016; Martin, 2014). Should law enforcement or other entities intercept messages as they move between email servers, it is not possible to read its contents without the decryption key which is available only to the account holder (Decary-Hetu et al., 2016; Martin, 2014). Some services will also not log personal information, including IP address details, reducing the potential for loss of sensitive details to outsiders (Decary-Hetu et al., 2016).

Next, potential customers must attempt to place an order with the vendor through whatever preferred contact method they may indicate. Buyers must be exact in their order, stating the quantity of product and any specifics associated with design or customization, as is the case with fraudulent identity documents (Decary-Hetu et al., 2016; Holt & Lee, 2020; Odabas et al., 2017). It is also possible for customers to negotiate price when purchasing in bulk quantities, or should the vendor allow for discount codes or coupons to reduce the final price (Barratt, 2012; Dupont et al., 2017; Holt & Lampke, 2010; Holt & Lee, 2020; Hutchings & Holt, 2015). The use of discounts is thought to be a way for reputable vendors to retain customers over the long term and provide a degree of customer service, akin to legitimate e-commerce models (Decary-Hetu & Leppannen, 2013; Holt et al., 2015; Hutchings & Holt, 2015).

Once the final price is set, customers must then pay the vendor as no goods are tendered until payment is received. It may take days or weeks for vendors to deliver a customer's purchased goods in the case of drugs, firearms or other physical items (Copeland et al., 2020; Decary-Hetu et al., 2017; Moeller et al., 2017). Digital items, such as data, malicious software, or cybercrime services, can typically be accessed within minutes or hours of purchase depending (Franklin et al., 2007; Holt, 2012; Holt & Lampke, 2010). Regardless, there is a clear risk

that vendors may either simply fail to send the goods purchased, or provide adulterated or unusable items. For instance, stolen data vendors who fail to deliver customer products are referred to as “rippers” or rip off artists, and are viewed as a scourge on the market (Holt, 2012; Holt & Lampke, 2010; Hutchings & Holt, 2015). It is also possible that goods may be detected in transit and either seized or used to enable an arrest, as has been observed in the sale of both drugs and guns that are shipped through common package delivery services like DHL, UPS, and FedEx (Copeland et al., 2020; Decary-Hetu et al., 2016). In fact, a number of arrests have occurred in the US and UK because US Homeland Security investigators identify the weapons in transit and notify the appropriate law enforcement agencies at the destination residence (Copeland et al., 2020). Police then use the delivery as a cause to arrest individuals on charges related to the illegal purchase and possession of firearms.

In the event that products are not delivered or there is some problem with their quality, buyers must carefully review the terms of service for their purchase as they vary across vendors (Holt & Lee, 2020; Hutchings & Clayton, 2016; Hyslip & Holt, 2019). Typically, there are rules posted within each shop or advertisement within a forum or cryptomarket regarding what sellers support in terms of product replacements or errors in documents or delivered items. Many stolen data vendors offer free replacements for inactive cards within a 24 to 48-hour period of purchase, though some offer no such support (Holt & Lampke, 2010; Holt et al., 2015). Malware and cybercrime-as-service providers also operate customer support lines for customers in the event of product failure or error (Holt, 2013; Hutchings & Clayton, 2016). Some vendors for physical products, like drugs and stolen identity documents, clearly state that they do not offer refunds but may give conditional returns if the error is reported within a certain amount of time after purchase, or there was a clear error related to the purchased item (Dupont et al., 2016; Holt et al, 2016; Hutchings & Holt, 2015).

If the vendor adheres to posted policies, then the customer may be able to gain some satisfaction from the transaction. In the event they are ignored or unable to obtain the products they paid for, customers often have little recompense (Decary-Hetu et al., 2016; Moeller et al., 2017). A customer cannot contact police as they are essentially complicit in an illegal activity by virtue of their paying for drugs or cybercrime services. In addition, many vendors do not

accept payment via services that would allow the customer to dispute a charge (Decary-Hetu et al., 2016; Hutchings & Holt, 2017). As a consequence, participants in illicit markets have developed a number of different mechanisms that serve as informal sources of social control and risk avoidance strategies to minimize the likelihood of harm resulting from bad transactions.

One of the primary strategies employed over time has been the use of informal reviews of vendors in various markets. For instance, individuals who performed transactions with vendors who posted ads in forums were regularly able to post their experiences in the same thread (Decary-Hetu & Leppannen, 2013; Holt & Lampke, 2010; Holt et al., 2016). The direct feedback of the speed of communications and qualities of the seller gave potential customers an ability to discern who offered the best products at the most reasonable prices (Odabas et al., 2017; Smirnova & Holt, 2017). The presence of negative feedback served as a warning that the vendor may be unreliable, though positive and negative comments could be manufactured to influence the perception of their services (Odabas et al., 2017; Smirnova & Holt, 2017).

In recent years, third party reviewing services have emerged to provide insights on the qualities of vendors operating via shops and other platforms. For instance, the site Deep Dot Web served as an Open Web resource for individuals seeking information on vendors operating on the Dark Web (Department of Justice, 2021). The site provided information on the URLs of active shops and cryptomarkets, as well as informal news related to their operations and the quality of their services. The operators of the site were eventually arrested and prosecuted in the US on charges associated with money laundering (Department of Justice, 2021). Specifically, they were alleged to have received payments from individuals trafficking in drugs, guns, and other illicit products on the basis that they make positive comments about the vendors (Department of Justice, 2021).

An additional method of risk reduction that can be employed by market participants is the use of escrow payment systems (Decary-Hetu et al, 2016; Holt, 2012; Holt et al., 2015; Hutchings & Holt, 2015). The use of escrow in online markets mirrors that of traditional escrow services in legitimate business operations, wherein a third party holds funds as a guarantee of payment for a service provider. Escrow services were first observed in stolen data and malicious software sales in forums, where an individual within the forum's management

structure could be designated as an escrow provider on behalf of buyers and sellers (Decary-Hetu & Lepannen, 2013; Holt, 2012; Holt & Lampke, 2010). That individual could intervene in the sales process and hold funds from the customer with guaranteed deliver to the seller so long as the customer received products. Escrow operations typically came with a fee for their services, though they helped to create trust between participants as they could ensure both parties benefited from a transaction (Holt, 2012; Holt & Lampke, 2010).

Escrow services persist on both the Open and Dark Web, though they have become decentralized to some degree as forums have become less prevalent. Instead, escrow services now exist as independent operations and are an option for customers who are unsure of the reliability of a seller (Decary-Hetu et al., 2016; Moeller et al., 2017). If both parties accept the use of escrow, it can increase the likelihood of a successful transaction. At the same time, there is now risk related to the identification of a reliable escrow service provider who will not simply abscond with funds given by a potential customer. In fact, a number of cryptomarkets held payments in escrow on behalf of customers and buyers and simply shuttered their sites without completing any transactions. These events are colloquially referred to as exit scams, and have become a somewhat common occurrence in cryptomarket operations (Riley, 2019; Schwartz, 2020). It is unclear if exit scams occur as a long-term scheme on the part of scammers, or are a calculated decision by cryptomarket operators to close before police actions occur (Riley, 2019). Regardless, the presence of exit scams creates a risk that all participants must consider in their decision to engage in a transaction through Dark Web markets.

CHALLENGES AND DIRECTION FOR RESEARCH ON ILLICIT MARKET OPERATIONS

Though research on illicit markets in online spaces has grown dramatically over the last decade, there are still foundational questions that must be addressed. First, there is a need for continuous qualitative and quantitative explorations of the practices of the market to track shifts in both buyer and seller behaviors (Decary-Hetu et al., 2016; Dupont et al., 2017; Hutchings & Holt, 2017). This is particularly essential as the COVID19 pandemic has had a transformative impact on the supply chains for products, as well as the overall habits of consumers. The extent to which consumers may be interested in acquiring narcotics and pharmaceuticals for recreational or prescription needs must be better understood (Barratt & Aldridge, 2020; Bergeron et al., 2020; Groshkova et al., 2020). There is also a need for research addressing the extent to which COVID19 vaccines, vaccination cards, and related materials have flooded the market (Bergeron et al., 2020; Groshkova et al., 2020).

Additionally, foundational research considering the decision-making processes of buyers for various products must be performed. For instance, several studies noted the rise of firearms markets on the Dark Web, though it is unclear who vendors are targeting with their advertisements (Copeland et al., 2020; Paoli et al., 2017). Survey research attempting to identify how many individuals in countries with restrictive gun laws have sought out weapons online may help to improve our understanding of the general audience for these ads (Copeland et al., 2020). Similar studies have explored the purchasing habits of narcotics users in Australia (Barratt et al., 2017), suggesting it may be possible to perform similar work regarding other illicit products, including identity documents (Holt & Lee, 2020) and firearms (Copeland et al., 2020).

The same is true regarding the ways that potential buyers identify vendors for products in the increasingly fragmented advertising environment for illicit goods. Not only do vendors operate on shops, forums, and cryptomarkets, but have also begun to sell products on social media platforms and communications systems (Bachhuber & Merchant, 2017; Moyle et al., 2019). This adds to the inherent difficulty in identifying vendors and distinguishing their legitimacy (Tzanetakis et

al., 2017). Qualitative investigations of customers would be essential to better understand the ways that they negotiate the online market and authenticate vendor claims over time (Holt et al., 2015; Hutchings & Holt, 2017).

Research is also needed to better understand the decision-making processes of vendors who operate illicit markets. Though there has been substantive focus on the perceived and real legitimacy of vendors operating in various markets (e.g Decary-Hetu & Leppanen, 2013; Holt et al., 2016), few have considered the factors that drive individuals to post advertisements for goods that are likely false. For instance, research and media reporting have noted the range of hitman advertisements on the Dark Web (Kassab & Rosen, 2019; Roddy & Holt, 2020). These sites are thought to be false, and serve only to rip off potential customers (Kassab & Rosen, 2019; Roddy & Holt, 2020). It is assumed that such ads generate profits for advertisers, though it is unclear if any other thought processes guide the decision to make false ads (Roddy & Holt, 2020). Additionally, it is unclear if such vendors operate multiple fictitious ads, or operate in both legitimate and fraudulent products simultaneously. Such work is vital to improve our knowledge of the extent to which fraud is a specific or general characteristic of illicit market operations in online spaces.

Similarly, work is needed to assess what factors compel vendors to engage in activities on the Open or Dark Web, or both environments simultaneously. For instance, a small number of studies has observed differences in both the quantities, qualities, and prices for products for sale when comparing Open and Dark Web advertisements (Holt & Lee, 2020; Smirnova & Holt, 2017). It is thought that such differences may be a function of the global reach of vendors on the Open Web relative to the Dark Web, which has a small, Western-nation user base (Holt & Lee, 2020; Smirnova & Holt, 2017). Research is needed to assess whether such differences stem from deliberate decision-making on the part of vendors to operate differently across environments. Furthermore, the degree to which vendors decide where to advertise on the basis of perceived risk of detection or other factors, such as an inability to be extradited or prosecuted must be explored (Decary-Hetu et al., 2017; Hutchings & Holt, 2017). Such research could greatly expand our knowledge of the degree to which rational choice and deterrent efforts guide the behaviors of vendors.

In much the same way, empirical inquiry is needed to understand the ways

that illicit markets for products persist in the face of law enforcement crackdowns (Decary-Hetu et al., 2016; Holt, Blevins, & Kuhns, 2008; 2014). For instance, a series of arrests were made by police agencies in the US and Europe, targeting both the customers and operators of booter and streser services (Jeffrey, 2018; Krebs, 2018; Krebs, 2019). Recent analyses suggest that the number of attacks performed by service providers decreased in the wake of enforcement efforts (Collier et al., 2019: Pritchard, 2020). Though these investigations reduced the operational capacities of vendors, the risk of arrest and detection was not enough to eliminate their operations from the Internet (Collier et al., 2019). Thus, research is needed to consider why and how these offenders practice restrictive deterrence strategies to continue offending (Collier et al., 2019; Holt & Bossler, 2016; Holt et al., 2015).

Finally, there is a need for researchers to identify data sources that extend beyond the current sampling strategies used in published studies (Holt & Dupont, 2019; Holt & Bossler, 2015; Yip et al., 2013). Most academic data is derived from shops, forums, and cryptomarkets that can be accessed by the general public. Though useful, this data only informs our understanding of the surface level, open markets that exist (Decary-Hetu et al., 2016; Holt & Dupont, 2017; Hutchings & Holt, 2017). The practices of those actors engaged in more serious, closed markets are less frequently examined due to the inherent difficulty in accessing these sources. Closed communities can require payment or social vetting in order to gain entry, which limits the ability of researchers to engage due to the ethical constraints in place in university settings (e.g. Holt & Bossler, 2015; Yip et al., 2013).

As a consequence, there is a need for researchers to develop alternative strategies for data collection that would improve our understanding of closed communities. For example, hacked or leaked data from forums have been used by researchers to understand the practices of hacker communities (Dupont et al., 2017; Holt & Dupont, 2019). Such data presents its own unique ethical dilemmas for researchers as the data may have been acquired illegally, even if it is available for public download (Holt & Bossler, 2015). Instead, researchers may find value in developing surveys and interview protocols that could be administered to active participants within these communities (e.g. Barratt et al., 2017; Hutchings & Holt, 2017). While they present a high risk of failure due to

low response rates, they could produce valuable findings in ways that conform to existing ethical guidelines.

Additionally, developing data through police files could be informative to understand the practices of known criminals and their associates (Holt & Bossler, 2015; Leukfeldt et al., 2017). Such efforts require collaborative agreements with law enforcement and cybersecurity providers could also prove invaluable as they have the capacity to access these communities. Creating memorandums of understanding that would enable data sharing without attribution to ongoing investigations or tradecraft could be extremely useful to understand the ways actors engage with one another without violating ethical practices (Holt & Bossler, 2015; Hutchings & Holt, 2017).

CONCLUSION

Criminological scholarship on illicit markets operating in online spaces has grown dramatically over the last two decades, assessing the state of both physical and digital goods for sale (Decary-Hetu et al., 2017; Holt & Bossler, 2015; Hutchings & Holt, 2017). The growth of the Internet, e-commerce applications, encrypted communications platforms and financial services have created an operating environment where virtually any good or service can be sold, mirroring the activities of real world illicit goods markets. These studies demonstrate the similarities between the practices of vendors and buyers operating in virtual and real spaces, particularly regarding the process of navigating illicit transactions (Barratt, 2012; Holt & Dupont, 2019; Holt et al., 2015; Hutchings & Holt, 2017). There are distinctions, however, in the risks that they face from law enforcement and from informal threats such as fraudulent vendors (Decary-Hetu et al., 2017; Holt et al., 2016; Tzanetakis et al., 2016).

Research on the processes of markets on both the Open and Dark Web provide substantive insights into the ways these forms of cybercrime are driven by social forces and assessments of risk and reward. These studies highlight potential opportunities for law enforcement, ISPs, and other place managers to more effectively regulate online spaces and limit the scope of illicit market operations (Hutchings & Holt, 2017). At the same time, the evolution of technology and its acceptance by the public will undoubtedly force changes in the practices of illicit markets in both virtual and real settings. The rise of cryptomarkets and various digital currencies will likely be replaced by other platforms in the near future, due in part to their perceived ease of use and minimized risk of detection by law enforcement (Holt et al., 2016). For instance, the use of encrypted messaging applications and social media may have a transformative impact on both virtual and real markets for illicit narcotics (Bachhuber & Merchant, 2017; Moyle et al., 2019). Thus, researchers must be vigilant in their investigation of illicit economies, regardless of where they operate to better understand their social and financial processes and ensure the efficacy of criminal justice responses to these offenses.

References

Adler, P. A. (1993). *Wheeling and dealing: An ethnography of an upper-level drug dealing and smuggling community*. Columbia University Press.

Bachhuber, M. A., & Merchant, R. M. (2017). Buying drugs online in the age of social media. *American journal of public health*, *107*(12), 1858.

Barratt, M. J. (2012). Silk Road: eBay for drugs. *Addiction, 107*/3: 683-683.

Barratt, M. J., & Aldridge, J. (2020). No magic pocket: Buying and selling on drug cryptomarkets in response to the COVID-19 pandemic and social restrictions. *International Journal of Drug Policy*, *83*, 102894.

Barratt, M. J., Ferris, J. A., Zahnow, R., Palamar, J. J., Maier, L. J., & Winstock, A. R. (2017). Moving on from representativeness: testing the utility of the Global Drug Survey. *Substance Abuse: Research and Treatment*, *11*.

Bateman, S. (2021). Sex slaves, human hunting trips, hitmen for hire: Dark web expert sorts fact from fiction. Daily Star, January 3, 2021. https://www.dailystar.co.uk/news/weird-news/sex-slaves-human-hunting-trips-23097531

Bergeron, A., Décary-Hétu, D., & Giommoni, L. (2020). Preliminary findings of the impact of COVID-19 on drugs crypto markets. *International Journal of Drug Policy*, *83*, 102870.

Carr, A. (2011). The Craigslist Crime Report: "Cesspool of Crime," Bold Use of Marketing. Fast Company, Feb. 24, 2011. https://www.fastcompany.com/1731352/craigslist-crime-report-cesspool-crime-bold-use-marketing-updated

Cook, P. J., Cukier, W., & Krause, K. (2009). The illicit firearms trade in North America. *Criminology & Criminal Justice*, *9*(3), 265-286.

Cooper, J., & Harrison, D. M. (2001). The social organization of audio piracy on the Internet. *Media, Culture & Society*, *23*(1), 71-89.

Copeland, C., Wallin, M., & Holt, T. J. (2020). Assessing the practices and products of Darkweb Firearm vendors. *Deviant Behavior*, *41*(8), 949-968.

Cunningham, S., & Shah, M. (eds., 2016). *The Oxford Handbook of the Economics of Prostitution.* Oxford: Oxford University Press.

Décary-Hétu, D., & Giommoni, L. (2017). Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. *Crime, Law and Social Change*, *67*(1), 55-75.

Décary-Hétu, D., Paquet-Clouston, M., & Aldridge, J. (2016). Going international? Risk taking by cryptomarket drug vendors. *International Journal of Drug Policy*, *35*, 69-76.

Décary-Hétu, D., & Leppänen, A. (2013). Criminals and signals: An assessment

of criminal performance in the carding underworld. *Security Journal*, 31: 1-19.

Department of Justice (2021). DeepDotWeb administrator pleads guilty to money laundering conspiracy. March 31, 2021. Washington D.C. [Online] Available at: https://www.justice.gov/opa/pr/deepdotweb-administrator-pleads-guilty-money-laundering-conspiracy

Dupont, B., Côté, A.-M. Boutin, J.-I., & Fernandez, J. (2017). Darkode: Recruitment patterns and transactional features of "the most dangerous cybercrime forum in the world." *American Behavioral Scientist* 61: 1219-1243.

Eck, J. (1995). A General Model of the Geography of Illicit Retail Marketplaces, in J. Eck and D. Weisburd, eds., *Crime and Place.Crime Prevention Studies, Vol.4.* Monsey, New York: Criminal Justice Press

Gibbs, J. (1975). *Crime, Punishment, and Deterrence*. New York: Elsevier.

Groshkova, T., Stoian, T., Cunningham, A., Griffiths, P., Singleton, N., & Sedefov, R. (2020). Will the current COVID-19 pandemic impact on long-term cannabis buying practices?. *Journal of Addiction Medicine*.

Hamid, A. (1998). *Drugs in America.* Gaithersburg, MD: Aspen

Holt, T. J. (2010). Exploring strategies for qualitative criminological and criminal justice inquiry using online data. *Journal of Criminal Justice Education, 21*/4: 466-487.

Holt, T. J. (2013). Examining the forces shaping cybercrime markets online. *Social Science Computer Review, 31*/2: 165-177.

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

Holt, T. J., Blevins, K. R., & Kuhns, J. B. (2014). Examining diffusion and arrest practices among johns. *Crime and Delinquency,* 60, 261–283.

Holt, T. J., & Dupont, B. (2019). Exploring the factors associated with rejection from a closed cybercrime community. *International journal of offender therapy and comparative criminology*, *63*(8), 1127-1147.

Holt, T. J. & Lampke, E. (2010). Exploring stolen data markets online: Products and market forces. *Criminal Justice Studies, 23*/1: 33-50.

Holt, T. J., & Lee, J. R. (2020). A Crime Script Analysis of Counterfeit Identity Document Procurement Online. *Deviant Behavior*, 1-18.

Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). *Data thieves in action: Examining the international market for stolen personal information.* New York: Palgrave.

Holt, T. J., Smirnova, O., Chua, Y. T., & Copes, H. (2015). Examining the risk reduction strategies of actors in online criminal markets. *Global Crime*, *16*(2), 81-103.

Holt, T. J., Smirnova, O., & Hutchings, A. (2016). Examining signals of trust in criminal markets online. *Journal of Cybersecurity*, *2*(2), 137-145.

Hospodar, M. (2021). 10 Underrated Horror Games (That Came Out in the Last 5 Years). Gamerant, Febuary 11, 2021. https://gamerant.com/underrated-horror-games-last-5-years/

Hureau, D. M., & Braga, A. A. (2018). The trade in tools: The market for illicit guns in high-risk networks. *Criminology*, *56*(3), 510-545.

Hutchings, A., & Clayton, R. (2016). Exploring the provision of online booter services. *Deviant Behavior*, *37*(10), 1163-1178.

Hutchings, A., & Holt, T. J. (2015). A crime script analysis of the online stolen data market. *British Journal of Criminology, 55*/3*:* 596-614.

Hutchings, A., & Holt, T. J. (2017). The online stolen data market: disruption and intervention approaches. *Global Crime*, *18*(1), 11-30.

Jacobs, B. A. (1996). Crack dealers' apprehension avoidance techniques: A case of restrictive deterrence. *Justice Quarterly, 13*/3: 359-381.

Jacobs, B. A. (2000). *Robbing drug dealers: Violence beyond the law.* Boston: Northeastern University Press.

Jacobs, B. A. (2010). Deterrence and Deterrability. *Criminology* 48: 417-441.

Johnson, B. D., & Natarajan, M. (1995). Strategies to avoid arrest: Crack sellers' response to intensified policing. *American Journal of Police, 14*/3/4: 49-69.

Johnson, B. D., Dunlap, E., & Tourigny, S. C. (2000). Crack distribution and abuse in New York. *Crime prevention studies*, *11*, 19-58.

Kassab, H. S., & Rosen, J. D. (2019). Illicit Markets and the Internet Age. In *Illicit Markets, Organized Crime, and Global Security* (pp. 155-175). Palgrave Macmillan, Cham.

Kennedy, D. M., Piehl, A. M., & Braga, A. A. (1996). Youth violence in Boston: Gun markets, serious youth offenders, and a use-reduction strategy. *Law and Contemporary Problems*, *59*(1), 147-196.

Klokars, C. B. (1974). The Professional Fence. New York: The Free Press.

Knowles, G. J. (1999). Deception, detection, and evasion: A trade craft analysis of Honolulu, Hawaii's street crack-cocaine traffickers. *Journal of Criminal Justice*, *27*(5), 443-455.

Lavorgna, A. (2014). Wildlife trafficking in the Internet age. *Crime Science*, *3*(1), 1-12.

Martin, J. (2014). *Drugs on the dark net: How cryptomarkets are transforming the global trade in illicit drugs*. New York: Springer.

May, T., & Hough, M. (2004). Drug markets and distribution systems. *Addiction Research and Theory*, 12: 549-563.

Meyer, G. R. (1989). *The Social Organization of the Computer Underground.*

Master's thesis, Northern Illinois University.

Moeller, K., Munksgaard, R., & Demant, J. (2017). Flow my FE the vendor said: Exploring violent and fraudulent resource exchanges on cryptomarkets for illicit drugs. *American Behavioral Scientist*, *61*(11), 1427-1450.

Moyle, L., Childs, A., Coomber, R., & Barratt, M. J. (2019). # Drugsforsale: An exploration of the use of social media and encrypted messaging apps to supply and access drugs. *International Journal of Drug Policy*, *63*, 101-110.

Paoli, G. P., Aldridge, J., Nathan, R., & Warnes, R. (2017). *Behind the curtain: The illicit trade of firearms, explosives and ammunition on the dark web.* Santa Monica, CA: Rand: [Online] Available at: https://www.research.manchester.ac.uk/portal/files/57841517/RAND_Behind_the_curtain.pdf

Potter, G. (2009). Exploring retail-level drug distribution: Social supply,"real" dealers and the user/dealer interface. *Old and new policies, theories, research methods and drug users across Europe*, 50-74.

Power, M. (2013). Online highs are as old as the net: The first e-commerce was a drugs deal. The Guardian, April 19, 2013. https://www.theguardian.com/science/2013/apr/19/online-high-net-drugs-deal

Riley, D. (2019). $30M stolen as popular dark web market closes. siliconANGLE, April 23, 2019. https://siliconangle.com/2019/04/23/30m-stolen-popular-dark-web-market-pulls-exit-scam/

Roddy, A. L., & Holt, T. J. (2020). An Assessment of Hitmen and Contracted Violence Providers Operating Online. *Deviant Behavior*, 1-13.

Schneider, J. L. (2005). Stolen-Goods Markets: Methods of Disposal 1. *British Journal of Criminology*, *45*(2), 129-140.

Schwartz, M. J. (2020). Bye-bye Bitcoins: Empire Darknet Market 'Exit Scams'. Euro Security Watch, September 2, 2020. https://www.bankinfosecurity.com/blogs/bye-bye-bitcoins-empire-darknet-market-exit-scams-p-2934

Scott, M. S., & Dedel, K. Street prostitution. *Problem Oriented Policing Guide Series (2)*. Washington D.C.: Office of Community Oriented Policing Services, U.S. Department of Justice.

Smirnova, O., & Holt, T. J. (2017). Examining the geographic distribution of victim nations in stolen data markets. *American Behavioral Scientist*, *61*(11), 1403-1426.

Sollund, R. A. (2019). *The crimes of wildlife trafficking: Issues of justice, legality and morality*. London: Routledge.

Sterk, C. (1999). *Fast lives: Women who use crack cocaine.* Philadelphia, PA: Temple University Press.

Topalli, V., Wright, R., & Fornango, R. (2002). Drug dealers, robbery and retaliation. Vulnerability, deterrence and the contagion of violence. *British Journal of Criminology, 4*2/2: 337-351.

Turnbull, R. (2002). *A Rock and a Hard Place: Drug Markets in Deprived Neighbourhoods*. Home Office Research Study No. 240. London: Home Office.

Tzanetakis, M., Kamphausen, G., Werse, B., & von Laufenberg, R. (2015). The transparency paradox. Building trust, resolving disputes and optimising logistics on conventional and online drugs markets. *International Journal of Drug Policy*, 35: 58-68.

VanNostrand, L. M., & Tewksbury, R. (1999). The Motives and Mechanics of Operating an Illegal Drug Enterprise." *Deviant Behavior* 20/1: 57-83.

Weitzer, R. (2012). *Legalizing prostitution: From illicit vice to lawful business*. NYU Press.

Wright, R., & Decker, S. H. (1994). *Burglars On the Job: Streetlife and Residential Break-ins.* Boston, MA: Northeastern University Press.

Wright, R., & Decker, S. H. (1997). *Armed Robbers in Action: Stickups and Street Culture.*

Boston, MA: Northeastern University Press.

Parenting Practices as a Mediating Factor between Neighborhood Disadvantage and Delinquency

*Young S. Kim, Ph.D.**
Professor of Criminology
Eastern Michigan University

Brian G. Sellers, Ph.D.
Associate Professor of Criminology
Eastern Michigan University

Abstract

The present study examines the mediating role of parenting practices between neighborhood disadvantage and adolescent delinquency by analyzing data from the first wave of the National Longitudinal Study of Adolescent Health (ADD-Health). The results showed that neighborhood disadvantage, parenting practices, adolescents' low self-control, and delinquency are significantly interrelated with each other. However, the significant effect of neighborhood disadvantage on delinquency at one time became 'insignificant' after four variables of parenting practices are controlled. Furthermore, parenting practices maintained their significant effects on delinquency even after controlling for adolescents' low self-control and other developmental outcomes. These findings suggest that not only may parenting practices mediate the relationship between neighborhood disadvantage and delinquency, but also parenting practices may have a direct independent effect on delinquency. The present study provides important implications for the development of delinquency prevention programs focused on improving parenting skills.

Keywords

Parenting Practices, Neighborhoods, Delinquency, Mediation

---

* Direct correspondence to Young S. Kim, Ph.D., Professor of Crimmology, Eastern Michigan University; e-mail: ykim4@emich.edu.
* http://dx.doi.org/10.36889/IJCJ.2021.001.
* Received 22 November 2020; Revised 4 January 2021; Accepted 8 January 2021; Available online 26 February 2021.
INTERNATIONAL JOURNAL OF CRIMINAL JUSTICE, Vol. 3 Issue 1, June 2021, 24-59

INTRODUCTION

A large volume of studies have suggested 'parenting' as a crucial source of influence among adolescents, showing its relationships with youths' various developmental outcomes, such as academic performance (e.g., Anunola, Stattin, & Nurmi, 2000; Juang & Silbereisen, 2002; Park & Bauer, 2002), self-esteem (e.g., Bulanda & Majumdar, 2008), mental health (e.g., Aquilino & Supple, 2001), substance abuse (e.g., Shakya, Christakis, & Fowler, 2012), and delinquency (e.g., Mowen & Schroeder, 2015; Schroeder & Mowen, 2014; Wright & Cullen, 2001). Also, numerous empirical studies show that neighborhood structural characteristics affect youth delinquency through social disorganization or ineffective collective efficacy (e.g., Bellair, 1997; Bernburg & Thorlindsson, 2007; Elliott, Wilson, Huizinga, Sampson, Elliott, & Rankin, 1996; Fagan & Wright, 2012; Morenoff, Sampson, & Raundenbush, 2001; Sampson, 2006; Sampson & Grove, 1989; Sampson, Morenoff, & Raudenbush, 2005; Sampson, Raudenbush, & Earls, 1997; Zimmerman, 2010). Thus, it is evident that youth delinquency is influenced simultaneously by both parenting practices within the family and neighborhood characteristics where adolescents and families are embedded.

However, parenting and the neighborhood would not affect delinquency independently in isolation from each other. Since family dynamics occur within the context of neighborhoods, 'parenting practices' would be a function of neighborhood structural characteristics. Several studies have reported that disadvantageous structural characteristics of neighborhoods negatively affect parenting, including inconsistent and harsh parenting practices, low expectations, poor care and control, and lack of warmth (e.g., Arditti, Burton, & Neeves-Botelho, 2010; Kerstenburg, Brooks-Gunn, & Duncan, 1994; Furstenburg, 1993; Kohen, Dahiten, Leventhal, & McIntosh, 2008; Taylor, 2000; Vieno, Nation, Perkins, Pastore, & Santinello, 2010; Zuberi, 2016). Such findings may suggest a mediating role of parenting practices between neighborhood and adolescents' delinquency.

Also, studies have reported that parenting is significantly related to youth' level of self-control that is a significant predictor of juvenile delinquency (e.g., Hay, 2001; Muftic & Updegrove, 2018; Perrone, Sullivan, Pratt, & Margaryan,

2004). Therefore, high delinquency involvement among adolescents in more disadvantaged neighborhoods may be partially due to parents' inability to exercise effective parenting practices which, in turn, leads to adolescents' development of low self-control.

A handful of empirical studies suggest that parenting mediates the relationship between neighborhood structural characteristics and delinquency (Beyer, Bates, Petit, & Dodge, 2003; Chung & Steinburg, 2006; Kohen, et. al, 2008; Leventhal & Brooks-Gunn, 2000; Mrug & Windle, 2009; Rankin & Quane, 2002; Sampson & Laub, 1994 & 2004; Tolan, Gorman-Smith, & Henry, 2003; Vieno, et al., 2010). Nevertheless, the generalizability of the findings is somewhat limited due to the fact that each of the studies used a small selective sample, such as African-American youths, male youths from urban cities, serious offenders, and so on.

Addressing the limitations of previous research, the present study aims to improve on the literature regarding the effects of neighborhoods and parenting on juvenile delinquency, by examining the importance of parenting practices as a more proximal and immediate mediating factor between neighborhood structure and youth delinquency with a nationally representative sample of adolescents and their neighborhoods.

THEORETICAL BACKGROUNDS

Social Disorganization and Collective Efficacy

The foundation of social disorganization theory can be traced back to the work of Shaw and McKay (1942 & 1969), which examined the effects on delinquency of social structural characteristics of the area called "zone in transition," where concentrations of poverty, a high frequency of people moving in and out of this area, and higher numbers of ethnic minorities residing in this zone disrupted the social cohesion and subsequently weakened the community's ability to exercise informal social controls, resulting in 'social disorganization' (Shaw & McKay, 1942 &1969).

Following in Shaw and McKay (1942)'s footsteps, numerous researchers have tested the theory by examining the effects of various variables of neighborhood structural characteristics on delinquency. Early research on the theory had focused

mostly on establishing a relationship between the two by utilizing aggregated neighborhood-level data, and reported that certain structural characteristics of neighborhoods (e.g., poverty rates, mobility rates, racial heterogeneity index, and etc.) are associated with high delinquency rates (Bursik, 1984, 1986; Bursik & Webb, 1982; Gordon, 1967; Kornhauser, 1978; Rosen & Turner, 1967; Schuerman & Koblin, 1986).

Later, several researchers tried to find a mechanism explaining how neighborhood structures affect delinquency. Sampson and Grove's (1989) work investigated how exogenous variables defining community structure affect social controls such as friendship and kinship networks along with unsupervised peer groups and local organizational participation. Their findings suggest that low friendship networks and high levels of unsupervised peer groups result in higher rates of victimization. In addition, when family disruption and ethnic heterogeneity increase, the level of adolescent street-corner groups also increases (Sampson & Groves, 1989).

After that, Sampson, Raudenbush, and Earls (1997) proposed the concept of "collective efficacy" to explain a mechanism of how neighborhood-level social structures affect delinquency rates. They defined collective efficacy as "the linkage of mutual trust and the willingness to intervene for the common good…" (Sampson et al., 1997, p. 919). Utilizing a more advanced multi-level approach, researchers attempted to identify and examine various indicators of collective efficacy and reported that the effect of neighborhood structures (e.g., concentrated disadvantage, heterogeneity, residential instability, family disruption, and population size or density) on delinquency is intervened by weakened collective efficacy or ineffective informal social control of neighborhoods (Bellair, 1997; Bernburg & Thorlindsson, 2007; Elliott, et. al., 1996; Fagan & Wright, 2012; Morenoff, et al., 2001; Sampson, 2006; Sampson, et. al., 2005; Sampson, et. al., 1997; Zimmerman, 2010). For example, Morenoff et al. (2001) reported that measures of local organizations, voluntary associations, and friend/kinship networks inhibited delinquency to the extent that they facilitated the collective efficacy of residents.

Despite recent researchers' successful attempts in establishing neighborhood-level social disorganization/collective efficacy as an intervening element between neighborhood structure and youth delinquency (Bernburg & Thorlindsson, 2007; Elliott, et al., 1996; Fagan & Wright, 2012; Osgood & Anderson, 2004; Sampson

et al., 2005), the effect of neighborhood-level social disorganization or collective efficacy on adolescents may be somewhat 'distal' due to the fact that adolescents are simultaneously imbedded in other micro-level socialization units within neighborhoods, such as family and peer groups (Cummings, Davis, & Campbell, 2002). Thus, research on social disorganization/collective efficacy could be expanded further via incorporating more proximal social units or processes that transmit the effects of neighborhood structure on adolescent delinquency. Probably, as an important socialization unit, family or parenting practices would be the best candidate.

Parenting – Social Control Theory and Self-control Theory

Parenting has been a key construct in many criminological theories. Especially, the social control theory and self-control theory emphasize the importance of parenting on adolescent's delinquency involvement. Hirschi's (1969) social control theory proposes that individual's strong social bond (consisting of attachment, commitment, involvement, and belief) functions as an important inhibition mechanism against deviant behaviors. Adolescents' strong attachment to parents may allow parents to become psychologically present when adolescents are tempted, performing a role of a shield against deviant behaviors (Wright & Cullen, 2001). Many empirical studies showed that adolescents' parental attachment is inversely related with their delinquency involvement (e.g., Parker & Benson, 2004; Rankin & Kern, 1994; Sokol-Katz, Dunham, & Zimmerman, 1997; Wright & Cullen, 2001). Also, the General Theory of Crime (or self-control theory) stresses the importance of parenting, proposing that parenting is the main source of children's 'low self-control', which includes traits that cause antisocial behaviors including crime and delinquency. Gottfredson and Hirschi (1990) claim that children fail to develop self-control, resulting in low self-control, if their parents perform inadequate parenting practices such as lack of attachment, supervision, and punishment.

However, despite the fact that Gottfredson and Hirschi's (1990) self-control theory itself treats parenting as an important exogenous variable for the development of self-control, most previous empirical research on the theory focused on identifying indicators of low self-control and on examining its effects on various behavioral outcomes, rather than paying attention to the examination of

the relationship between parenting and self-control (Perrone et. al., 2004; Cullen et al., 2014). A handful of empirical studies examined the relationship between parenting and self-control, and supported Gottfredson and Hirschi's claim. For example, Perrone et. al. (2004) analyzed the relationships among parental efficacy, self-control, and delinquency by using a nationally representative sample of youth and reported that parental efficacy (a combined measure with attachment, effectiveness in recognizing and responding to problematic behavior) is a significant predictor of youths' level of self control, which 'partially' mediate the effects of parental efficacy on delinquency.

Parenting – Styles

The socialization efforts from parents play an important role in the child's development of conscience (e.g., guilt and empathy), especially since the child must gain the ability to conform to societal standards and restrain antisocial or destructive impulses (Kochanska, 1993). Kochanska's work (1991, 1993, 1995, 1997) found that emotional arousal and temperament was key to the development of conscience. The optimal level of arousal, which is needed for moral socialization, is best realized through the appropriate interaction between the child's temperament and the type of parenting the child receives (Frick & Morris, 2004). Thus, a child with a fearful temperament requires parenting to be gentle, consistent, and non-power-assertive because harsh and power-assertive approaches to parenting will impair conscience development (Kochanska, 1995, 1997).

In the case of a fearless child, a mutual interpersonal orientation between parent and child is especially important (Frick & Morris, 2004) because temperament moderates the association between parenting and conscience development in the child. Therefore, children who lack fearful inhibitions or possess callous unemotional (CU) traits may exhibit undue child effects that disrupt parental attempts at socialization (Frick & Morris, 2004). Although certain temperamental styles make socialization tasks more difficult, such tasks are not rendered impossible because the quality of parental socialization may prove to be more important in determining whether the child will avoid developing an antisocial interpersonal style (Frick, Kimonis, Dandreaux, & Farell, 2003; Frick & Morris, 2004; see also, Larsson, Viding, & Plomin, 2008, p.209).

Perhaps the most influential research on parenting styles comes from the work

of Diana Baumrind (1966, 1991). Baumrind's findings reveal that parents often differ on four important dimensions: (1) Expressions of warmth, (2) Strategies for discipline, (3) Communication, and (4) Expectations for maturity (Baumrind, 1966). Based on these four dimensions, Baumrind (1991) developed four distinct parenting styles that are present prior to adolescence. Permissive parents are more responsive than they are demanding, they are lax on discipline, they do not require mature behavior, and they nurture the child but avoid confrontation. Authoritative parents are demanding yet responsive and their disciplinary methods are supportive rather than punitive. Additionally, authoritative parents set limits and enforce rules; however, they listen to the child and do not restrict the child's autonomy. Also, authoritative parents communicate well, explain the reasons for the discipline, and usually forgive rather than resort to punishment. Conversely, authoritarian parents are demanding, obedience-oriented, set high standards for behavior, strictly punish misconduct, restrict the child's autonomy, and are not responsive. Finally, rejecting-neglecting parents are disengaged from their children and are neither demanding nor responsive. Instead, rejecting-neglecting parents do not provide structure, are not supportive, and neglect their childrearing responsibilities (Baumrind, 1966, 1991).

Authoritative parenting has proven to be successful in preventing children from developing drug use problems as well as generating competence within the child (Baumrind, 1991). As a result, authoritative parenting is a favorable form because it engages the parents so that they are committed with high levels of responsiveness and "demandingness," which creates a healthy balance for the child (Baumrind, 1991, p.62). As such, authoritative parenting could easily be associated with "positive parenting," which has previously been measured with items including parental involvement, positive reinforcement, and consistent discipline (see Frick & Morris, 2004; Shelton, Frick, & Wootton, 1996).

When broader parenting variables (e.g., parental acceptance-involvement, psychological autonomy granted to the child, use of fair discipline, and use of non-physical discipline), which are linked to Baumrind's authoritative parenting style, were included in addition to monitoring-discipline, it was found that the additional parenting factors tripled the amount of variance explained (Hay, 2001). Thus, the context and manner in which parental control is administered is important beyond mere parental monitoring and discipline (Hay, 2001, p.725).

Nevertheless, other studies regarding the effects of parenting and self-control on antisocial behavior among adolescents have conflicting findings. For example, a study found that parental support (i.e., whether the parents are loving, responsive, and involved) failed to reduce antisocial behavior among adolescents who are low in consideration of others (Jones, Cauffman, & Piquero, 2007). This finding is not consistent with previous research (Hay, 2001) that suggests authoritative parenting styles are perhaps more effective in reducing involvement in delinquent acts. Future research should endeavor to incorporate better measures of parenting styles.

Disadvantaged Neighborhoods and Parenting

Elliott Currie (1998) argues that neighborhood structural factors (e.g., poverty, inequality, and social exclusion) influence youth violence indirectly through their impact on the close-in institutions of the family and community by weakening the ability of these institutions to exert informal social controls and provide appropriate levels of social support (see also Colvin & Pauly, 1983; Shihadeh & Steffensmier, 1994). Informal social control, which is generally exercised by significant others, such as families, friends, neighbors, and community networks, involves any sanctions and constraints (i.e., beyond legal, formal, or bureaucratic) used in an effort to control another's behavior, so he or she may conform to social norms (Cullen, 1994).

Cullen (1994) emphasized the importance of family as a main source of social support. Social support refers to perceived or actual instrumental provisions supplied by the community, social networks, and confiding partners. Cullen (1994) argued that as the support a family provides increases, the less likely a youth will engage in crime. Thus, parental expressive support acts as a protective factor capable of reducing the risk of delinquent or criminal involvement (Cullen, 1994). However, family does not exist in a vacuum. Currie (1985) stresses that families are embedded in a larger social context; therefore, what occurs within the family unit cannot be fully separated from forces that are affecting it from the outside. Meta-analytic work also shows that a lack of parental support increases delinquent outcomes, which reveals that child-parent involvement (e.g., intimate communication, sharing activities, and seeking help) is very important (Loeber & Stouthamer-Loeber, 1986). Indeed, Cullen (1994) and Hagan (1994) state that parents are the best source of support; however, high-risk environments may

hinder parents, who strive to provide nurturance, safety, and guidance, from obtaining the opportunities to do so. Currie's (1998) review of the research highlights the following findings: "(1) extreme deprivation inhibits children's intellectual development; (2) extreme deprivation breeds violence by encouraging child abuse and neglect; (3) extreme poverty creates multiple stresses that undermine parents' ability to raise children caringly and effectively; (4) poverty breeds crime by undermining parents' ability to monitor and supervise their children" (p. 135-139).

Thus, when disadvantaged families are living in communities suffering from capital disinvestment processes, the lack of resources and experiences with emotional stress diminish those families' capacity to provide human and social capital (i.e., skills, capabilities, and knowledge acquired by individuals through training, education, and socially structured relationships with individuals and groups) to their children via family processes (Hagan, 1994; Jocson & McLoyd, 2015; Minor, 1993). Indeed, parents, especially mothers, responding to high levels of distress due to chronic economic disadvantage, exhibit harsh disciplinary behavior toward their children that is inconsistent and lacks care, control, and warmth (Arditti et al., 2010; Colvin & Pauly, 1983). Failed socialization efforts by the family reduce or weaken informal social controls and the capacity to provide social support networks for youth (Cullen, 1994; Currie, 1998). Sampson and Laub (1993) suggest "structural context mediated by informal family and school social controls explains delinquency in childhood and adolescence" (p. 7). The weakening of family's ability to instill informal social controls through discipline, supervision, and attachment create the conditions necessary for youth to become involved in delinquency (Sampson & Laub, 1993).

LIMITATIONS OF PREVIOUS RESEARCH AND THE PRESENT STUDY

Previous research on neighborhood effects on delinquency utilized social disorganization theory and tended to focus on neighborhood-level informal social control or collective efficacy as an intervening variable. Relatively few studies have examined the importance of family-level parenting practices as a potential

mediating variable between neighborhood structural characteristics and adolescent delinquency (Cuellar, Jones, & Sterrett, 2015). Only a handful studies investigated mediating effect of parenting between neighborhood disadvantage and delinquency outcomes (e.g., Chung & Steinberg, 2006; Mrug & Windle, 2009; Rankin & Quane, 2002; Tolan et al., 2003). Rankin and Quane (2002) found that increases in community collective efficacy were associated with improved parental supervision, fewer deviant peer affiliations, and lower levels of youthful problem behaviors. Thus, parenting influences mediated the link between collective efficacy and deviance. Similarly, Tolan and colleagues (2003) used longitudinal data to determine if parenting practices mediated the relationship between neighborhood effects on gang affiliation and violent offending. They found that ineffective parenting mediated the relationship between neighborhood structural characteristics and gang membership (Tolan et al., 2003). Chung and Steinberg (2006) also found that neighborhood disorganization was indirectly related to higher levels of juvenile offending by way of ineffective parenting practices and exposure to deviant peer affiliations. Additionally, Mrug and Windle (2009) reported that the effect of neighborhood disadvantage on children's externalizing behavior is fully mediated by neighborhood social process and parenting qualities. Those studies have provided very important insights, however, their findings may suffer from a certain degree of generalizability issue mainly due to the use of a limited sample, such as African-American youths (e.g., Mrug & Windle, 2009; Rankin & Quane, 2002), urban males (e.g., Tolan et al. 2003), or serious juvenile offenders from urban cities (e.g., Chung & Steinburg, 2006). Thus, the findings need to be cautiously interpreted.

The current study aims to improve on previous research by examining a mediating effect of parenting practices between neighborhood characteristics and juvenile delinquency with a nationally representative sample of adolescents and their neighborhoods from the National Longitudinal Study of Adolescent Health (Add-Health study). More specifically, this investigation examines whether or not parenting practices (1) are affected by neighborhood structural characteristics, (2) more importantly, mediate the effects of neighborhood disadvantage on delinquency, and (3) have independent effects on delinquency even after controlling for low self-control and other developmental outcomes.

METHOD

Data

The present study utilized information from 'in-home interviews' during Wave-1 (1994-1995) of the National Longitudinal Study of Adolescents (Add-Health). Add-Health is one of the most comprehensive longitudinal study of adolescents which consists of information gathered from various sources, such as 'In-school questionnaire', 'In-home interviews', 'Parent questionnaire', 'School administrator questionnaire', and 'Contextual data' (Harris, Halpern, Whitsel, Hussey, Tabor, Entzel, & Udry, 2009). The ADD-Health consists of over 90,000 students from a stratified sample of 80 high schools and their 52 feeder schools (Junior high or middle school). From among those students, a core sample was produced by selecting students based on stratification (by grade and sex) in each school. The 'in-home interviews' dataset includes a core sample of 12,604 students in grades 7-12 (mostly between 12 and 18 years old). However, this study employed the 'public-use dataset', which consists of a sub-sample of 6,504 students. Use of the public-use data would not undermine the validity of the findings, since it consists of a randomly selected one-half of the original sample, which is classified as a 'restricted-use data' to which researchers have a limited access only by contractual agreement. Although the ADD Health data is somewhat old, it best serves the purposes of the present study since it is one of few data sets with a nationally representative sample that contain information for both adolescents' individual characteristics and their neighborhood-related characteristics. This study utilized a cross-sectional analysis approach with delinquency of only Wave_1 as the dependent variable because the analysis with the delinquency of Wave_2 substantially reduced the number of case that contains information on delinquency (from 6,415 cases for Wave_1 to 4,786 cases for Wave_II).

Delinquency

Adolescents' self-reported delinquency was measured with a 10-item index including 4-violent delinquency questions and 6-property delinquency questions. The types of delinquent behaviors covered in this study include serious physical fight, hurting someone, use or threat to use a weapon, group fights, damaging

property, and different types of stealing. Each delinquency item was measured with a four-point scale (0:never ~ 3:5 or more times), and the sum of all 10-responses was used as an overall count of delinquent behavior. The reliability coefficient of Cronbach's Alpha is a=.797.

Parenting Practices

Previous studies on parenting employed different dimensions of parenting practices/behaviors. For example, Chung and Steinberg (2006) measured three dimension of parenting behaviors: warmth, knowledge, and monitoring; Mrug and Windle (2009) measured parental nurturance and harsh/inconsistent punishment to reflect parenting; Rankin and Quane (2002) used parental monitoring; and Tolan et al. (2003) included four dimensions for parenting practices: positive parenting, discipline effectiveness, avoidance of discipline, and extent of involvement.

Based on the commonly appeared dimensions of parenting from previous studies, the present study measured four parenting dimensions using adolescents' perceptions on their parents' behaviors. The first dimension was parents' availability/ability to control/supervise (will be called 'Control/Supervision' hereafter) their children at home, which closely emulates the monitoring dimension used in previous studies. This dimension was measured with six questions (3 for mom and 3 for dad) regarding whether their parents are at home when respondents leave for school, return from school, and go to bed. Each item was measured with five-point scale (1:never ~5:always). Responses were summed to indicate parents' overall availability/ability to control/supervise their children. The overall score ranges from 6 to 30, indicating that higher values reflect higher 'control/supervision' capabilities.

The second dimension is the level of 'shared activities' between parents and adolescents, which reflects the extent of involvement dimension. Shared activities include gone shopping, played a sport, gone to a religious service, gone to a movie/play/museum/concert/sport events, and worked on a project for school. Originally, each item was measured with a dichotomous response (0:no ~1:yes), and all 10-responses (5 for mom and 5 for dad) were summed to create an overall level of shared-activities, ranging from 0 to 10. 'Conversation/Communication' level is the third dimension and it reflects parents' knowledge about their children. It was measured with 8 questions (4 for mom and 4 for dad) with a

dichotomized response (0:no ~ 1:yes) regarding whether the respondents talked with parents about their friends, personal problems, and school-related issues. The possible maximum score is 8 if two parents raised an adolescent and it is 4 if a single parent (mom or dad) raised an adolescent. Higher scores reflect parents' higher level of communication/conversation with children meaning better knowledge about their children. The fourth and last dimension is the 'attachment' between parents and respondents. This dimension reflects the dimensions of warmth or nurturance from previous studies. The questions include whether the respondents feel close to their parents, are satisfied with their relationship with parents, and think their parents care about them (1:Strongly disagree ~ 5:strongly agree). All 10 responses (5 for mom and 5 for dad) were added and higher values indicate strong attachment between parents and children.

Proximal Indicator of Low Self-control and Other Developmental Outcomes

Parenting is known to be an important source of adolescents' various developmental outcomes. Therefore, the present study incorporated developmental outcomes of parenting to investigate if (or how) they play roles within the links among neighborhood disadvantage, parenting practices, and delinquency.

According to Gottfredson and Hirschi (1990), parenting is the main source of low self-control. In this study, 'impulsivity' was measured as a proximal indicator of low self-control with an index of 5 items that reflects respondents' decision-making style and behavioral pattern. Examples of the items include "When making decisions, you usually go with your "gut feeling" without thinking too much about consequences of each alternative", "When you have a problem to solve, one of the first things you do is get as many facts about the problem as possible", and so on. Each item was measured with a five-point scale (1:strongly disagree ~ 5:strongly agree) and each response was recoded so that higher score can reflect higher impulsivity.

Previous research also found that parenting produces other developmental outcomes such as adolescents' academic performance (Anunola, Stattin, & Nurmi, 2000; Juang & Silbereisen, 2002; Park & Bauer, 2002) and self esteem (Bulanda & Majumdar, 2008). The present study measured 'academic performance' with a composite measure of GPA (with grades of English, Science, Mathematics, and Social studies). Each grade was measured with a four-point scale (1:D or lower ~

4:A). Lastly, 'self esteem' was measured with a seven-item index regarding respondents' self-evaluations on various aspects about themselves (score ranges from 7 to 35). Examples of questions are "You have a lot of good qualities (1:strongly disagree ~ 5:strongly agree)", "You have a lot to be proud of", and so on. Demographic variables such as sex (0:female, 1:male), race (White, Black, other) and age are also included.

Neighborhood Disadvantage

The 'neighborhood disadvantage' of each neighborhood where the respondents lived was measured by combining 6 structural characteristics such as racial heterogeneity, residential mobility, median household income, proportion living under poverty, unemployment rate, and modal education level. Indicators were recoded, standardized, and summed in a way that a higher value indicates a higher cumulative neighborhood disadvantage. The reliability coefficient of Cronbach's Alpha for the cumulative neighborhood disadvantage is a=.693. Descriptive summary of the variables is presented in Table_1.

Table 1. Descriptive Statistics

		N	%	Mean	Sd
Gender	Female (0)	3356	51.6		
	Male (1)	3147	48.4		
Race	Whites (0)	4291	66		
	Blacks (1)	1601	24.6		
	Others (2)	612	9.4		
Age				15.04	1.773
Delinquency		6415		2.16	3.41
School Performance				11.37	2.994
Impulsivity				11.75	2.837
Self-Esteem				28.66	4.07
Parenting Practices	Control/Supervision			18.25	6.242
	Shared Activities			2.81	1.729
	Conversation/ Communication			3.37	1.811
	Attachment			36.43	11.425
Neighborhood Disadvantage				0.022	2.523

Analytical Strategy

Several analytical techniques were employed. First, bivariate correlation analyses were used to find whether neighborhood disadvantage, parenting practices, adolescents' developmental outcomes (impulsivity, school performance and self esteem), and delinquency are significantly related with each other. Second, OLS multiple regression analyses with parenting practices as dependent variables were performed to examine whether parenting practices are affected by neighborhood disadvantage and adolescents' developmental outcomes. Third, a series of Negative Binomial (NB) regression analyses were conducted to examine whether parental practices mediate the effect of neighborhood disadvantage on adolescent delinquency. A negative binomial (NB) regression model was utilized because delinquency was measured with four discrete categories of count and the

delinquency count has an issue of 'overdispersion' in which the mean is not equal to the variance, showing a high frequency of zero delinquency followed by a rapid decrease in frequencies of subsequent delinquency counts. Despite the high frequency of zero delinquency, the zero-inflated negative binomial (ZINB) regression model was not utilized both because the difference between 'observed' and 'expected' count of zero delinquency was not substantially large (2,908 and 2,797, respectively) and because the use of ZINB regression would make the interpretation of the findings unnecesarily more complicated although the preliminary analyses with ZINB showed very similar findings to those of NB (Hilbe, 2007; Land, McCall, & Nagin, 1996; Long, 1997).

The negative binomial regression model with a log link function was expressed with the following equations with which the log of the outcome is predicted with the variables included (Cameron & Trivedi, 1998). Model_1 includes only respondents' demographic control variables and neighborhood disadvantage as the basic model.

Model_1.

$$\log(Y/\text{Delinquency}) = \alpha + \beta 1(\text{Age}) + \beta 2(\text{Male}) + \beta 3(\text{Blacks}) + \beta 4(\text{Others}) + \beta 5(\text{Neighborhood Disadvantage})$$

Model_2 adds four parenting practices to Model_1 to examine whether parenting practices mediate the effect of neighborhood disadvantage on delinquency. If the effect of neighborhood disadvantage on delinquency is significantly reduced after the parenting variables are included, then it suggests that parenting practices have a mediation effect between neighborhood disadvantage and delinquency.

Model_2.

$$\log(Y/\text{Delinquency}) = \alpha + \beta 1(\text{Age}) + \beta 2(\text{Male}) + \beta 3(\text{Blacks}) + \beta 4(\text{Others}) + \beta 5(\text{Neighborhood Disadvantage}) + \beta 6(\text{Control/Supervision}) + \beta 7(\text{Shared activities}) + \beta 8(\text{Conversation/Communication}) + \beta 9(\text{Attachment})$$

Model_3 is used to investigate the nature of the effects of the parenting practices. A comparison between Model_2 and _3 would suggest if parenting practices have direct effects on delinquency or their effects on delinquency are mediated through low self-control and/or other developmental outcomes.

Model_3.

$$\log(Y/\text{Delinquency}) = \alpha + \beta1(\text{Age}) + \beta2(\text{Male}) + \beta3(\text{Blacks}) + \beta4(\text{Others}) + \beta5(\text{Neighborhood Disadvantage}) + \beta6(\text{Control/Supervision}) + \beta7(\text{Shared activities}) + \beta8(\text{Conversation/Communication}) + \beta9(\text{Attachment}) + \beta10(\text{Impulsivity}) + \beta11(\text{Academic performance}) + \beta12(\text{Self-Esteem})$$

RESULTS

Correlations among Variables

The results of correlation analyses are presented in Tables_2. Delinquency was significantly related to all independent variables. As social disorganization theory suggests, neighborhood disadvantage had a significant positive correlation with adolescent delinquency ($r=.05$, $p<.001$), meaning that adolescents from more structurally disadvantaged neighborhoods reported higher delinquency involvement.

All four parenting practices had significant, negative correlations with adolescents' delinquency: control/supervision ($r=-.12$, $p<.001$), shared activities ($r=-.11$, $p<.001$), Conversation/Communication ($r=-.08$, $p<.001$), and Attachment ($r=-.17$, $p<.001$). This means that the more parents have effective parenting practices - being more available/able to control/supervise through being at home at certain time of a day, sharing more activities together, communicating more, or developing attachment - the less adolescents would get involved in delinquency. In addition, each of the four parenting practices had significant, positive relationships with each other, suggesting that parents with one dimension of effective parenting are more likely to have other effective dimensions, too. More importantly, all four parenting practices had significant, negative correlations with neighborhood disadvantage: control/supervision ($r=-.09$, $p<.001$), shared activities ($r=-.11$, $p<.001$), conversation/communication ($r=-.11$, $p<.001$), and

attachment (r=-.18, p<.001). Parents who lived in structurally more disadvantaged neighborhoods showed lower levels of being available to control/supervise, of sharing activities, of conversation/communication, and of attachment.

Delinquency was positively associated with impulsivity (r=.17, p<.001) as the self-control theory suggests (Goffredson & Hirschi, 1990), but it was negatively related to academic performance (r=-.25, p<.001) and self-esteem (r=-.13, p<.001). Further, parenting practices and individual developmental outcomes showed significant relationships with expected directions: Impulsivity had significant, negative relationships with all four parenting practices meaning that higher parenting practices are associated with low impulsivity; and school performance and self-esteem had significant, positive relationships with parenting practices. Also, impulsivity, school performance, and self-esteem were significantly correlated with each other with expected directions.

Table 2. Correlations among Variables

	1	2	3	4	5	6	7	8
1. Delinquency	1.00							
2. Neighborhood Disadvantage	.05							
3. Control/Supervision	-.12	-.09						
4. Shared activities	-.11	-.11	.25					
5. Conversation/ Communication	-.08	-.11	.25	.31				
6. Attachment	-.17	-.18	.66	.41	.40			
7. Impulsivity	.17	-.03 *	-.03 *	-.09	-.11	-.08		
8. School Performance	-.25	-.13	.10	.23	.18	.21	-.16	
9. Self Esteem	-.13	.00 ns	.08	.17	.12	.25	-.27	.14

Note: All correlations were significant at p<.001, except for *:p<.05, ns: p>.05

In order to further investigate if and how a certain specific neighborhood structural characteristic is related to parenting practices, additional correlation analyses were performed between each of neighborhood characteristics and parental practices. The findings are presented in Table_3. Racial heterogeneity, proportion living under poverty, and unemployment rate had significant, negative correlations with each of the parenting practices, whereas median household income and modal education level had significant, positive correlations. However, residential mobility was not significantly correlated with parenting practices.

Table 3. Correlations between Neighborhoods Characteristics and Parenting Practices

	Control/ Supervision	Shared Activity	Conversation/ Communication	Attachment
Racial Heterogeneity	-0.065 *	-0.073 ***	-0.087 ***	-0.124 ***
Residential Mobility	-0.012 *ns*	0.003 *ns*	-0.005 *ns*	-0.009 *ns*
Median household Income	0.059 ***	0.109 ***	0.100 ***	0.154 ***
% under Poverty	-0.064 ***	-0.095 ***	-0.092 ***	-0.170 ***
Unemployment rate	-0.080 ***	-0.091 ***	-0.081 ***	-0.153 ***
Modal Education Level	0.024 ***	0.068 ***	0.063 ***	0.101 ***
Neighborhood Disadvantage	**-0.089** ***	**-0.105** ***	**-0.110** ***	**-0.183** ***

*: p<.05, ***: p<.001, ns: p>.05

Effects of Neighborhood Disadvantage on Parenting Practices

One important purpose of the present study is to examine whether parenting practices are affected by neighborhood structural characteristics. Given the facts that neighborhood disadvantage, parenting practices, and adolescents' developmental outcomes are significantly inter-correlated in Table_2, parents' ability to utilize different parenting practices may be a function of both neighborhood disadvantage and adolescents' individual characteristics. Therefore, it is necessary to examine if neighborhood disadvantage has an independent effect above and beyond the effects of adolescents' individual characteristics on parenting practices. Multiple regression analyses with each of the parenting practices as a dependent variable were performed to examine if the effects of neighborhood disadvantage on parenting practices are significant even after controlling for three developmental outcomes and demographic control variables. Results are presented in Table_4. Age had a positive association with parent's availability for control/supervision (b=.123, p<.05) and conversation/communication (b=.131, p<.001) controlling for other variables, but a negative association with shared activities (b=-.151, p<.001) and attachment (b=-.329, p<.001). No significant gender differences in parenting practices were found, except for conversation/communication. Males reported a have lower level of conversation/communication with parents (b=-.327, p<.001) controlling for other variables. Black adolescents showed lower levels than white adolescents of control/supervision (b=-2.271, p<.001), shared activities (b=-.263,

p<.001), conversation/communication (b=-.443, p<.001), and attachment (b=-5.189, p<.001), and adolescents in other racial groups showed significantly lower levels of parenting practices as well, except for control/supervision (b=-.0283, p>.05). In addition, school performance and self-esteem had positive associations with each of the parenting practices, while impulsivity had no significant relationships with parenting practices.

It is important to note that neighborhood disadvantage had significant associations with three of four parenting practices after controlling for adolescents' impulsivity, school performance and self-esteem: shared activities (b=-.028, p<.001), communication(b=-.029, p<.001), and attachment (b=-.364, p<.001). Although neighborhood disadvantage was not significantly associated with parents' availability for control/supervision (b=-.119, p<.001), the general findings may suggest that different parenting practices are indeed a function of neighborhood disadvantage.

Table 4. Regression Analyses for the Effects of Neighborhood Disadvantage on Parenting Practices

	Control/ Supervision		Shared Activities		Conversation/ Communication		Attachment	
	B	SE	B	SE	B	SE	B	SE
Intercept	12.153	*1.356* ***	*2.645*	*0.395* ***	*-0.275*	*0.405* ns	18.29	*2.292* ***
Age	0.123	*0.055* *	*-0.151*	*0.016* ***	*0.131*	*0.016* ***	-0.329	*0.093* ***
Sex								
Female								
Male	0.134	*0.190* ns	*-0.053*	*0.055* ns	*-0.327*	*0.057* ***	0.508	*0.323* ns
Race								
Whites								
Blacks	-2.271	*0.230* ***	*-0.263*	*0.066* ***	*-0.443*	*0.068* ***	-5.189	*0.388* ***
Others	-0.283	*0.331* ns	*-0.186*	*0.095* *	*-0.212*	*0.099* *	-1.099	*0.559* *
Impulsivity	-0.008	*0.034* ns	*-0.028*	*0.010* **	*-0.035*	*0.010* ***	-0.059	*0.058* ns
School performance	0.138	*0.033* ***	*0.109*	*0.009* ***	*0.072*	*0.010* ***	0.508	*0.055* ***
Self-Esteem	0.122	*0.025* ***	*0.055*	*0.007* ***	*0.056*	*0.007* ***	0.676	*0.042* ***
Neighborhood Disadvantage	-0.055	*0.029* ns	*-0.028*	*0.008* ***	*-0.029*	*0.009* ***	-0.364	*0.050* ***
R-Square		*0.041* ***		*0.101* ***		*0.080* ***		*0.156* ***
		df=4,431		df=4,040		df=4,005		df=4,552

:p<.01;*:p<.001;*ns*:p>.05

*(*): close to p<.01; **(*): close to p<.001

Mediating Effect of Parenting Practices

The principal purpose of this study is to examine whether parenting practices mediate (or intervene) the effect of neighborhood structural characteristics on delinquency. Three Negative Binomial (NB) regression analyses were performed. First model included only respondents' demographic variables and neighborhood disadvantage to serve as a basic model. Model_1 in table_5 shows that males had a high delinquency involvement than females (b=.651, p<.001). There was no significant difference in delinquency between white and black adolescents (b=.042, p>.05), whereas youths in other racial groups reported a significantly higher delinquency involvement than white adolescents (b=.195, p<.001), after controlling for other variables. As expected, neighborhood disadvantage had a significantly positive association with delinquency (b=.013, p<.001). The NB regression coefficient of b=.013 is equivalent to an odds ratio of 1.013 which means that one-unit increase in neighborhood disadvantage increases the odds of delinquent behavior by 1.013 times. Similar interpretation can be applied to all other NB coefficients.

Model_2 shows that three parenting practices had significant effects on delinquency. Shared activities (b=-.075, p<.001) and attachment (b=-.022, p<.001) produced significant negative associations with delinquency. An interesting result is that the level of conversation/communication between parents and adolescents had a positive association with delinquency (b=.039, p<.01) after controlling for other variables, despite the negative bivariate correlation between the two (r=-.08, p<.001). This finding is not surprising or unusual, however. The variable measures level of conversation between parents and respondents about friends and school-related aspects. Therefore, parents are more likely to have conversation with their children who exhibited signs of problems, resulted in a positive association after controlling for other parenting variables. Although control/supervision and delinquency showed a significant 'bivariate' correlation (r=-.12, p<.001) in table_2, its effect on delinquency became insignificant (b=-.0004, p>.05) when other parenting variables are included in the model. This finding suggests that when parents perform other positive parenting practices, their being at home at certain time of a day may not be an important factor for their children's delinquency. More importantly, Model_2 is used to investigate whether parenting practices

mediate the effect of neighborhood disadvantage on delinquency and the results support that there may be a mediating effect of parenting practices. The significant effect of neighborhood disadvantage on delinquency (b=.013, p<.001) in Model_1 became 'insignificant' after four parenting practices were added (b=-.003, p>.05). A comparison of chi-square values indicates that the addition of parenting practice variables (Model_2) significantly improved the model fit.

Adolescents might develop low self-control and other developmental outcomes as the consequence of parenting practices and it is possible that those variables might mediate the effects of parenting practices on delinquency. Therefore, based on the significant correlations between parenting practices and individual developmental outcomes (Table_2), Model_3 was used to investigate whether parenting practices have direct independent effects on delinquency or whether their effects are mediated through adolescent's developmental outcomes, such as impulsivity, academic performance, or self-esteem. The results show that, while controlling for other variables, impulsivity (b=.074, p<.001) had a significant positive relationship with delinquency as the self-control theory suggests (Gottfredson and Hirschi,1990). Also, school performance (b=-.1, p<.001) and self-esteem (b=-.017, p<.01) showed significant positive effects on delinquency as expected. Importantly, even after controlling for adolescents' impulsivity, school performance and self-esteem, the significant effects of three parenting practices on delinquency remained significant: control/supervision (b=-.004, p>.05), shared activities (b=-.034, p<.05), communication (b=.060, p<.001), and attachment (b=-.016, p<.001). It suggests that parenting practices, while mediating the effect of neighborhood disadvantage on delinquency, exert direct effects on delinquency above and beyond their indirect effects through individual developmental outcomes. And, the addition of individual developmental outcomes (Model_3) significantly improved the model fit.

Table 5. Negative Binomial Regression Analyses with Delinquency as a Dependent Variable

	Model1			Model2			Model3		
	B	SE	Odds Ratio	B	SE	Odds Ratio	B	SE	Odds Ratio
Intercept	0.960	0.1418	2.612 ***	2.509	0.1909	12.287 ***	2.669	0.3194	14.424 ***
Age	-0.039	0.0094	0.962 ***	-0.087	0.0117	0.916 ***	-0.080	0.0140	0.923 ***
Sex									
Female									
Male	0.651	0.0316	1.917 ***	0.757	0.0380	2.132 ***	0.692	0.0459	1.997 ***
Race									
Whites									
Blacks	0.042	0.0383	1.043 ns	0.005	0.0467	1.005 ns	0.073	0.0551	1.076 ns
Others	0.195	0.0537	1.215 ***	0.190	0.0643	1.209 **	0.202	0.0771	1.224 **
Neighborhood Disadvantage	0.013	0.0049	1.013 ***	-0.003	0.0059	0.997 ns	-0.013	0.0070	0.987 ns
Parenting practices									
Control/Supervision				-0.004	0.0040	0.996 ns	-0.004	0.0047	0.996 ns
Shared activities				-0.075	0.0123	0.928 ***	-0.034	0.0141	0.966 *
Conversation/ Communication				0.039	0.0115	1.039 **	0.060	0.0134	1.062 ***
Attachment				-0.022	0.0025	0.978 ***	-0.016	0.0030	0.984 ***
Impulsivity							0.074	0.0077	1.077 ***
School Performance							-0.096	0.0079	0.908 ***
Self-Esteem							-0.017	0.0060	0.983 **
Chi-Square	df=5		448.5 ***	df=9		645.0 ***	df=12		797.0 ***
Log Likelihood	-11821.4			-8291.9			-6160.4		
AIC	23654.8			16603.8			12346.8		
BIC	23695.1			16667.9			12426.7		

:p<.01;:p<.001;ns:p>.05*

SUMMARY AND DISCUSSION

According to recent research on the contextual effects of neighborhood, structural characteristics of neighborhoods have indirect effects on delinquency through the intervening concept of social disorganization or collective efficacy (Bernburg & Thorlindsson, 2007; Elliott et al., 1996; Fagan & Wright, 2012; Morenoff et al., 2001; Sampson, 2006; Sampson et al., 2005; Zimmerman, 2010). However, the relatively weak explanatory power of the neighborhood-level social disorganization or collective efficacy on individual-level delinquency may suggest that a more proximal unit or process needs to be incorporated for better explanations of neighborhood effects on adolescent delinquency. The present study focused on 'parenting practices' to examine whether or not (1) neighborhood structural characteristics affect parenting practices, (2) parenting practices mediate the effect of neighborhood disadvantage on adolescents' delinquency involvement, and (3) parenting practices have significant direct effects on delinquency even after controlling for adolescents' low self-control and other developmental outcomes.

The analyses produced several important findings that need to be addressed. First, neighborhood disadvantage, which is a composite measure of several indicators of neighborhood structural characteristics, has a significant association with adolescent delinquency, as social disorganization theory suggests (Shaw & McKay, 1942 & 1969). Adolescents from neighborhoods that have higher poverty, racial heterogeneity, residential mobility, unemployment rate, or lower median income or education level, reported higher delinquency involvement. Second, adolescents whose parents exhibited lower levels of availability to control/supervise, lower levels of shared activities together, of conversation, and lower levels of attachment, showed higher levels of delinquency. These findings are consistent with previous research on the effects of parenting on various outcomes of adolescents (Anunola et. al., 2000; Aquilino & Supple, 2001; Bulanda & Majumdar, 2008; Juang & Silbereisen, 2002; Park & Bauer, 2002; Mowen & Schroeder, 2015; Schroeder & Mowen, 2014; Shakya et. al., 2012). Also, parents' parenting practices are significantly associated with adolescents' impulsivity (an indicator of low self-control) and other developmental outcomes,

such as school performance and self-esteem.

The important goal of the present study was to examine whether parenting practices mediate the effect of neighborhood disadvantage on delinquency. In order to address this, this study first examined whether or not neighborhood disadvantage is significantly associated with parenting practices. The analyses revealed that neighborhood disadvantage has significant correlations with all four parenting practices. Adolescents who live in more disadvantaged neighborhoods are more likely to report lower levels of availability for control/supervision, of shared activities, of conversation/communication, and of attachment. This finding, in general, is consistent with previous studies on parenting, which reveal that parents from disadvantaged neighborhoods utilized more punitive discipline, perform looser supervision, and so on (Arditti et al., 2010; Kerstenburg et al., 1994; Furstenburg, 1993; Kohen et al., 2008; Zuberi, 2016).

The more significant findings came from the model comparisons to predict delinquency involvement. Neighborhood disadvantage had a significant association with delinquency in a basic model but lost its significance when four parenting practices were introduced. This indicates that parenting may work as a mediating factor between neighborhood disadvantage and delinquency. Furthermore, the significant associations of parenting practices with delinquency remained significant even after controlling for an indicator of low self-control (impulsivity) and other developmental outcomes (school performance and self-esteem), indicating that parenting practices have significant independent direct effects on delinquency above and beyond their effects through other developmental outcomes.

Such findings described above may provide some important implications to the criminological theories. Social disorganization theory suggests that disadvantageous neighborhood structures affect adolescent delinquency through social disorganization or weakened collective efficacy. While previous research on the theory succeeded to persuade that neighborhood-level social disorganization/collective efficacy is an essential variable that intervenes the relationship between neighborhood structures and delinquency (Morenoff et al., 2001; Sampson, 2006; Sampson et al., 2005), empirical research findings on parenting suggest that family-level parental practices would be another important candidate as a mediator (Chung & Steinburg, 2006; Mrug & Windle, 2009; Rankin & Quane, 2002; Tolan et al., 2003). Thus, findings of the present study suggest (1) that parents may take certain parenting

practices as a reaction to or a consequence of certain neighborhood structures, and (2) that there may be a causal chain-process among neighborhood disadvantage, parenting practices, and delinquency: neighborhood disadvantage affects ineffective parenting practices, and ineffective parenting practices lead to adolescent delinquency. Or, at least, neighborhood disadvantage and ineffective parenting practices are associated maybe due to ineffective neighborhood-level collective efficacy (based on an assumption, not measured directly in this study). In other words, ineffective parenting in disadvantaged neighborhoods could be a function of weak neighborhood-level collective efficacy rather than direct effects of neighborhood structures. Such findings (and the assumed relationships) of the present study might imply that the research on social disorganization or collective efficacy can be expanded by incorporating parenting as a closer or a more proximal source of influence in the link between neighborhood structures/collective efficacy and adolescent delinquency, such that neighborhood disadvantage affects low collective efficacy which influences ineffective parenting, which in turn leads to delinquency.

The results may provide some significant implications to the General Theory of Crime, too. Gottfredson and Hirschi (1990) argue that inadequate parenting - such as a lack of proper attachment, supervision, and punishment - results in youth having low levels of self-control that will result in increased delinquency. However, the theory utilizes parenting primarily as an exogenous variable for low self-control without explaining internal or external factors that affect parenting itself (Cullen, Agnew, & Wilcox, 2014; Muftic & Updegrove, 2018), and most previous research on the self-control theory have focused only on identifying the elements of low self-control and/or on the causal relationship between low self-control and delinquency (see, Evans, Cullen, Burton, Dunaway, & Benson, 1997; Pratt & Cullen, 2000; Zimmerman, et al., 2015) without examining the effects of parenting itself on self-control and delinquency or without identifying the factors that affect parenting itself. Such factors may include either parents' or children's individual characteristics such as temperaments or personality (e.g., Kochanska, Friesonborg, Lange, & Martel, 2004), or external influences such as neighborhood structures (e.g., Pinderhughes, Nix, Foster, Jones, & the conduct problems prevention research groups, 2001; Zuberi, 2016). The significant associations between neighborhood disadvantage and parenting practices indicate that one crucial source of parenting that produces children's low self-control and

delinquency would be neighborhood structures. Therefore, the present study implies that incorporating 'parenting' and/or 'neighborhood context' as the exogenous explanatory variables in the link between low self-control and delinquency can expand research on self-control theory. The implications of the present study for both social disorganization theory and self-control theory would suggest further that both theories can be integrated by utilizing a common concept: parenting.

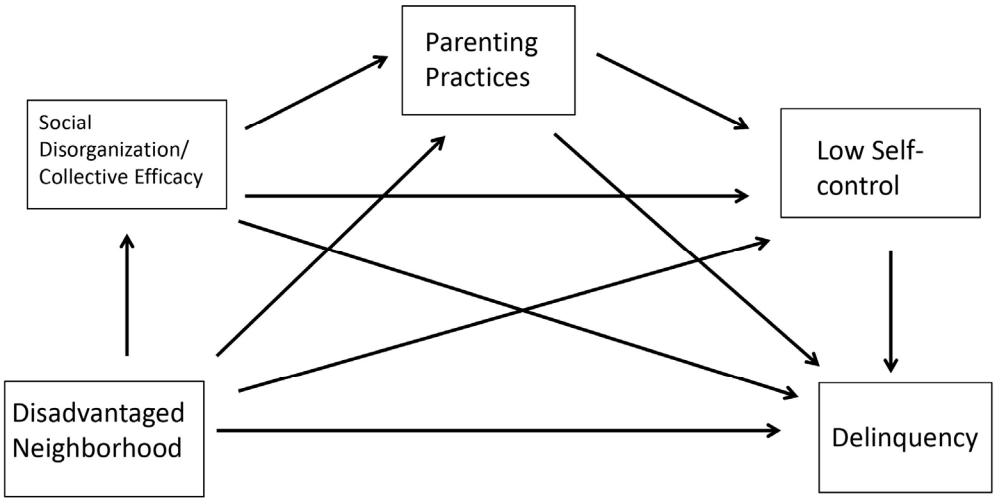

Figure 1. A Hypothetical Integration Model of Social-disorganization and Self-control

Limitations and Suggestions for Future Research

This study can be highlighted with some strengths and limitations. The biggest strength is that it adopted a broader scope to understand a more complete mechanism in which neighborhood structural characteristics, parenting practices, adolescents' low self-control, and delinquency are interrelated. Although there have been an abundance of studies that addressed the issues regarding the relationships among those variables, most previous research employed a somewhat weak approach with respect to model specifications, target adolescent samples, neighborhood contexts, and so on.

The present study addresses such limitations of previous research by using a nationally representative sample of adolescents and their neighborhoods, and by incorporating neighborhood characteristics, parenting practices, low self-control/other developmental outcomes, and delinquency in a single study simultaneously to

provide more complete understandings about the relationships among those variables.

However, there are also some limitations that need to be addressed. The first limitation is related to the inference of the causal relationships among neighborhood structure, parenting practices, low self-control, and delinquency. Although there are significant associations among the variables and it is more natural to assume that neighborhood disadvantage affects parenting practices rather than assuming parenting practices affect neighborhood disadvantage, the cross-sectional nature of the present study has a limitation in making a definite conclusion about the causal inference.

The second limitation comes from the fact that the 'public-use' version of ADD-Health data was utilized. Although this dataset provides neighborhood structural characteristics for each respondent, it does not provide a geo-code of each neighborhood. This means that the present study could not utilize a multi-level approach to examine the contextual effects of neighborhood disadvantage on delinquency. This study took a perspective of mediating role of parenting practices between neighborhood disadvantage and delinquency. However, it is also possible that neighborhood disadvantage may moderate or contextualize the effects of parenting on delinquency, or vice versa. Examining the relationships with a different perspective would provide alternative ways to understand the nature of these associations. The third limitation is the lack of information on the parents' individual characteristics. Although neighborhoods exert significant influence on parenting practices, parents' ability to employ effective parenting could also be a function of their individual characteristics, such as socioeconomic status, temperament, personality, criminality, substance abuse, and so on. Therefore, additional research with those variables would provide more complete explanations about the relationships.

CONCLUSION

This study does not try to undermine the importance of neighborhood-level social organization or collective efficacy. Rather it might emphasize the importance of supplementary functions of parenting practices. It would not be easy to change social structure itself or to establish strong collective efficacy of the neighborhoods in a short period of time. Instead, it may take enormous time, efforts, and resources. Although findings suggest that neighborhood disadvantage affects ineffective parental practices and delinquency, it also implies that the effects of neighborhood disadvantage on delinquency can be minimized if parents can develop more effective and positive parenting skills. Therefore, it would be very important to develop and implement education programs for effective parenting as a relatively easier way to reduce delinquency in more disadvantaged neighborhoods. Improving the parenting skills of more and more families/parents in the neighborhoods, in the long run, could serve as a basis for the strong neighborhood-level collective efficacy. This means that in case some parents failed to provide effective parenting practices, their children may be discouraged to commit delinquency by other parents in the neighborhood who are equipped with effective parenting practices. Although the present study recommends parenting-based programs as a relatively easier and more immediate approach to reduce/prevent delinquency for adolescents who live in more disadvantaged neighborhoods, a more fundamental approach for delinquency prevention should be the development/implementation of policies that aim to improve general social structural conditions of neighborhoods (e.g., poverty and concentrated disadvantage) and larger social contexts (e.g., social inequalities produced by stratified economic, legal, political, and cultural systems).

References

Aquilino, W.S., & Supple, A.J. (2001). Long-term effects of parenting practices during adolescence on well-being outcomes in young adulthood. *Journal of Family Issues, 22*: 289-308. doi: 10.1177/019251301022003002

Arditti, J., Burton, L., & Neeves-Botelho, S. (2010). Maternal distress and parenting in the context of cumulative disadvantage. *Family Process, 49*: 142-164. doi: 10.1111/j.1545-5300.2010.01315.x

Aunola, K., Stattin, H., & Nurmi, J.E. (2000). Parenting styles and adolescents' achievement strategies. *Journal of Adolescence, 23*: 205-222. doi: 10.1006/jado.2000.0308

Baumrind, D. (1966). Effects of authoritative parental control on child behavior. *Child Development*, 37: 887-907. doi: 10.2307/1126611

Baumrind, D. (1991). The influence of parenting style on adolescent competence and substance use. *Journal of Early Adolescence*, 11(1): 56-95. doi: 10.1177/0272431691111004

Bellair, P. E. (1997). Social interaction and community crime: Examining the importance of neighborhood networks. *Criminology, 35*: 677-703. doi: 10.1111/j.1745-9125.1997.tb01235.x

Bernburg, J., & Thorlindsson. (2007). Community structure and adolescent delinquency in Iceland: A contextual analysis. *Criminology, 45(2)*: 415-444. doi: 10.1111/j.1745-9125.2007.00083.x

Beyer, J.M., Bates, J.E., Petit, G.S., & Dodge, K.A. (2003). Neighborhood structure, parenting processes, and development of youths' externalizing behaviors: A multilevel analysis. *American Journal of Community Psychology, 31*: 33-53. doi: 10.1023/A:1023018502759

Bulanda, R.E., & Majumdar, D. (2008). Perceived parent-child relations and adolescent self-esteem. Journal of child & Family Studies, 18: 203-212. doi: 10.1007/s10826-008-9220-3

Bursik, R. J. Jr. (1984). Urban dynamics and ecological studies of delinquency. Social Forces, 63: 393-413. doi: 10.1093/sf/63.2.393

Bursik, R. J. Jr. (1986). Ecological stability and the dynamics of delinquency. In Albert J. Reiss, Jr., and Michael Tonry (Eds.), Communities and Crime. Chicago: University of Chicago Press.

Bursik, R. J., & Webb, J. (1982). Community change and patterns of delinquency. *American Journal of Sociology, 88(1)*: 24-42.

Cameron, A. C. and Trivedi, P. K. 1998. *Regression Analysis of Count Data*. New York: Cambridge Press.

Chesney-Lind, M. & Pasko, L. (2004). *The Female Offender: Girls, Women,*

and Crime, 2nd Edition. Thousand Oaks, CA: Sage Publications, Inc.

Chung, H. L., & Steinberg, L. (2006). Relations between neighborhood factors, parenting behaviors, peer deviance, and delinquency among serious juvenile offenders. *Developmental Psychology, 42(2)* : 319-331. doi/10.1037/0012-1649.42.2.319

Colvin, M. & Pauly, J. (1983). A critique of Criminology: Toward an integrated structural-Marxist theory of delinquency production. *American Journal of Sociology, 89*: 513-551. Retrieved from http://www.jstor.org/stable/2779004.

Cuellar, J., Jones, D.J., & Sterrett, E. (2015). Examining parenting in the neighborhood context: A review. Journal of Child and Family Studies, 24:195-219. doi: 10.1007/s10826-013-9826-y

Cullen, F.T. (1994). Social support as an organizing concept for Criminology: Presidential address to the Academy of Criminal Justice Sciences. *Justice Quarterly, 11*: 527-559. doi:10.1080/07418829400092421

Cullen, F.T., Agnew R., Wilcox, P. (2014). *Criminological theory: Past to Present. 5th eds*. Oxford: Oxford University Press.

Cummings, E.M., Davies, P.T., & Campbell, S.B. (2002). Developmental psychopathology and family process: Theory, practice, and clinical implications. *Journal of the American Academy of Child and Adolescent Psychiatry, 41(7)*: 886-886.

Currie, E. (1985). *Confronting crime: An American challenge.* New York: Pantheon.

Currie. E. (1998). *Crime and punishment in America*. New York: Metropolitan Books.

Elliott, D. S., Wilson, W. J., Huizinga, D., Sampson, R. J., Elliott, A., & Rankin, B. (1996). The effects of neighborhood disadvantage on adolescent development. *Journal of Research in Crime and Delinquency, 33*: 389-426. doi: 10.1177/0022427896033004002

Evans, T.D., Cullen, F.T., Burton, Jr.V.S., Dunaway, R.G., & Benson, M.R. (1997). The social consequences of self-control: Testing the general theory of crime. *Criminology, 35*:475-504. doi: 10.1111/j.1745-9125.1997.tb01226.x

Fagan, A. A., & Wright, E. M. (2012). The effects of neighborhood context on youth violence and delinquency: Does gender matter? *Youth Violence and Juvenile Justice, 10(1)*: 64-82. doi: 10.1177/1541204011422086

Frick, P. J., Kimonis, E. R., Dandreaux, D. M., & Farell, J. (2003). The 4 year stability of psychopathy traits in non-referred youth. *Behavioral Sciences and the Law, 21*: 713-736. doi: 10.1002/bsl.568

Frick, P. J., & Morris, A. S. (2004). Temperament and developmental pathways to conduct problems. *Journal of Clinical Child and Adolescent*

Psychology, 33(1): 54-68. doi:10.1207/S15374424JCCP3301_6

Furstenburg, F.F. Jr. (1993). How families manage risk and opportunity in dangerous neighborhoods. In W.J. Wilson (Ed.) Sociology and the Public Agenda (pp.231-258). Newbury Park, CA: Sage

Gordon, R. A. (1967). Issues in the ecological study of delinquency. *American Sociological Review, 32*: 927-944. Retrieved from http://www.jstor.org/stable/2092846.

Gottfredson, M. R., & Hirschi, T. (1990). *A General Theory of Crime.* Stanford, CA: Stanford University Press.

Hagan, J. (1994). *Crime and disrepute*. Thousand Oaks, CA: Pine Forge Press.

Harris, J. R. (1995). Where is the child's environment? A group socialization theory of development. *Psychological Review, 102*:458-489.

Harris, K.M., Halpern, C.T., Whitsel, E., Hussey, J., Tabor, J., Entzel, P., & Udry, J.R.,(2009). The National Longitudinal Study of Adolescent to Adult Health: Research Design [WWW document]. URL:http://www.cpc.unc.edu/projects/addhealth/design.

Hay, C. (2001). Parenting, self-control, and delinquency: A test of self-control theory. *Criminology, 39(3)*: 707-736. doi: 10.1111/j.1745-9125.2001.tb00938.x

Hilbe, J. M. (2007). *Negative Binomial Regression*. Cambridge, UK: Cambridge University Press.

Hirschi, T. (1969). *Causes of Delinquency*. Berkley, CA: University of California Press. Jocson, R.M., & McLoyd, V.C., (2015). Neighborhood and Housing Disorder, Parenting, and Youth Adjustment in Low-Income Urban Families. *American Journal Of Community Psychology, 55(3-4)*: 304-313. doi: 10.1007/s10464-015-9710-6.

Jones, S., Cauffman, E., & Piquero, A. R. (2007). The influence of parental support among incarcerated adolescent offenders: The moderating effects of self-control. *Criminal Justice and Behavior, 34(2)*: 229-245. doi: 10.1177/0093854806288710

Juang, L.P., & Silbereisen, R. K. (2015). The relationship between adolescent academic capability beliefs, parenting and school grades. *Journal of Adolescence, 25*:3-18. doi: 10.1006/jado.2001.0445

Kerstenburg, P.K., Brooks-Gunn, J., & Duncan, G.J. (1994). Does neighborhood and family poverty affect mothers' parenting, mental health, and social support? *Journal of Marriage and the Family, 56*: 441-455. doi: 10.2307/353111

Kochanska, G. (1991). Socialization and temperament in the development of guilt and conscience. *Child Development, 62*:1379-1392. doi: 10.1111/j.1467-8624.1991.tb01612.x

Kochanska, G. (1993). Toward a synthesis of parental socialization and child temperament in early development of conscience. *Child Development, 64*: 325-347. doi: 10.1111/j.1467-8624.1993.tb02913.x

Kochanska, G. (1995). Children's temperament, mothers' discipline, and security of attachment: Multiple pathways to emerging internalization. *Child Development, 66*: 597-615. doi: 10.1111/j.1467-8624.1995.tb00892.x

Kochanska, G. (1997). Multiple pathways to conscience for children with different temperaments: From toddlerhood to age 5. *Developmental Psychology, 33*: 228-240. doi: 10.1037/0012-1649.33.2.228

Kochanska, G., Friesenborg, A.E., Lange, L.A., & Martel, M.M. (2004). Parents' personality and infants' temperament as contributors to their emerging relationship. *Journal of Personality and Social Psychology, 86(5)*: 744-759. doi:10.1037/0022-3514.86.5.744

Kohen, D.E., Dahiten, V.S., Leventhal, T., & McIntosh, C.N. (2008). Neighborhood disadvantage: Pathways of effects for young children. *Child Development, 79*:156-169. doi: 10.1111/j.1467-8624.2007.01117.x

Kornhauser, R. (1978). *Social Sources of Delinquency*. Chicago: University of Chicago Press.

Land, K.C., McCall, P.L., & Nagin, D.S. (1996): A comparison of Poisson, nega-tive binomial, and semiparametric mixed Poisson regression models with empirical applications to criminal careers data. *Sociological Methods and Research, 24*: 387-442.

Larsson, H., Viding, E., & Plomin, R. (2008). Callous-unemotional traits and antisocial behavior: Genetic, environmental, and early parenting characteristics. *Criminal Justice and Behavior, 35(2)*: 197-211. doi: 10.1177/0093854807310225

Leventhal, T., & Brooks-Gunn, J. (2000). The neighborhoods they live in: The effects of neighborhood residence on child and adolescent outcomes. *Psychological Bulletin, 126(2)*: 309-337. doi: 10.1037/0033-2909.126.2.309

Loeber, R., & Stouthamer-Loeber, M. (1986). Family factors as correlates and predictors of juvenile conduct problems and delinquency. In *Crime and justice: An annual review of research*, ed. M. Tonry and N. Morris. Vol. 7 Chicago: University of Chicago Press.

Long, J. S. (1997). *Regression Models for Categorical and Limited Dependent Variables.* Thousand Oaks, CA: Sage Publications.

Minor, K. I. (1993). Juvenile delinquency and the transition to monopoly capitalism. *Journal of Sociology and Social Welfare, 20*: 59-80.

Morenoff, F. D., Sampson, R. J., & Raudenbush, S. W. (2001). Neighborhood inequality, collective efficacy, and the spatial dynamics of urban violence. *Criminology, 39*: 517-559.

Mowen, T. J., & Schroeder, R. D. (2015). Maternal parenting style and delinquency by race and the moderating effect of structural disadvantage. *Youth & Society*, Doi: 10.1177/0044118X15598028

Mrug, S., & Windle, M. (2009). Mediators of neighborhood influences on externalizing

behavior in preadolescent children. *Journal of Abnormal Child Psychology, 37*: 265−280.

Muftic, L. R., & Updegrove, A. H. (2018). The Mediating Effect of Self-Control on Parenting and Delinquency: A Gendered Approach With a Multinational Sample. *International Journal of Offender Therapy and Comparative Criminology, 62*(10): 3058-3076.

Osgood, D. W., & Anderson, A. (2004). Unstructured socializing and rates of Delinquency. *Criminology, 42*: 519-549.

Park, H.S., & Bauer, S. (2002). Parenting practices, ethnicity, socioeconomic status and academic achievement in adolescents. *School Psychology International, 23(4)*: 386-396. doi: 10.1177/0143034302234002

Parker, J. S., & Benson, M. J. (2004). Parent-adolescent relations and adolescent functioning: Self-esteem, substance abuse, and delinquency. *Adolescence, 39*(155): 519-530.

Perrone, D., Sullivan, C.J., Pratt, T.C., & Margaryan, S. (2004). Parental efficacy, self-control, and delinquency: A test of a General Theory of Crime on a nationally representative sample of youth. *International Journal of Offender Therapy and Comparative Criminology, 48*(3): 298-312.

Pinderhughes, E.E., Nix, R., Foster, E.M., & Jones, D. (2001). Parenting in context: Impact of neighborhood poverty, residential stability, public services, social networks, and danger on parental behaviors. *Journal of Marriage and Family, 63*: 941-953. doi: 10.1111/j.1741-3737.2001.00941.x

Pratt, T.C. & Cullen, F.T. (2000). The empirical status of Goffredson and Hirschi's gnenral theory of crime: A meta-analysis. *Criminology, 38*: 931-964.

Rankin, B. H., & Quane, J. M. (2002). Social contexts and urban adolescent outcomes: The interrelated effects of neighborhoods, families, and peers on African-American youth. *Social Problems, 49*: 79−100. doi: 10.1525/sp.2002.49.1.79

Rankin, J. H., & Kern, R. (1994). Parental attachments and delinquency. *Criminology, 32*(4): 495-515.

Rosen, L. & Turner, S. H. (1967). An evaluation of the Lander approach to the ecology of delinquency. *Social Problems, 15*:189-200. doi: 10.2307/799512

Sampson, R. J. (2006). How does community context matter? Social mechanisms and the explanation of crime. In *The Explanation of Crime: Context, Mechanisms, and Development*, eds. Per-Olof H. Wikstrom and Robert J. Sampson. Cambridge, UK: Cambridge University Press.

Sampson, R. J., & Groves, W. B. (1989). Community structure and crime: Testing social disorganization theory. *American Journal of Sociology, 94(4)*: 774-802. Retrieved from http://www.jstor.org/stable/2780858

Sampson, R. J., & Laub, J.H. (1993). *Crime in the making: Pathways and turning points through life.* Cambridge, MA: Harvard University Press.

Sampson, R. J., & Laub, J.H. (1994). Urban poverty and the family context of delinquency: A new look at structure and process in a class study. *Child Development, 65*: 523-540. doi: 10.1111/j.1467-8624.1994.tb00767.x

Sampson, R. J., & Laub, J. H. (2004). A life-course theory of cumulative disadvantage and the stability of delinquency. In T. P. Thornberry (Ed.), Developmental theories of crime and delinquency (pp.133-161). New Brunswick, NJ: Transaction Publishers.

Sampson, R. J., Morenoff, J. D., & Raudenbush, S. W. (2005). Social anatomy of racial and ethnic disparities in violence. American Journal of Public Health, 95: 224-232. doi: 10.2105/AJPH.2004.037705

Sampson, R. J., Raudenbush, S. W., & Earls, F. (1997). Neighborhoods and violent crime: A multilevel study of collective efficacy. Science, 277: 918-924. doi: 10.1126/science.277.5328.918

Schroeder, R.D., & Mowen, T.J. (2014). Parenting style transitions and delinquency. Youth & Society, 46(2): 228-254. doi: 10.1177/0044118X12469041

Schuerman, L. A., & Koblin, S. (1986). Community careers in Crime. In Alber J. Reiss, Jr., and Michael Tonry (Eds.), Communities and Crime. Chicago: University of Chicago Press.

Shakya, H.B., Christakis, N.A., & Fowler, J.H. (2012). Parental influence on substance use in adolescent social networks. *Archives of Pediatrics & Adolescent Medicine, 166(12)*: 1132-1139. doi:10.1001/archpediatrics.2012.1372

Shaw, C. R., & McKay, H. D. (1942). *Juvenile Delinquency and Urban Areas.* Chicago: University of Chicago Press.

Shaw, C. R., & McKay, H. D. (1969). *Juvenile delinquency and urban areas, 2nd Edition*. Chicago: University of Chicago Press.

Shelton, K. K., Frick, P. J., & Wootton, J. (1996). Assessment of parenting practices in families of elementary school-age children. *Journal of Clinical Child Psychology*, *25(3)*: 317-329. doi:10.1207/s15374424jccp2503_8

Shihadeh, E.S., & Steffensmier, D.J. (1994). Economic inequality, family disruption, and urban black violence: Cities as units of stratification and social control. *Social Forces*, 73: 729-751. doi: 10.1093/sf/73.2.729

Sokol-Katz, J., Dunham, R., & Zimmerman, R. (1997). Family structure versus parental attachment in controlling adolescent deviant behavior: A Social control model. *Adolescence, 32*(125): 199-216.

Taylor, R. D. (2000). An examination of the association of African American mothers' perceptions of their neighborhoods with their parenting and adolescent adjustment. *The Journal of Black Psychology, 26*: 267–287. doi:10.1177/0095798400026003001.

Tolan, P. H., Gorman-Smith, D., & Henry, D. (2003). The developmental ecology of urban males' youth violence. *Developmental Psychology, 39*: 274–291. doi: 10.1037/0012-1649.39.2.274

Unnever, J.D., Cullen, F.T., & Agnew, R. (2006). Why is "bad" parenting criminogenic? Implications from rival theories. *Youth Violence and Juvenile Justice, 4*: 3-33. doi: 10.1177/1541204005282310

Vieno, A., Nation, M., Perkins, D.D., Pastore, M. & Santinello, M. (2010). Social capital safety concerns, parenting, and early adolescents' antisocial behavior. *Journal of Community Psychology, 38(3)*:314-328. doi: 10.1002/jcop.20366

Wright, J. P., & Cullen, F. C. (2001). Parental efficacy and delinquent behavior: Do control and support matter? *Criminology, 39*(3): 677-705.

Zimmerman, G.M. (2010). Impulsivity, offending, and the neighborhood: Investigating the person-context nexus. *Journal of Quantitative Criminology, 26(3)*: 301-332. doi: 10.1007/s10940-010-9096-4

Zimmerman, G.M, Botchkovar, E.V., Antonaccio, O., & Hughs, L.A. (2015). Low self-control in "Bad" neighborhoods: Assessing the role of context in the relationship between self-control and crime. *Justice Quarterly, 32*:56-84. doi:10.1080/07418825.2012.737472

Zuberi, Anita. (2016). Neighborhoods and Parenting: Assessing the influence of neighborhood quality on the parental monitoring of youth. *Youth & Society, 48(5)*: 599-627

Moving Beyond Criminal Law Responses to Cybersecurity Governance in Africa

Uchenna Jerome Orji, Ph.D.[*]
Assistant Professor
School of Law
American University of Nigeria

Abstract

Measures to address the security challenges of the information society have given rise to the concept of cybersecurity governance. One major aspect of cybersecurity governance is the establishment of legal measures to criminalize and deter malicious acts that affect the integrity, confidentiality, availability and security of digital data and computer systems. Accordingly, several States and intergovernmental organizations across the world have established legal frameworks to promote cybersecurity governance. This is also the case in Africa. The African Union has adopted a Convention on Cyber Security and Personal Data Protection, while other African regional intergovernmental organizations such as the Economic Community of West African States, the Common Market for Eastern and Southern Africa and the Southern African Development Community have established legal and policy frameworks for cybersecurity governance. In addition, many African States have developed legal and policy frameworks to promote cybersecurity, while some others in the process of developing such frameworks. However, most of Africa's responses to cybersecurity governance have been focused on the establishment of criminal law measures. Yet while the establishment of criminal law measures is regarded as a critical component of cybersecurity governance, the isolated existence of such measures may not produce desirable outcomes in terms of minimizing cybersecurity vulnerabilities in Africa's information society. This paper seeks to make a case for the development of other critical components of cybersecurity governance, including technical and organizational measures and user education. It suggests that 'stand-alone' criminal law measures will not be able to reduce the rising trends of cyber-criminality in Africa, and that the timely development of other critical components of cybersecurity governance is imperative especially due to the peculiar challenge of weak law enforcement capacities and justice delivery systems in many African States.

Keywords

Africa, Cybercrime, Cybersecurity Governance Measures, Law, Policy

* Direct correspondence to Uchenna Jerome Orji, Ph.D., Assistant Professor, School of Law, American University of Nigeria; e-mail: jeromuch@yahoo.com; uchenna.orji@aun.edu.ng.
* http://dx.doi.org/10.36889/IJCJ.2021.002.
* Received 15 Nov 2020; Revised 19 March 2021; Accepted 13 April 2021; Available online 26 April 2021.
INTERNATIONAL JOURNAL OF CRIMINAL JUSTICE, Vol. 3 Issue 1, June 2021, 60-98

INTRODUCTION

During the 20th century advances in information and communications technologies brought about the convergence of telecommunications and computer technologies. This signified the beginning of an era known as the information age. A very distinctive feature of the information age is the continuous integration of computers and digital communication technologies in virtually all aspects of life and critical services that support modern societies and the tendency towards "connecting everything to everything".[1] This has given rise to the emergence of the information society. However, with the emergence of the information society, the security of computer systems, digital data, digital communication technologies and networks now have an overwhelming influence on almost all aspects of life in modern societies. Malicious acts that target computer systems and their networks now have the potential of affecting individuals, countries and the global economy in ways previously unimagined. In particular, the most critical challenges of the information society have been the security of computer systems and digital data and the prevention of the malicious misuse of information communications technologies by criminals, terrorist groups, or State actors. Measures to address these security challenges of the information society have given rise to the concept of cybersecurity governance.

One major aspect of cybersecurity governance is the establishment of legal measures to criminalize and deter malicious acts that affect the integrity, confidentiality, availability and security of digital data and computer systems. Accordingly, several States and intergovernmental organizations across the world have established legal and policy frameworks to promote cybersecurity governance. In Africa, Internet penetration has also raised concerns on the need to strengthen cybersecurity and prevent Africa from becoming a "safe harbour" for cybercrime.[2] There are also concerns over the negative impact of cybercrime on African economies. For example, a survey conducted on Nigeria which has the largest Internet User population in Africa estimates that the country annually loses around

---

1) M. Dunn, A Comparative Analysis of Cybersecurity Initiatives Worldwide, World Summit on Information Society (WSIS) Thematic Meeting on Cybersecurity, Geneva, ITU: June 2005, p.5.

2) L. Kharouni, 'Africa: A New Safe Harbour for Cyber criminals?", Trend Micro Research Paper, Trend Micro Inc: USA, 2013, pp.1-26.

13 Billon US Dollars to cybercrime including loss of potential foreign investments.[3] South Africa is also reported to annually lose over 5.7 Billion Rand due to cybercrime,[4] while Norton reports that 70 percent of South Africans have fallen victim to cybercrime compared with a global average of 50 percent.[5] It is estimated that cyber-attacks cost African businesses around 1.048 billon US Dollars a year.[6] To address cybersecurity governance concerns and promote the control of cybercrime, the African Union (AU) adopted a Convention on Cyber Security and Personal Data Protection, while African regional intergovernmental organizations such as the Economic Community of West African States (ECOWAS), the Common Market for Eastern and Southern Africa (COMESA) and the Southern African Development Community (SADC) have all established legal frameworks for cybersecurity governance. In addition, many African States have developed legal and policy frameworks for cybersecurity governance, while some States are in the process of developing such frameworks. However, most of Africa's responses to cybersecurity governance have focused on the establishment of criminal law measures. While there is no doubt that the establishment of criminal law measures is an essential component of cybersecurity governance, the isolated existence of such measures may not produce desirable outcomes in terms of minimizing cybersecurity vulnerabilities in Africa's information society.

This paper makes a case for the development of other critical components of cybersecurity governance including technical and organizational measures and user education. It suggests that 'stand-alone' criminal law measures will not reduce rising trends of cyber-criminality in Africa and that the timely development of other critical components of cybersecurity governance is imperative especially due to the peculiar challenge of weak law enforcement capacities and justice delivery

---

3) G. Sesan, et al, Economic Cost of Cybercrime in Nigeria, Paradigm Initiative: Nigeria: 2013, p.11, available at < https://pinigeria.org/download/download/cybercost.pdf> last accessed on 18 March, 2021.

4) T. Mastile, 'South Africa Loses R.5.7 Billion Annually to Cybercrime', CNBC Africa, 12 February, 2015, available at <http://www.cnbcafrica.com/news/special-report/2014/06/10/safrica-loses-r57-billion-annually-to-cybercrime> last accessed on 18 March, 2021.

5) T. Jackson, 'Can Africa Fight Cybercrime and Preserve Human Rights?', BBC News, 10 April, 2015, available at <http://www.bbc.com/news/business-32079748> last accessed on 18 March, 2021.

6) Serianu Limited, Africa Cybersecurity Report 2017: Demystifying Africa's Cyber Security Poverty Line (Kenya: Serianu Limited, 2017), p.3.

systems in many African States.

The paper is divided into six sections. The first section which includes this introduction examines the concept of cybersecurity and the major components of cybersecurity governance. The second section looks at Africa's cybersecurity threat landscape. The third section presents an overview of African responses to cybersecurity governance. The fourth section examines current challenges to cybersecurity governance in Africa. The fifth section makes proposals for the development of other critical aspects for cybersecurity governance aside from criminal law measures. The conclusion then follows.

Cybersecurity

Cybersecurity is an information age terminology that was derived by merging the prefix – 'cyber' with the concept of 'security'. The term is defined as "the collection of tools, policies, guidelines, risk management approaches, actions, training, best practices, assurances and technologies that can be used to protect the cyber-environment and organization, as well as users' assets".[7][8] Cybersecurity also refers to the following:

(1) "a set of activities and other measures, technical and non-technical, intended to protect computers, computer networks, related hardware and devices software, and the information they contain and communicate, including software and data, as well as other elements of cyberspace, from all threats, including threats to the national security;

(2) the degree of protection resulting from the application of these activities and measures;

(3) the associated field of professional endeavour, including research and analysis, aimed at implementing and those activities and improving their quality".[9]

Cybersecurity is primarily concerned with protecting the cyberspace and information communications technologies from all forms of cyber threats. Within

---

7) ITU High Level Experts Group [HLEG] ITU Global Cyber-Security Agenda (GCA) High Level Experts Group [HLEG] Global Strategic Report, Geneva, ITU 2008, p.27.

8) U. J. Orji, Cybersecurity Law and Regulation, The Netherlands, Wolf Legal Publishers, 2012, pp.10-16.

9) M. Dunn, A Comparative Analysis of Cybersecurity Initiatives Worldwide, World Summit on Information Society (WSIS) Thematic Meeting on Cybersecurity, Geneva, ITU: June 2005, p.4.

the context, “cyber threats” refer to malicious acts that are perpetrated in the electronic environment known as the ‘cyberspace’ and other species of malicious acts that target information communication technologies. These have been classified into the following forms of threats: threats to individual users such as viruses or identity theft, as well as annoyances such as spam, spyware or pop-ups; threats to businesses, governments or other organizations, for instance, through the exploitation of vulnerabilities in their data storage, industrial espionage or denial of service etc; threats to critical public infrastructure such as electronic communication networks, financial systems, emergency services, navigation systems, electrical power grids, air traffic control, and water control systems etc.[10)]

Cybersecurity Governance

The concept of governance[11)] basically refers to the organized control or direction of activities, States, societies, individuals and organizations to achieve desired objectives. To a large extent, the definition of the concept of governance would vary in meaning depending on the context in which it is used. For example, “governance” has been defined as a government's “ability to make and enforce rules and to deliver services”.[12)] Governance has also been defined as referring to structures and processes designed to ensure accountability, transparency, responsiveness, rule of law, stability, and also represent the norms, values and rules through which public affairs are managed in a responsive and transparent manner.[13)] Another definition refers to governance as “the conscious management of regime structures, with a view to enhancing the public realm”.[14)] Since 1990s, the term ‘governance’ has acquired the status of a generalized concept to classify the act of regulation and has been applied by institutions, States, policy-makers,

10) ITU, ‘Challenges to Building a Secure Information Society’, 2007 World Information Society Report: Beyond WSIS, ITU, Geneva, 2007, p. 83.

11) The word “governance” originates from the Latin word “gubernare,” which means “to steer. See M. M. Tamayao, What Is Governance?, available at <https://tamayaosbc.wordpress.com/2014/08/ 21/what-is-governance/> last accessed on 18 March, 2021.

12) F. Fukuyama, ‘What Is Governance?’, CGD Working Paper 314 (Washington, DC: Center for Global Development, January 2013), p.3.

13) International Bureau of Education, ‘Concept of Governance’, available at <http://www.ibe.unesco.org/en/geqaf/technical-notes/concept-governance> last accessed on 18 March, 2021.

14) ‘Understanding the Concept of Governance’, available at <https://www.gdrc.org/u-gov/governance-understand.html> last accessed on 18 March, 2021.

researchers and other commentators to diverse aspects of human endeavour.[15] When placed within the cybersecurity context, the concept of governance would generally encompass the establishment, implementation and monitoring of a broad range of measures and activities technical and non-technical, including legal, policy and institutional measures intended to protect computers, computer networks, related hardware and software, and the information they contain and communicate, including software and data, as well as other elements of cyberspace, from all threats, including threats to the national security. As such, cybersecurity governance concerns the establishment and effective implementation of technical and non–technical measures (including legal and policy measures, institutional measures, end user education and research and development) that aim to promote cybersecurity, as well as the monitoring of such measures to achieve desired objectives.

Cybercrime

Malicious acts which are prohibited by cybersecurity laws are commonly referred to as 'cybercrime' or 'computer crime'. These terms are often used interchangeably to refer to instances where computer technologies are the target of a malicious or unlawful activity or the instrument for facilitating a crime or malicious activity. However, there is no universally accepted legal definition of cybercrime or computer crime[16] and cybersecurity laws generally tend to avoid such explicit definitions. For example, the African Union Convention on Cyber Security and Data Protection[17] and the Council of Europe Convention on Cybercrime[18] does not explicitly define the terms 'cybercrime' or 'computer crime'. However, the Council of Europe Convention on Cybercrime criminalize a range of acts in its Articles 2-10 on substantive criminal law in four different categories, namely:

---

15) J. Graham, B. Amos and T. Plumptre, Governance Principles for Protected Areas in the 21st Century 5 (Ottawa: Institute of Governance, 2003) p. 2-7; D. Olowu, 'Environmental Governance Challenges in Kiribati: An Agenda for Legal and Policy Responses', Law, Environment and Development Journal (2007) Vol .3, Issue 3, p.259.

16) U. J. Orji, Cybersecurity Law and Regulation, The Netherlands, Wolf Legal Publishers, 2012, pp.17-19.

17) The African Union Convention on Cyber Security and Personal Data Protection EX.CL/846 (XXV) adopted by the 23rd Ordinary Session of the African Union Assembly, Malabo, 27 June, 2014.

18) The Council of Europe, Convention on Cybercrime, 41 I.L.M. 282 (Budapest, 23.XI, 2001).

(1) offences against the confidentiality, integrity and availability of computer data and systems;
(2) computer-related offences;
(3) content-related offences, and;
(4) offences related to infringement of copyright and related rights.

The above categories of offences under Convention are regarded as establishing a minimum universal standard of what can be classified as cybercrime or computer crime.[19]

Cybersecurity basically appears a broader concept than cybercrime. For example, while cybercrime control measures aim to criminalize and tackle intentional acts that impair the confidentiality, integrity and availability of computer data and systems. On the other hand, cybersecurity governance measures seek to address non-intentional cyber incidents including natural disasters and accidents that affect information communication technology (ICT) infrastructure, as well as intentional attacks against the confidentiality, integrity and availability of computer systems and data offences and any offences involving electronic evidence.[20]

Critical Components of Cybersecurity Governance

Cybersecurity governance encompasses multi-disciplinary components including but not limited to legal measures, technical measures, institutional/organizational measures, end user education and research and development. These components are discussed below.

Legal measures

This component covers all legal aspects of cybersecurity governance and it is usually regarded as probably the most relevant aspect especially in the control of cybercrime.[21] This aspect entails the establishment of adequate legal measures such as laws, regulations, and policies to criminalize instances where computer systems, digital technologies or critical information infrastructure are the target of

---

19) S. Schjolberg, 'The History of Global Harmonization on Cybercrime Legislation - the Road to Geneva', (2008), pp. 8-9, available at <http://www.cybercrimelaw.net/documents/cybercrime_history.pdf> last accessed on 18 March, 2021.

20) UNODC, Comprehensive Study on Cybercrime (Draft – February 2013), United Nations, New York, 2013, p.228.

21) G. Marco, Understanding Cybercrime: A Guide for Developing Countries, ITU, Geneva, 2009, p.84. See also G. Marco, 'The Slow Wake of a Global Approach against Cybercrime', Computer Law Review International, 2006, Issue 5, p. 141.

a malicious activity, or where computer systems or digital technologies are the instrument for facilitating a malicious activity. The establishment of legal measures for cybersecurity governance is usually best approached through the enactment of new laws that are drafted in a technology neutral[22] language. This approach enables legal regulation to keep up with new technological developments and emerging trends in the criminal misuse of information technologies. Legal aspects of cybersecurity governance also cover issues relating to procedures for investigating cybercrimes, the handling of evidence and prosecution of cybercrimes, and the development of international cooperation mechanisms for controlling cybercrime and responding to cybersecurity incidents.[23]

Technical measures

The technical aspects of cybersecurity governance cover the development and implementation of technical protection measures for computer systems and network infrastructure. Generally, computer systems or digital technologies that are well protected are hard to attack or penetrate. Technical protection measures are usually implemented based on a computer's security architecture through the use of tools such as fire walls, passwords or synchronized passwords, voice or fingerprint identification or retinal and biometric access protocols, antivirus software and real time intrusion detection software. Technical aspects of cybersecurity governance also include the development and implementation of active countermeasures to secure computers and digital technologies. An example is the use of software bombs by software developers to secure software. Software bombs are sometimes built into software by developers as a means of enforcing payment in the event of a dispute[24] or for the purpose of curtailing unauthorized access or distribution of such software. However, the use of such active countermeasures may be unlawful in some jurisdictions.[25]

---

22) Technological neutrality is a regulatory principle that implies that legislation should define the objectives to be achieved and should neither impose, nor discriminate in favour of, the use of a particular type of technology to achieve those objectives. See C. Reed, 'The Law of Unintended Consequences – Embedded Business Models in IT Regulation', Journal of Information Law and Technology, 2007 (2), p.2.

23) U. J. Orji, 'Multilateral Legal Responses to Cybersecurity in Africa: Any Hope for Effective International Cooperation?' in M. Maybaum, et al (eds.), Architectures in Cyberspace- 7th International Conference on Cyber Conflict, NATO CCD COE, Tallinn, Estonia, pp.110-112.

24) T.J. McIntyre, 'Computer Crime in Ireland: A Critical Assessment of the Substantive Law', Irish Criminal Law Journal, 2005, Vol. 15 (1), p.7.

Institutional/Organizational measures

This component of cybersecurity governance deals with the development of institutional capacities to promote cybersecurity. It includes the establishment of law enforcement organizations as well as the development of the capacities of such organizations to prevent and detect cybercrime or enforce cybersecurity laws. This aspect of cybersecurity governance also includes the establishment of Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs)[26] to manage cybersecurity incidents by providing prevention, early warning, detection, reaction and crisis management platforms. CERTs are usually responsible for a range of functions which include:

(1) monitoring cybersecurity threats and issuing early warnings of such threats;
(2) effectively responding to emergencies arising from threats against computer systems and critical information infrastructure and;
(3) providing security analysis of potential vulnerabilities against computer systems.[27]

A CERT may be established by a national government or a private organization or through public–private partnership arrangements.[28] However, the responsibilities of a national CERT are broader than that of a private organization, because a national CERT is usually responsible for coordinating national emergency responses to cyber threats and establishing related best practices within a State.[29]

End-user education

The individual operating a computer system is usually regarded as the weakest link in the cybersecurity chain.[30] Hence, end-user education is regarded as a vital

---

25) Rubicon Computer Systems v. United Paints Limited (2000) 2 TCLR 453. See T. J. McIntyre, 'Computer Crime in Ireland: A Critical Assessment of the Substantive Law', Irish Criminal Law Journal, 2005, Vol. 15 (1), p.7. See also T. Sewart, 'Time to Drop the Bomb', *Computers & Law*, 2003 Vol.14 (4), p.22.

26) The terms 'CERT' and 'CSIRT' are used interchangeably. See ITU High Level Experts Group [HLEG] ITU Global Cyber-Security Agenda (GCA) High Level Experts Group [HLEG] Global Strategic Report, Geneva, ITU: 2008, p.96.

27) *Ibid*, pp. 96-97.

28) *Ibid,* pp. 94-96.

29) ITU Study Group Q.22/1, Report on Best Practices For A National Approach To Cybersecurity: A Management Framework For Organizing National Cybersecurity Efforts [Draft], Geneva, ITU-D, January 2008, p. 39/71.

30) ITU High Level Experts Group [HLEG] ITU Global Cyber-Security Agenda (GCA) High Level Experts Group [HLEG] Global Strategic Report, Geneva, ITU: 2008, p.31.

component of cybersecurity governance. Computer users are usually the major target of criminals in the cyber environment. This is because, it is usually easier to attack private computers to obtain sensitive financial information rather than the well protected computer systems of a financial institution.[31] Also, cybercrimes such as phishing, spoofing and e-mail scams[32] are usually successful not because of the absence of technical cybersecurity measures, but rather due to a victim's lack of awareness.[33] Accordingly, it has been aptly observed that: "if users are aware that their financial institutions will never contact them by E-mail requesting passwords or bank accounts details they cannot fall victim to phishing or identity fraud attacks".[34]

User education in the cybersecurity context involves the education of end-users of computer systems and digital technologies on the risks they face in the information society so as to enable them manage such risks. User education can be undertaken through several avenues such as public enlightenment campaigns, lessons in schools, ICT centers, universities, and ICT equipment user guide provided by manufacturers or service providers. Organizations that can play strategic roles in promoting end-user education include network service providers, manufacturers of ICT equipment, financial institutions, non-governmental organizations, schools and CERTs.

Research and development

This component of cybersecurity governance deals with the promotion of research on cybersecurity issues. Relevant research topics in cybersecurity governance range from legal and policy issues to technical, social and national security issues. Cybersecurity governance has already become a major research issue in developed countries with a great deal of research being undertaken by States organs (including law enforcement and military institutions), private sector research institutes and the research institutes of universities and international organizations. For example, international organizations such as the NATO Cooperative Cyber Defense Center of Excellence, the International Telecommunication Union (ITU), and the Council of Europe have been very active in researching cybersecurity governance issues.

---

31) G. Marco, Understanding Cybercrime: A Guide for Developing Countries, Geneva, ITU, 2009, p.86.

32) One the most common forms of e-mail scams in the cyberspace is the Nigerian email Scam commonly known as Yahoo-Yahoo in Nigeria. This term derives its origin from Yahoo mail a popular free email service provider on the Internet.

33) G. Marco, Understanding Cybercrime: A Guide for Developing Countries, Geneva, ITU, 2009, p.86.

34) G. Marco, ibid, p.87.

AFRICA'S CYBERSECURITY THREAT LANDSCAPE

The increasing penetration of information communication technologies (ICTs) in Africa[35] has naturally given rise to their growing integration in critical national sectors.[36] For example, banking and financial services sectors in African States are increasingly integrating ICTs to enhance service delivery and improve consumer satisfaction.[37] Also, across several African States, critical sectors including transportation, energy, health, immigration services, education and manufacturing are increasingly deploying ICTs in their operations.[38] This increasing integration of ICTs in critical national sectors is also seen a means of facilitating Africa's economic development and regional integration.[39] However, while African States have not achieved a high level of digitalization that is comparable to developed countries, the rise of digitalization in Africa has increased the reliance of critical national sectors on information infrastructure to the extent that the disruption of such infrastructure by accidents or cyber-attacks will cause the disruption of economic and social activities and public services in a manner that could trigger serious national security concerns. For example, while mobile phone banking innovations and platforms has enhanced the penetration of financial services to unbanked individuals, while further increasing financial flows and ecommerce across African countries, there are also increased chances that such platforms and institutions that operate them can suffer cyber-attacks.[40] In South Africa alone, an average of over 19, 842 cyber –attacks are daily

35) GSMA, The Mobile Economy Africa 2020 (GSMA: London, 2020) pp. 2, 8 &19. See also, Miniwatts Marketing Group, 'Internet Usage Statistics for Africa', (31 December, 2020), available at <http://www.internetworldstats.com/stats1.htm> last accessed on 18 March, 2021.

36) S. R. Ponelis and M. A. Holmer, 'ICT in Africa: Building a Better Life for all', Information Technology for Development (2015)B. T. Mbatha, D.N. Ocholia and J.L. Roux, 'Diffusion of ICTs in Selected Government Departments in KwaZulu −Natal, South Africa', Information Development, (2011) , Vol. 27 (4), pp251-263.

37) M. K. Luka and I. A. Frank, 'The Impacts of ICTs on Banks: A Case Study of the Nigerian Banking Industry', International Journal of Advanced Computer Science and Applications (2012), Vol. 3 (9), pp.145-150; M. Andrianaivo and Kangni Kpodar, 'ICT, Financial Inclusion, and Growth: Evidence from African Countries', *IMF Working Paper*, WP/11/73 (2011), pp.4-41

38) P. Wallet, Information and Communication Technology (ICT) in Education in Sub-Saharan Africa: A Comparative Analysis of basic e-readiness in Schools (UNESCO Institute for Statistics: Canada, 2015), pp.5-25; R. Bahrini and A. Qaffas, 'Impact of Information and Communication Technology on Economic Growth: Evidence from Developing Countries', Economies (March, 2019) Vol. 7 (21), pp.1-13.

39) U.J Orji, International Telecommunications Law and Policy (Cambridge Scholars Publishing: United Kingdom, 2018), p.237.

reported on ecommerce platforms.[41] This is observed as a major factor that degrades consumer confidence in terms of the widespread adoption of ecommerce services in Africa.[42] Recent research also indicate that attacks on critical infrastructure are becoming "frequent" in Africa with banks particularly being the common targets and losing billions of dollars to theft and service disruption.[43] As such, there is no doubt that African States are also vulnerable to cybersecurity threats which affect elements of critical sectors that rely on information infrastructure.

In addition, the increasing spread of ICTs and Internet penetration within Africa around the first decade of the 21st century also brought about the migration of advance fee fraud scammers to Internet platforms, with some African countries being classified as major sources of Internet advance fee fraud email scams.[44] Aside from email fraud scams, there has also been a growing trend in perpetration of other sophisticated forms of cybercrime such as hacking, credit card scams, identity theft, web cloning, phishing, Business Email Compromise fraud, and tax scams.[45] A survey conducted by the INTERPOL amongst its member countries in West Africa (including Benin, Cape Verde, Côte d'Ivoire, Gambia, Ghana, Liberia, Mauritania, Niger, Nigeria, Senegal, and Sierra Leone) revealed that cybercriminals in the West African region have gained a high level of expertise in committing crimes against individuals and businesses.[46] A report by Trend Micro report indicates the rise of an underground cybercrime economy in West Africa due to the constant increase in the volume of cybercrime-related complaints received by law enforcement agencies in the region.[47]

There are also concerns over the negative impact of cyber-attacks on African

40) I. Gagliardone and N. Sambuli, 'Cyber Security and Cyber Resilience in East Africa', Global Commission on Internet Governance Paper Series, No. 15 (May, 2015), p.1.

41) A. A. Odonkor, Unveiling the cost of cybercrime in Africa, CGTN (27/10/2020), available at <https://news.cgtn.com/news/2020-10-27/Unveiling-the-cost-of-cybercrime-in-Africa-UVhmu1PJeM/index.html> last accessed on 18 March, 2021.

42) Ibid.

43) N. Allen, 'Africa's Evolving Cyber Threats', African Center for Strategic Studies, (19 January, 2021), available at <https://africacenter.org/spotlight/africa-evloving-cyber-threats/> last accessed on 18 March, 2021.

44) Internet Crime Complaint Center, 2010 Internet Crime Report (National White Collar Crime Center: United States, 2011) p.11; Internet Crime Complaint Center, 2013 Internet Crime Report (National White Collar Crime Center: United States, 2014) pp. 15 & 21.

45) R. Flores, et al, Cybercrime in West Africa: Poised for an Underground Market (Trend Micro and INTERPOL, 2017) p.3.

46) Ibid, pp.12-13.

47) Ibid, p.4.

economies. For example, South Africa is also reported to annually lose over 5.7 Billion Rand due to cybercrime,[48] while Norton reports that 70 percent of South Africans have fallen victim to cybercrime compared with a global average of 50 percent.[49] A survey conducted on Nigeria which has the largest Internet User population in Africa estimates that the country annually loses around 13 Billon US Dollars to cybercrime including loss of potential foreign investments.[50] Another report published by the United States based Center for Strategic and International Studies (CSIS) on the global economic impact of cybercrime estimates that about 0.08 percent of Nigeria's gross domestic product (GDP) is lost to cybercrime.[51] In Ghana, the Cybercrime Unit of the Police Service Criminal Investigation Department reported that 230 million US Dollars was lost due to cybercrime cases between 2016 and August, 2018.[52] Ghana's Cybercrime Unit also estimates that the country annually loses an average of 166 million US Dollars to cybercrime.[53] The annual financial cost of cybercrime in Senegal is estimated at 27 million US Dollars;[54] while Kenya which is East Africa's central information technology hub is estimated to annually lose over 295 million US Dollars to cybercrime.[55] It has been generally estimated that cyber-attacks cost African businesses around 1.048 billon US Dollars a

48) T. Mastile, 'South Africa Loses R.5.7 Billion Annually to Cybercrime', CNBC Africa, 12 February, 2015, available at <http://www.cnbcafrica.com/news/special-report/2014/06/10/safrica-loses-r57-billion-annually-to-cybercrime> last accessed on 18 March, 2021.

49) T. Jackson, 'Can Africa Fight Cybercrime and Preserve Human Rights?', BBC News, 10 April, 2015, available at <http://www.bbc.com/news/business-32079748> last accessed on 18 March, 2021.

50) G. Sesan, et al, Economic Cost of Cybercrime in Nigeria, Paradigm Initiative: Nigeria: 2013, p.11, available at < https://pinigeria.org/download/download/cybercost.pdf> last accessed on 18 March, 2021.

51) Center for Strategic and International Studies, Net Losses: Estimating the Global Cost of Cybercrime (Center for Strategic and International Studies: Washington, DC, June, 2014) pp.9 and 21.

52) G. Akweiteh Allotey, 'Ghana Loses $230 Million to Cyber Criminals – CID', Citinews (4 October, 2018), available at <https://citinewsroom.com/2018/10/04/ghana-loses-230m-to-cyber-criminals-cid/> last accessed on 18 March, 2021.

53) 'Cybercrime Impact and the Way Forward', Business & Financial Times Online (5 November, 2018), available at <https://www.thebftonline.com/2018/features/cybercrime-impact-and-the-way-forward/> last accessed on 18 March, 2021.

54) L. S. and K. Signe, 'Global Cybercrimes and Weak Cybersecurity Threaten Businesses in Africa', Brookings: Africa in Focus (30 May, 2018), available at <https://www.brookings.edu/blog/africa-in-focus/2018/05/30/global-cybercrimes-and-weak-cybersecurity-threaten-businesses-in-africa/> last accessed on 18 March, 2021.

55) Serianu Limited, Africa Cybersecurity Report 2018: Kenya (Kenya: Serianu Limited, 2018), p.12.

year.[56] A recent report by the INTERPOL also estimates that Africa lost about 3.5 billion US Dollars in 2017.[57] However, to a large extent there appears to be a dearth of empirical and verifiable data on the economic cost of cyber-attacks in African countries due to the under-reporting of cyber-attacks.[58] Notwithstanding this state of affairs, there is no doubt that African countries are suffering economic losses from cyber-attacks[59] which further limits the social and economic development prospects of the Internet within the African region.[60]

AN OVERVIEW OF AFRICAN RESPONSES TO CYBERSECURITY GOVERNANCE

African States and intergovernmental organizations have established frameworks to promote cybersecurity governance and also prevent Africa from becoming a "safe harbour" for cybercrime.[61] This section will undertake an overview of African regional and national responses to cybersecurity governance. In this regard, the section will review cybersecurity governance responses from African regional intergovernmental organizations such as the AU, the ECOWAS, the COMESA and the SADC, and also provide an overview of national responses in African States.

The AU Convention on Cyber Security

The African Union (AU) was originally founded as the Organization of African Unity on 25 May, 1963, and later assumed its current name and structure in 2002.[62]

---

56) Serianu Limited, Africa Cybersecurity Report 2017: Demystifying Africa's Cyber Security Poverty Line (Kenya: Serianu Limited, 2017), p.3.

57) INTERPOL, Online African Organized Crime from Surface to Dark Web (INTERPOL: France, July 2020), p.8.

58) Ibid, p.67.

59) Solutions Consulting, West Africa Cybersecurity Indexing and Readiness Assessment (Solutions Consulting: Florida, United States, 2018). See Serianu Limited, Africa Cyber Security Report 2017: Demystifying Africa's Cyber Security Poverty Line (Serianu Limited: Kenya, 2017) p.11; African Union and Symantec Corporation, Cybercrime & Cybersecurity Trends in Africa (Symantec Corporation and African Union, November, 2016), p.7.

60) Nigerian Communications Commission (NCC), Final Report on Effects of Cyber Crime on Foreign Direct Investment and National Development (NCC: Abuja, 2017). See U.J. Orji, 'Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria', Tilburg Law Review (2019) Vol. 24(1), pp.109 &122.

61) L. Kharouni, 'Africa: A New Safe Harbour for Cyber criminals?", Trend Micro Research Paper, Trend Micro Inc: USA, 2013, pp.1-26.

62) African Union, 'African Union in a Nutshell', available at <http://www.au.int/en/abut/nutshell>

The AU is the most prominent regional intergovernmental organization that unites African States and it comprises of 55 sovereign States.[63] The aims of the AU include to "accelerate the political and socio-economic integration" of the African continent[64] and to coordinate and harmonize the policies between the existing and future Regional Economic Communities.[65] In line with its mandate, the AU established a Cybersecurity Convention which was adopted by AU Heads of State and Government during the 23rd Ordinary Session of the AU Assembly in Malabo on 27 June, 2014. The Convention which is known as the AU Convention on Cyber Security and Personal Data Protection[66] aims to harmonize the laws of African States on electronic commerce, data protection, cybersecurity promotion and cybercrime control. The Convention will to enter into force after it has been ratified by 15 AU Member States.[67] However, according to a report by the AU, as of June 2020, only 14 AU Member States (Benin, Chad, Comoros, Congo, Ghana, Guinea-Bissau, Mozambique, Mauritania, Rwanda, Sierra Leone, Sao Tome & Principe, Togo, Tunisia and Zambia) had signed the Convention, while eight Member States (Angola, Ghana, Guinea, Mauritius, Mozambique, Namibia, Rwanda and Senegal) had ratified the Convention.[68] The AU report also shows that the signatures and ratifications were done in 2015, 2016, 2017, 2018, 2019 and 2020 with none in 2014 when the Convention was adopted.[69]

The Convention recognizes that cybercrime constitutes "a real threat to the security of computer networks and the development of the Information Society in Africa".[70] Under the Convention Member States are required to establish national legal, policy and institutional governance mechanisms to promote cybersecurity. This

last accessed on 18 March, 2021.

63) African Union, 'Member States' <http://www.au.int/en/member_states/country profiles> last accessed on 18 March, 2021

64) Article 3 (c) Constitutive Act of the African Union, adopted the Thirty-Sixth Ordinary Session of the Assembly of Heads of State and Government, 11 July, 2000 (Lome, Togo).

65) Article 3 (i) ibid.

66) African Union (AU) Convention on Cyber Security and Personal Data Protection, EX.CL/846(XXV) adopted at the 23rd Ordinary Session of the Assembly of the African Union (Malabo, 27th June 2014). [Hereafter AU Convention on Cyber Security].

67) Article 36 AU Convention on Cyber Security.

68) African Union, List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection, (18/06/2020), available at <https//au.int/sites/default/files/treaties/29560-sl-African%20Union%Convention%20On%Cyber%20Security%20And%Personal%20Data%20Protection.pdf> last accessed on 18 March, 2021.

69) Ibid.

70) Preamble, AU Convention on Cyber Security.

includes the establishment of a National Cybersecurity Framework that comprises a National Cybersecurity Policy, a National Cybersecurity Strategy[71] and National Cybersecurity Governance Structures.[72] In addition, the Convention requires Member States to establish laws to criminalize offences such as attacks against computer systems[73] and data,[74] as well as online child pornography[75] and also establish procedural measures for the control of cybercrime.[76]

The Convention further establishes legal provisions to promote international cooperation on cybersecurity.[77] In particular, Member States are required to "encourage the establishment of institutions that exchange information on cyber threats and vulnerability assessment such as Computer Emergency Response Teams (CERTS) or Computer Security Incident Response Teams (CSIRTS)"[78] and also make use of existing channels of international cooperation (including intergovernmental or regional, or private and public partnerships arrangements) for the purpose of promoting cybersecurity and tackling cyber threats.[79] To a large extent, the Convention adopts a holistic cybersecurity governance approach that apparently goes beyond that of the Council of Europe Convention on Cybercrime which limits its focus to the criminalization of cybercrime and the establishment of procedural mechanisms for law enforcement and international cooperation.[80]

The ECOWAS Directive on Fighting Cybercrime

The ECOWAS was founded by the Treaty of Lagos on 28 May, 1975.[81] Its aims to promote regional cooperation and integration that will lead to the establishment of an economic union in West Africa and also foster economic stability

71) Article 24 ibid.
72) Article 25 ibid.
73) Article 29:1 ibid.
74) Article 29:2 ibid.
75) Article 29:3(1) ibid.
76) Articles 29:3(4), 31:3(a) ibid.
77) Article 28 ibid.
78) Article 28:3 AU Convention on Cyber Security.
79) Article 28: 4 ibid.
80) U. J. Orji, 'Examining Missing Cybersecurity Governance Mechanisms in the African Union Convention on Cybersecurity and Personal Data Protection', Computer Law Review International, October, 2014, Issue 5, pp.131-132.
81) Treaty of ECOWAS (Revised, 24 July, 1993), 35 ILM 660, (1996) [Hereafter, ECOWAS Treaty].

and relations amongst Member States.[82] The ECOWAS Treaty requires Member States to ensure "the harmonization and co-ordination of national policies and the promotion of integration programmes" in areas including communications, technology and legal matters.[83] On the basis of the above mandates the ECOWAS Council of Ministers adopted Directive C/DIR.1/08/11 on Fighting Cybercrime at its Sixty Sixth Ordinary session at Abuja, in August, 2011.[84] The adoption of the Directive was underscored by the need to curb cybercrime within the ECOWAS region as some Member States were beginning to gain global notoriety as major sources of email scams commonly known as the West African Letter Scam.[85] Accordingly, the Directive requires Member States to criminalizes cybercrime[86] including unauthorized access to a computer system;[87] unauthorized interference with the operation of a computer system;[88] unauthorized modification of computer data;[89] unauthorized interception of computer data;[90] computer fraud; [91] unauthorized manipulation of personal data;[92] and online child pornography.[93] The Directive also establishes a framework to facilitate international cybersecurity cooperation.[94]

In order to facilitate the development and harmonization of national cybersecurity laws in Member States, the Directive establishes binding obligations on Members to implement its provisions. Accordingly, Article 35 of the Directive declares that: "Member States shall adopt the necessary legislative, regulatory and administrative measures in order to comply with this Directive not later than 1st January, 2014".[95] However, some Member States have not complied with the obligations under the

82) Article 3 ECOWAS Treaty.

83) Articles 3(2) (a), 33 (2) and 57(1), Treaty of ECOWAS.

84) ECOWAS Directive C/DIR.1/08/11 on Fighting Cybercrime, adopted at the Sixty Sixth Ordinary Session of the ECOWAS Council of Ministers at Abuja, Nigeria (August 2011).

85) U. J. Orji, 'Curbing Advance Fee Fraud in Nigeria: An Analysis of the Regulatory Framework and Contemporary Challenges', International Company and Commercial Law Review, Issue 12, November 2011, pp. 408-421. See also A. Atta-Asamoah, 'Understanding the West African Cybercrime Process', African Security Review, Vol. 18, No. 4, pp.106-114.

86) Article 2 ECOWAS Directive on Cybercrime.

87) Article 4 ibid.

88) Article 6 ibid.

89) Articles 7 and 9 ibid.

90) Article 8 ibid.

91) Articles 10 and 11 ibid.

92) Article 12 ibid.

93) Article 16 ibid.

94) Article 33 (1) ibid.

95) Article 35 (1) ibid.

Directive. As of March, 2021, some ECOWAS Members including Guinea–Bissau, Liberia, and Sierra Leone[96] were yet to establish national cybersecurity laws, although there were ongoing initiatives to develop laws in those States.

The COMESA Model Cybercrime Bill

The Common Market for Eastern and Southern Africa (COMESA) is a free trade union that was formed in December, 1994 and aims to achieve regional integration by reducing barriers to cross border trade amongst Member States.[97] In line with its objectives, the COMESA developed a Model Cybercrime Bill in October 2011,[98] with a view to providing a uniform framework that would serve as a guide for the development of cybersecurity laws in Member States. Thus, the Model Cybercrime Bill provides a guide for the criminalization of offences against computer systems and data such as unauthorized access, data interference; data interception; misuse of digital devices; digital forgery; digital fraud, and cyber extortion.[99] However, the Bill does not establish any binding obligations on Member States to criminalize cybercrimes. As of March, 2021, COMESA Member States including Eritrea, Libya, Comoros, Swaziland, Democratic Republic of Congo, and South Sudan did not have cybercrime laws.[100]

The SADC Model Law on Computer Crime and Cybercrime

The Southern Africa Development Community (SADC) was founded in 1980 to promote economic integration and cooperation amongst Member States.[101] In March, 2012, the SADC adopted a Model Law on Computer Crime and Cybercrime[102] to serve as a guide for the development of cybercrime laws in SADC Member States. However, the model law does not impose any binding obligations on Members to

---

96) African Union and Symantec Corporation, Cybercrime & Cybersecurity Trends in Africa, Symantec Corporation and African Union, November, 2016, pp.53-55.

97) Articles 3 and 6, Treaty Establishing the Common Market for Eastern and Southern Africa (1994).

98) Official Gazette of the Common Market for Eastern and Southern Africa (COMESA) Vol. 16 No. 2 (15 October 2011).

99) Part VI COMESA Model Cybercrime Bill.

100) African Union and Symantec Corporation, Cybercrime & Cybersecurity Trends in Africa, Symantec Corporation and African Union, November, 2016, pp.53-55.

101) See <http://www.sadc.int/> last accessed on 18 March, 2021.

102) SADC Model Law on Computer Crime and Cybercrime Version 2.0 Adopted on 02 March 2012.

establish cybercrime laws. As of March, 2021, SADC Members including Democratic Republic of Congo, Lesotho, Mozambique, and Swaziland did not have cybercrime laws.

National Responses to Cybersecurity Governance in Africa

Notwithstanding, the fact that only eight AU Member State have ratified the AU Convention on Cyber Security,[103] many Member States have already established national frameworks for cybersecurity governance. For example, as of March, 2020, 39 States out of the 55 AU Member States had established cybersecurity laws, while 21 States had established national cybersecurity policies, 23 States also had national CERT frameworks (see Table 1 below). However, aside from the establishment of cybersecurity laws and policies, there appears to be very slow or no efforts towards developing other critical aspects of cybersecurity governance such as technical and organizational measures and user education at the national levels in AU Member States.

103) T. Jackson, 'Can Africa Fight Cybercrime and Preserve Human Rights?', BBC News, (10 April, 2015), available at <http://www.bbc.com/news/business-32079748>; D. Finnan, 'Lack of Laws Governing Cybercrime Making Africa a Safe Haven for Cyber Criminals (Interview)', Radio France Internationale, (16 February 2015), available at <http://www.english.rfi.fr/africa/20150215-lack-laws-governing-cybercrime-making-africa-safe-haven-cybercriminals-interview> last accessed on 18 March, 2021.

Table 1. A Summary of National Responses to Cybersecurity Governance in Africa (March, 2021)

	Country	Cybersecurity Legislation	National Cybersecurity Policy	Computer Emergency Response Teams (CERTS)
1	Algeria	√	No information	No information
2	Angola	√	None	None
3	Benin	√	√	√
4	Botswana	√	√	√
5	Burkina Faso	√	√	√
6	Burundi	√	None	None
7	Cameroon	√	None	√
8	Cape Verde	√	√	No information
9	Central African Republic	None	None	None
10	Chad	None	None	None
11	Comoros	None	None	None
12	Côte d'Ivoire	√	√	√
13	Democratic Republic of the Congo	None	None	None
14	Djibouti	√	None	None
15	Egypt	√	√	√
16	Equatorial Guinea	None	None	None
17	Eritrea	None	None	None
18	Ethiopia	√	√	√
19	Gabon	√	√	None
20	Gambia	√	In progress	None
21	Ghana	√	√	√
22	Guinea	√	None	None
23	Guinea-Bissau	None	None	None
24	Kenya	√	√	√
25	Lesotho	None	None	None
26	Liberia	In progress	None	None
27	Libya	None	None	√

	Country	Cybersecurity Legislation	National Cybersecurity Policy	Computer Emergency Response Teams (CERTS)
28	Madagascar	√	None	None
28	Malawi	√	In progress	√
29	Mali	√	None	None
30	Mauritania	√	√	None
31	Mauritius	√	√	√
32	Morocco	√	√	√
33	Mozambique	None	In progress	√
34	Namibia	√	None	None
35	Niger	√	None	None
36	Nigeria	√	√	√
37	Arab Saharawi Democratic Republic	No information	No information	No information
38	Republic of the Congo	None	None	None
39	Rwanda	√	√	√
40	São Tomé and Príncipe	√	None	None
41	Senegal	√	√	√
42	Seychelles	√	None	None
43	Sierra Leone	None	None	None
44	Somalia	None	None	None
45	South Africa	√	√	√
46	South Sudan	None	None	None
47	Sudan	√	√	√
48	Swaziland	In progress	None	None
49	Tanzania	√	None	√
50	Togo	√	None	None
51	Tunisia	√	√	√
52	Uganda	√	√	√
53	Zambia	√	In progress	√
54	Zimbabwe	√	√	None
55				

CHALLENGES TO CYBERSECURITY GOVERNANCE IN AFRICA

Aside from the absence of legal and policy frameworks for cybersecurity governance in many African States as seen in the table above, there are also other peculiar challenges arising from the absence of requisite institutional capacities in terms of cybercrime law enforcement.[104] For example, law enforcement authorities in many African States still lack capacities that are necessary to detect, investigate and prosecute cybercrime.[105] In this regard, an INTERPOL report recently observed the lack of investment and limited capacities to prevent, detect, and investigate cyber-attacks in many African countries, which is further driving cyber criminality on the continent.[106] Although, there have been various initiatives to build capacities in law enforcement authorities in some States, however, it appears that such initiatives have not yet achieved the intended results.[107] In some countries, policy makers have expressed a lack of interest in funding training for cybersecurity skills that will enhance cybercrime control due to fears over the dual use of such skills. For example, in 2016, it was reported that policy makers in Cameroon were in the process of launching cybersecurity skill development programs, but however feared that after completing the training program, the trainees could use the skills acquired to commit cybercrime.[108] Weak institutional capacity is also reflected in terms of

---

104) A. Fassassi and C. F. Akoussan, 'Cybercrime in Africa: Facts and Figures' , Sci Dev Net, (7 July,2016), available at <https://www.scidev.net/sub-saharan-africa/features/cybercrime-africa-facts-figures/> last accessed on 18 March, 2021; N. Kshetri, 'Cybercrime and Cybersecurity in Sub-Saharan African Economies', in Cybercrime and Cybercrime in the Global South, Palgrave Macmillan, 2013, pp.152-170.

105) African Union and Symantec Corporation (2016) Cyber Crime & Cyber Security Trends in Africa. United States: Symantec Corporation, pp.60, 61,63,66,70, and 83.

106) INTERPOL, Online African Organized Crime from Surface to Dark Web (INTERPOL: France, July 2020), p.67.

107) Ibid, pp.70, 83,134. See also.F.E. Eboibi, 'Concerns of Cyber Criminality in South Africa, Ghana, Ethiopia and Nigeria: Rethinking Cybercrime Policy Implementation and Institutional Accountability', Commonwealth Law Bulletin, (2020), Vol. 46, Issue 1, pp.78-99; M. Lucchetti, Cybercrime Legislation in Africa: Regional and International Standards, African Union/Council of Europe Joint Programme on Cyber Security and Cybercrime for African Diplomats (12 April, 2018: Addis Ababa), p.3, available at <https://au.int/sites/default/files/newsevents/workingdocuments/34122-wd-05.press_cybercrime_legislation _in_africa_12apr2018_matteo.l.pdf> last accessed on 18 March, 2021.

108) N. K. Chimtom, 'Cameroon's Dilemma in Fighting Cybercrime', African Independent (16 April, 2016), available at <https://www.africanindy.com/business/cameroons-dilemma-in-fighting-cybercrime-5073265> last

lack of up to date technological tools to enhance law enforcement and lack of awareness and expertise amongst law enforcement officials,[109] as well as the absence of requisite technical and infrastructural frameworks to promote cybersecurity.[110] Another indicator of weak institutional capacities is the absence of functional national CERTs to coordinate responses to cybersecurity threats in most African States.[111]

The challenge of weak institutional capacities can also be traced to the fact that most African States have not dedicated adequate financial resources to promoting cybersecurity governance initiatives.[112] Poor funding of cybersecurity initiatives is to a large extent responsible for the absence of highly skilled cybersecurity experts that will render cybersecurity governance services including assisting law enforcement authorities in the prevention, investigation or prosecution of cybercrime. [113] Another challenge that arises from poor funding is the limitation of research and development initiatives that would promote cybersecurity governance. To some extent, the poor government funding of cybersecurity initiatives is caused by the fact that cybersecurity is not really considered as a national security priority in many African States.[114] This is also not unconnected with the fact many African States face physical national security challenges such as terrorism which policy makers usually consider more pervasive than cybercrime and other cybersecurity challenges.[115]

---

accessed on 18 March, 2021. See also, N. Kshetri, 'Cybercrime and Cybersecurity in Africa', Journal of Global Information Technology Management (2019), Vol. 22, No.2, p.77

109) *Ibid*, p.10.

110) INTERPOL, Online African Organized Crime from Surface to Dark Web (INTERPOL: France, July 2020), p.67; S. Dlamini and C. Mbambo, 'Understanding Policing of Cybercrime in South Africa: The Phenomena, Challenges and Effective Responses', Cogent Social Sciences, (2019) Vol. 5:1, p.17.

111) Solutions Consulting (2018) West Africa Cybersecurity Indexing and Readiness Assessment. United States :Solutions Consulting, p.37

112) Serianu Limited, Africa Cybersecurity Report 2017: Demystifying Africa's Cyber *Security* Poverty Line (Kenya: Serianu Limited, 2017), p.9; N. Kshetri, 'Cybercrime and Cybersecurity in Africa', Journal of Global Information Technology Management (2019), Vol. 22, No.2, p.78; N. N. Schia, 'The Cyber Frontier and Digital Pitfalls in the Global South', Third World Quarterly, (2018), Vol. 39, No. 5, pp.821-837.

113) African Union and Symantec Corporation, Cyber Crime & Cyber Security Trends in Africa, United States: Symantec Corporation, 2017, pp.70, 76, 88, 89, and 92. See also, Serianu Limited, Africa Cybersecurity Report 2016, Kenya: Serianu Limited, 2016, p.46; W. Mcanyana and C. Brindley, Insight into The Cyber Threat Landscape in South Africa (Accenture: South Africa, 2020), p.6.

114) U.J Orji, International Telecommunications Law and Policy (Cambridge Scholars Publishing: United Kingdom, 2018), p. 369. See also, African Union and Symantec Corporation, Cyber Crime & Cyber Security Trends in Africa (Symantec Corporation: United States, 2016), p. 60; U. J. Orji, 'The African Union Convention on Cybersecurity: a Regional Response towards Cyber Stability', Masaryk University Journal of Law and Technology (2018) Vol. 12 (2), pp.119

Another major challenge to cybersecurity governance in most African States arises from lack of awareness by the end-users of ICT applications and information society services.[116] Lack of awareness amongst a large segment of Africa's growing ICT user population has been a major contributory factor to the increasing rates of cybercrime on the continent.[117] Many end-users of ICT products and services in Africa are getting connected to the Internet for the first time and lack basic knowledge to protect themselves from cyber threats and which exposes them to cyber-attacks.[118] This also raises grave concerns about the negative impact of cybercrime on African economies. For example, South Africa is reported to have the third highest number of cybercrime victims globally,[119] while a survey by Norton indicates that 70 percent of South Africans have fallen victim to cybercrime which is higher than the global average of 50 percent.[120] In Nigeria which has the largest Internet user population in Africa, it is estimated that over 17,600 bank customers lost over 39 million US Dollars in 2018 to due to cybercrime.[121]

---

115) M. Shuaibu and L.D. Bernsah, 'An Analysis of the Macroeconomic Impact of Insecurity on Nigeria: A Dynamic Modeling Approach', Journal of Social and Management Sciences, (2016) Vol.2 (1), pp. 3, 4, 6; L. Ploch, Countering Terrorism in East Africa: The U.S. Response. Congressional Research Service, (2010), R41473, p. 19. See Vanguard, Federal Government Committing Significant Share of 2017 Budget to North-East – Onyeama (2017), available at <https://www.vanguardngr.com/2017/02/fgcommittingsignificant-share-2017-budget-northeast-onyeama/> last accessed on 18 March, 2021; U.J. Orji, 'Regionalizing Cybersecurity Governance in Africa: An Assessment of Responses', in C. Samuel and M. Sharma, (eds.) Securing Cyberspace: International and Asian Perspectives, New Delhi, India: Institute for Defence Studies and Analyses & Pentagon Press, 2016, p.213.

116) M. Bada, B. Von Solms, and I. Agrafiotis, 'Reviewing National Cybersecurity Awareness for Users and Executives in Africa', International Journal on Advances in Security (2019), Vol. No. 1 &2, pp.108-118.

117) O. Regha, 'Aggressive Consumers Awareness Initiatives: A Proactive & Consistent Mechanism to Preventing E-fraud' in Nigerian E-Fraud Forum 2015 Annual Report: Improving and Securing the Cyber Environment, Central Bank of Nigeria: 2015, pp.10-13.

118) The Cyber Diplomat, 'Cybercrime in West Africa – An Overview' (18 April, 2020), available at <https://medium.com/@cyberdiplomacy/cybercrime-in-west-africa-an-overview-e3af22ebdb9a>; A. A. Odonkor, Unveiling the cost of cybercrime in Africa, CGTN (27/10/2020), available at <https://news.cgtn.com/news/2020-10-27/Unveiling-the-cost-of-cybercrime-in-Africa-UVhmu1PJeM/index.html> last accessed on 18 March, 2021.

119) See B. Koigi, 'South Africa has the third –highest number of Cybercrime Victims Globally, Report', Africa Tech, (4 July, 2020), available at <https://www.africabusinesscommunities.com/tech/tech-news/south-africa-has-third-highest-number-of-cybercrime-victims-globally-report/> last accessed on 18 March, 2021.

120) T. Jackson, 'Can Africa Fight Cybercrime and Preserve Human Rights?', BBC News, (10 April, 2015), available at <http://www.bbc.com/news/business-32079748> last accessed on 18 March, 2021.

121) M. Ogbonnaya, 'Cybercrime in Nigeria Demands Public-Private Action', Institute for Security Studies-ISS Today, (19 October, 2020), available at <https://www.issafrica.org/iss-today/cybercrime-in-nigeria-demands-public-private-action> last accessed on 18 March, 2021.

Lack of awareness by the end-users also raises serious concerns that Africa could become a "safe harbour" for cybercrime.[122] This is because most African States already lack efficient law enforcement capacities to tackle cybercrime as well as effective criminal justice delivery systems.[123] Thus, aside from lack of capacities for cybercrime control amongst law enforcement authorities in most African States[124], there also appears to be a lack of skills for administering cybercrime cases in the judiciary.[125] In addition, it is possible that few cybercrime cases which are eventually brought before the Court would spend very long trial periods. For example, in some African States it could take up to an average of five years for a High Court to determine a criminal matter that is not related to cybercrime.[126] Consequently, it is probable that cybercrime cases which are inherently technical and require skilled expertise and the use of digital evidence during trial may even take more years for determination. Therefore, with the challenge of lack of awareness, it is foreseeable that the impact of cybercrime on African economies will continue to rise with their increasing dependence on ICTs and the availability of broadband capacity, and criminal law enforcement mechanisms will not be able to provide enough deterrence to cybercrime.

---

122) L. Kharouni, 'Africa: A New Safe Harbour for Cyber criminals?', Trend Micro Research Paper, USA, Trend Micro Inc, 2013, pp.1-26.

123) C. M. Fombad, 'The Context of Justice in Africa: Emerging Trends and Prospects', in Evelyn Edroma (ed), Rethinking the Role of Law and Justice in Africa's Development: An Edited Volume of Discussion Papers, United Nations Development Programme: Addis Ababa, Ethiopia, June, 2013, pp.16 and 17. See also, M. Shaw and T. Reitano, 'The Evolution of Organized Crime and Illicit Trafficking in Africa, and its Implications for Citizen and State Security', in Evelyn Edroma (ed), ibid, p.38.

124) K. A. Barfi, et al, 'Internet Users and Cybercrime in Ghana: Evidence from Senior School in Brong Ahafo Region', Library Philosophy and Practice (e-Journal), 2018, 1715. See M. Sarrab, et al, 'Challenges of Computer Crime Investigation in North Africa's Countries', The International Arab Conference of Information Technology, 2013, pp1-6.

125) I. A. Yusuf, 'Nobody has been prosecuted for Cybercrime in Nigeria', The Nation, 16 April, 2017, available at <http://thenationlineng.net/nobody-prosecuted-cybercrime-nigeria/> last accessed on 18 March, 2021. See also, 'Cybercrime in Africa: Facts and Figures' (07/07/2016), available at <https://www.scidev.net/sub-saharan-africa/icts/feature/cybercrime-africa-facts-figures.html> last accessed on 18 March, 2021.

126) J. Agbonika and A. Musa, 'Delay in the Administration of Criminal Justice in Nigeria: Issues from a Nigerian Viewpoint', Journal of Law, Policy and Globalization, 2014, Vol.26, pp.126 -138. See also, Hon. Justice D. Mann, Curbing Delays in the Administration of Justice: Case Management in the Magistrate Courts. [A paper presented at the orientation for newly appointed Magistrates at National Judicial Institute, Abuja, 24 July, 2017], available at <http://www.nji.gov.ng/images/Workshop_Papers/2017/Orientation_Newly_Appointed_Magistrates/s2.pdf>; T. Soniyi, 'CJN Decries in Criminal Trials', Thisday, 18 April, 2016, available at <https://www.thisdaylive.com/index.php/2016/04/18/cjn-decries-delay-in-criminal-trials/amp/> last accessed on 18 March, 2021.

PROPOSALS FOR THE DEVELOPMENT OF OTHER ASPECTS OF CYBERSECURITY GOVERNANCE ASIDE FROM CRIMINAL LAW MEASURES

As seen in table 1 above, cybersecurity governance responses in Africa have been focused mainly on the development of criminal law measures. For example, with respect to African countries within the SADC it has been observed that their cybersecurity governance responses have been focused cybercrime offences and criminalizing online behavior.[127] With respect to African countries within the ECOWAS, it has been observed that financial constraints have also impeded the timely implementation of comprehensive governance measures in many Member States who are challenged by other development concerns which are considered priority areas that require increased government funding, such as curbing the spread of diseases, tackling widespread poverty, and promoting the sustainable exploitation of natural resources.[128] As such, there exists a lack of requisite capacities in terms of cybersecurity governance in many African countries[129] with more focus on the development of criminal law measures, and without an adequate development of other critical governance measures such as organizational measures,[130] user education[131] and international cooperation.[132] This section will make proposals on the development of those critical governance measures beyond criminal law measures.

---

127) E. Calandro, and N. Berglund, 'Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: the SADC Case' (2020), pp.10-11, available at <https://www.researchictafrica.net/wp/wp-content/uploads/2019/11/33_Calandro_Berglund_Unpacking-Cyber-Capacity-Building-1.pdf> last accessed on 18 March, 2021.

128) U.J Orji, 'An Inquiry into the Legal Status of ECOWAS Cybercrime Directive and the Implications of its Obligations for Member States' Computer Law & Security Review, 2019, Vol. 35 (6), p.14.

129) U.J Orji, International Telecommunications Law and Policy (Cambridge Scholars Publishing: United Kingdom, 2018), p. 369. See also, African Union and Symantec Corporation, Cyber Crime & Cyber Security Trends in Africa (Symantec Corporation: United States, 2016), p. 60; U. J. Orji, 'The African Union Convention on Cybersecurity: a Regional Response towards Cyber Stability', Masaryk University Journal of Law and Technology (2018) Vol. 12 (2), pp.119

130) N. Waag ⁻Cowling, 'Living below the Cyber Poverty Line: Strategic Challenges for Africa' Humanitarian Law & Policy (11 June, 2020), available at <https://blogs.icrc.org/law-and-policy/2020/06/11/cyber-poverty-line-africa/> last accessed on 18 March, 2021.

131) R. Butler and M. Butler, 'It Will Take Education, Not Just Legislation, To Take Cybercrime', The Conversation, (10 March, 2016), available at <https://www.theconversation.com/it-will-take-education-not-just-legislation-to-tackle-cybercrime-56030> last accessed on 18 March, 2021.

132) E. Tamarkin, 'The AU's Cybercrime Response: A Positive Start, but Substantial Challenges Ahead', ISS Policy Brief (January, 2015), Issue 73, p.3.

Building Institutional Capacities

It is imperative for African States to focus on building technical and human capacities in various institutions that are responsible for cybersecurity governance including CERTs and law enforcement authorities. In particular, CERTs and law enforcement authorities should be adequately funded and equipped and their personnel regularly trained and updated on emerging trends in cybercrime and cybersecurity governance.[133] Institutional capacity building for cybersecurity governance should also include the establishment of cybercrime units in law enforcement authorities. In addition, African States will have to ensure that judicial officers and prosecutors undergo constant training to keep up with developments in cybersecurity law and the handling of electronic evidence, as well as other related issues in the judicial administration of cybercrime cases.

Building Capacities for End-User Education

End-user education should be effectively integrated into national cybersecurity governance frameworks in African States. One way of building capacities for the implementation of end-user education is by imposing legal requirements on the manufacturers of ICT products, electronic service providers (such as financial institutions) and communications service providers to integrate end-user education components in their products and services. For example, banks that provide electronic/online banking services could be required to develop mandatory cybersecurity awareness programmes to educate consumers on the secure usage of such services. Failure to fulfill such obligations by service providers should give rise to civil and regulatory liabilities.[134]

---

133) N. Waag ⁻Cowling, 'Living below the Cyber Poverty Line: Strategic Challenges for Africa', Humanitarian Law & Policy (11 June, 2020), available at <https://blogs.icrc.org/law-and-policy/2020/06/11/cyber-poverty-line-africa/> last accessed on 18 March, 2021.

134) For example in the United States, banks have been held liable for failing to create an electronic banking environment that will ensure consumer protection. See Ognibene v. Citibank (446 NYS 2d 845 (CIV.Ct.1981).In that case, a rogue standing near a bank's ATM terminal memorized the personal identification number (PIN) of a cardholder who was using the machine. The rogue pretended to be servicing the ATM terminal and used an adjacent telephone to conduct a fictitious telephone conversation with his employees, after which he asked the cardholder to let him have the use of his card to ensure the terminal was in order. After withdrawing the money by keying in the number, the rogue returned the cardholder saying all was well. The cardholder contested the banks right to debit his account with the amount withdrawn by the rogue, claiming that the bank had failed to introduce a

Another way of building capacities for end-user education is through the establishment of policies that will encourage institutions such as universities, non-governmental organizations, and other stake holders to promote end-user awareness on cybersecurity. Such policies could also create incentives for institutions that are engaged in research and development initiatives to enhance end-user awareness on cybersecurity. Imposing a form of social corporate responsibility obligation on mass media organizations to promote cybersecurity awareness will also help in creating a culture of cybersecurity amongst end-users in African States.

Building Capacities to Enhance the Implementation of Technical Solutions to Cybersecurity

African States may have to consider establishing legal obligations that will require the manufacturers/vendors and providers of ICT products and services to integrate the implementation of technical protection measures in such products and services before making them available to end-users. Capacities for technical protection can also enhanced by establishing obligations on network service providers and end-users to report cybersecurity incidents to the appropriate authorities such as CERTs. For example, in Nigeria, the Cybercrimes Act imposes obligations on persons or institutions that operate a computer network to report cyber threats to the national CERT Coordination Center so that the National CERT can take the necessary measures to address such issues.[135] In addition, the Central Bank of Nigeria's Risk-based Cybersecurity Framework and Guidelines for Deposit money banks and Payment Service Providers imposes a similar reporting obligation banks and electronic payment service providers by requiring them "to report all cyber-incidents whether successful or not immediately after such incident was identified to the Director of Banking Supervision of the CBN".[136] The implementation of such obligations aims to facilitate timely national responses to cybersecurity incidents that may affect data held on the computer systems and networks of organizations including banks and financial institutions that provide electronic banking and payment services, and also helps to timely mitigate the effect and spread of cybersecurity threats.

---

safe method for the use of a card. The Court held that the bank had been negligent in not taking measures to combat fraud and that the bank ought to have provided the cardholder with sufficient information to handle such dangers.

135) Section 21(1) Cybercrimes (Prohibition and Prevention, etc) Act, 2015.

136) Central Bank of Nigeria, Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers, 25 June, 2018, at paragraph 7.6, p.10.

Establishment of Computer Emergency Response Teams (CERTs)

It is imperative for African States to timely establish well equipped and functional national CERTs to enhance the protection of their national critical information infrastructure and their capabilities to respond to cybersecurity threats in a timely and coordinated manner. As seen in the table above, only 23 African States had national CERT frameworks. However, there are also indications that CERTs are not actually functioning in some African States that have formally established CERT frameworks as some of the established CERTs appear to be inactive or offline[137] and therefore not providing critical computer emergency response services that qualify them as CERTs. This implies that many African States still do not have the requisite national capacity to effectively provide emergency responses to cybersecurity threats, even though they may have established CERTs. Therefore, there is need to ensure that established CERTs are fully functional so that they can efficiently provide services in their States.

Building Capacities for the Regional Cooperation on Cybersecurity

Cybersecurity issues are inherently transnational due to the ubiquitous nature of electronic communications networks. This state of affairs underscores the need for regional and international cooperation on cybersecurity governance. In order to enhance such cooperation in the African context, it will be necessary for the African Union to establish an institutional framework for cybersecurity governance that is similar to the European Information Security Agency (ENSIA)[138] to coordinate regional cybersecurity efforts and responses to cybersecurity incidents. Also the establishment of such regional institutional framework can enhance global cybersecurity cooperation and further serve as a forum for the dissemination of information and national best practices amongst African States. A legal basis may be found for the establishment of a network security agency within the African Union framework under Article 32 of the African Union Convention on Cybersecurity which provides for an operational mechanism for the Convention.[139] Some of the functions of the

---

137) G. van Zyl, 'Africa Lacks Computer Emergency Response Team Readiness', IT Web Africa, 27 May, 2014, available at <http://www.itwebafrica.com/m/news/zw2Wo44AaJQDo>; Africa Cert <africacert.org/African-csirts> last accessed on 18 March, 2021.

138) EC Regulation No 460/2004 establishing the European Network and Information Security Agency.

Convention's operational mechanism include:

(1) Promoting the adoption and implementation of measures to strengthen cyber security in electronic services and combating cybercrime and human rights violations in cyberspace;

(2) Advising African governments on measures to promote cybersecurity and combat cybercrime; and;

(3) Analyzing the criminal behaviors of cyberspace users within Africa and transmitting such information to competent national authorities. [140]

The above mandates may be broadly interpreted to create a regional network agency which is similar to the ENISA which was established in 2004 by the European Commission to promote cybersecurity and critical information infrastructure protection.[141] The Agency serves as a center of excellence for Member States of the European Union and European institutions on cybersecurity issues. Its responsibilities include providing advice and recommendations on cybersecurity and disseminating information on standards for best practices.[142] A regional network agency that is established under article 32 of the Convention may also function as a regional CERT where its mandate is enlarged to function as such.[143]

Promoting Private Sector Participation

The private sector has an enormous role to play in promoting cybersecurity governance in African States. Following market liberalization in several economic sectors in Africa, the private sector now controls significant segments of networked critical sectors in African States. Such critical sectors include banking and financial services, broadcasting services and telecommunications.[144] This state of affairs makes the private sector a critical stakeholder in promoting cybersecurity and protecting

---

139) U. J. Orji, 'Multilateral Legal Responses to Cybersecurity in Africa: Any Hope for Effective International Cooperation?' in M. Maybaum, et al (eds.), Architectures in Cyberspace- 7th International Conference on Cyber Conflict, NATO CCD COE, Tallinn, Estonia, p.116.

140) Article 32 African Union Convention on Cyber Security and Personal Data Protection

141) Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency.

142) See <http://www.enisa.europa.eu/>.

143) U. J. Orji, 'Multilateral Legal Responses to Cybersecurity in Africa: Any Hope for Effective International Cooperation?' in M. Maybaum, et al (eds.), Architectures in Cyberspace- 7th International Conference on Cyber Conflict, NATO CCD COE, Tallinn, Estonia, 2015, p.116.

144) M.D.J. Williams, et al, Africa's ICT Infrastructure: Building on the Mobile Revolution, World Bank: Washington DC, 2011, pp.9, 11, 15 -16.

critical information infrastructure. Therefore, it is imperative for national cybersecurity governance frameworks to recognize the strategic position of the private sector in promoting cybersecurity.[145] One way of achieving this, is for cybersecurity laws and policies to create clear frameworks for cooperation between government agencies and private sector organizations through arrangements for the sharing of information and critical resources that can enhance responses to cyber incidents that affect national critical infrastructure sectors or through other public-private partnership arrangements. Public-private partnerships are also usually very important in setting cybersecurity standards on issues including software accreditation, public key infrastructure (PKI) regulation and end-user education. Public-private partnership arrangements can also be used to fund the operation of national CERTs.

CONCLUDING REMARKS

African States still lack efficient capacities and resources for cybersecurity governance. This absence of capacities and resources remains a major contributory factor that has been responsible for creating an enabling environment for the rising trend of cybercrime in African States. Although, most African States have established criminal law measures to promote cybersecurity governance, however standing alone, such measures would produce very little impact in terms of minimizing cybersecurity vulnerabilities. Therefore, only criminal law measures would never be able enough to deter cybercrime or minimize exposure to cybersecurity threats in Africa's information society. This state of affairs requires that the governments of African States should actively go beyond the establishment of criminal law measures in their cybersecurity governance responses in order to effectively cover other critical aspects of cybersecurity governance including technical and organizational measures and user education. This is also imperative given the peculiar challenges that impede effectiveness of cybercrime law enforcement measures in Africa. In concluding, it is important to point out that there can be no silver bullet for addressing Africa's cybersecurity challenges, however there is a higher probability that the timely implementation of holistic approaches to cybersecurity governance would reduce vulnerabilities in Africa's information society.

---

145) ITU-D Secretariat, ITU Study Group Q.22/1 Report on Best Practices for a National Approach to Cybersecurity: A Management Framework for Organizing National Cybersecurity Efforts, Geneva, ITU, January, 2008, p.19.

References

A. Odonkor, Unveiling the cost of cybercrime in Africa, CGTN (27/10/2020), available at <https://news.cgtn.com/news/2020-10-27/Unveiling-the-cost-of-cybercrime-in-Africa-UVhmu1PJeM/index.html>.

A. Allotey, 'Ghana Loses $230 Million to Cyber Criminals – CID', Citinews (4 October, 2018), available at <https://citinewsroom.com/2018/10/04/ghana-loses-230m-to-cyber-criminals-cid/>.

A. Atta-Asamoah, 'Understanding the West African Cybercrime Process', African Security Review, Vol. 18, No. 4.

A. Barfi, et al, 'Internet Users and Cybercrime in Ghana: Evidence from Senior School in Brong Ahafo Region', Library Philosophy and Practice (e-Journal), 2018, 1715.

A. Fassassi and C. F. Akoussan, 'Cybercrime in Africa: Facts and Figures', Sci Dev Net, (7 July, 2016), available at <https://www.scidev.net/sub-saharan-africa/features/cybercrime-africa-facts-figures/>.

A. Odonkor, Unveiling the cost of cybercrime in Africa, CGTN (27/10/2020), available at <https://news.cgtn.com/news/2020-10-27/Unveiling-the-cost-of-cybercrime-in-Africa-UVhmu1PJeM/index.html>.

A. Yusuf, 'Nobody has been prosecuted for Cybercrime in Nigeria', The Nation, 16 April, 2017, available at <http://thenationlineng.net/nobody-prosecuted-cybercrime-nigeria/>.

Africa Cert <africacert.org/African-csirts>.

African Union (AU) Convention on Cyber Security and Personal Data Protection, EX.CL/846(XXV) adopted at the 23rd Ordinary Session of the Assembly of the African Union (Malabo, 27th June 2014).

African Union and Symantec Corporation, Cyber Crime & Cyber Security Trends in Africa, United States: Symantec Corporation, 2016.

African Union Convention on Cyber Security and Personal Data Protection.

African Union, 'African Union in a Nutshell', available at <http://www.au.int/en/abut/nutshell>.

African Union, List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection, (18/06/2020), available at <https//au.int/sites/default/files/treaties/29560-sl-African%20Union%Convention%20On%Cyber%20Security%20And%Personal%20Data%20 Protection.pdf>.

B. Koigi, 'South Africa has the third –highest number of Cybercrime Victims Globally, Report', Africa Tech, (4 July, 2020), available at <https://www.africabusiness communities.com/tech/tech-news/south-africa-has-third-highest-number-of-cybercrime-victims-globally-report/>.

B. T. Mbatha, D.N. Ocholia and J.L. Roux, 'Diffusion of ICTs in Selected Government Departments in KwaZulu –Natal, South Africa', Information Development, (2011) , Vol. 27 (4).

'Cybercrime Impact and the Way Forward', Business & Financial Times Online (5 November, 2018), available at <https://www.thebftonline.com/2018/features/cybercrime-impact-and-the-way-forward/>.

'Cybercrime in Africa: Facts and Figures' (07/07/2016), available at <https://www.scidev.net/sub-saharan-africa/icts/feature/cybercrime-africa-facts-figures.html>.

C. Reed, 'The Law of Unintended Consequences – Embedded Business Models in IT Regulation', Journal of Information Law and Technology, 2007 (2).

Center for Strategic and International Studies, Net Losses: Estimating the Global Cost of Cybercrime (Center for Strategic and International Studies: Washington, DC, June, 2014).

Central Bank of Nigeria, Risk-Based Cybersecurity Framework and Guidelines for Deposit Money Banks and Payment Service Providers, 25 June, 2018.

COMESA Model Cybercrime Bill, Official Gazette of the Common Market for Eastern and Southern Africa (COMESA) Vol. 16 No. 2 (15 October 2011).

Constitutive Act of the African Union, adopted the Thirty-Sixth Ordinary Session of the Assembly of Heads of State and Government, 11 July, 2000 (Lome, Togo).

Council of Europe, Convention on Cybercrime, 41 I.L.M. 282 (Budapest, 23.XI, 2001).

D. Finnan, 'Lack of Laws Governing Cybercrime Making Africa a Safe Haven for Cyber Criminals (Interview)', Radio France Internationale, (16 February 2015), available at <http://www.english.rfi.fr/africa/20150215-lack-laws-governing-cybercrime-making-africa-safe-haven-cybercriminals-interview>.

D. Olowu, 'Environmental Governance Challenges in Kiribati: An Agenda for Legal and Policy Responses', Law, Environment and Development Journal (2007) Vol. 3, Issue 3.

E. Calandro, and N. Berglund, 'Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: the SADC Case' (2020), available at <https://www.researchictafrica.net/wp/wp-content/uploads/2019/11/33_Calandro _Berglund_Unpacking-Cyber-Capacity-Building-1.pdf>.

E. Tamarkin, 'The AU's Cybercrime Response: A Positive Start, but Substantial Challenges Ahead', ISS Policy Brief (January, 2015), Issue 73.

EC Regulation No 460/2004 establishing the European Network and Information Security Agency.

ECOWAS Directive C/DIR.1/08/11 on Fighting Cybercrime, adopted at the Sixty Sixth Ordinary Session of the ECOWAS Council of Ministers at Abuja, Nigeria (August 2011).

F. Fukuyama, 'What Is Governance?', CGD Working Paper 314 (Washington, DC: Center for Global Development, January 2013).

F.E. Eboibi, 'Concerns of Cyber Criminality in South Africa, Ghana, Ethiopia and Nigeria: Rethinking Cybercrime Policy Implementation and Institutional Accountability', Commonwealth Law Bulletin, (2020), Vol. 46, Issue 1.

G. Marco, 'The Slow Wake of a Global Approach against Cybercrime', Computer Law Review International, 2006, Issue 5.

G. Marco, Understanding Cybercrime: A Guide for Developing Countries, Geneva, ITU, 2009.

G. Sesan, et al, Economic Cost of Cybercrime in Nigeria, Paradigm Initiative: Nigeria: 2013, available at <https://pinigeria.org/download/download/cybercost.pdf>.

G. van Zyl, 'Africa Lacks Computer Emergency Response Team Readiness', IT Web Africa, 27 May, 2014, available at <http://www.itwebafrica.com/m/news/zw2Wo44AaJQDo>.

GSMA, The Mobile Economy Africa 2020 (GSMA: London, 2020).

Hon. Justice D. Mann, Curbing Delays in the Administration of Justice: Case Management in the Magistrate Courts. [A paper presented at the orientation for newly appointed Magistrates at National Judicial Institute, Abuja, 24 July, 2017], available at <http://www.nji.gov.ng/images/Workshop_Papers/2017/Orientation_Newly_Appointed_Magistrates/s2.pdf>.

I. Gagliardone and N. Sambuli, 'Cyber Security and Cyber Resilience in East Africa', Global Commission on Internet Governance Paper Series, No. 15 (May, 2015).

International Bureau of Education, 'Concept of Governance', available at <http://www.ibe.unesco.org/en/geqaf/technical-notes/concept-governance>.

Internet Crime Complaint Center, 2010 Internet Crime Report (National White Collar Crime Center: United States, 2011).

Internet Crime Complaint Center, 2013 Internet Crime Report (National White Collar Crime Center: United States, 2014).

INTERPOL, Online African Organized Crime from Surface to Dark Web (INTERPOL: France, July 2020).

ITU High Level Experts Group [HLEG] ITU Global Cyber-SecurityAgenda (GCA) High Level Experts Group [HLEG] Global Strategic Report, Geneva, ITU 2008.

ITU Study Group Q.22/1, Report on Best Practices For A National Approach

To Cybersecurity: A Management Framework For Organizing National Cybersecurity Efforts [Draft], Geneva, ITU-D, January 2008.
ITU, 'Challenges to Building a Secure Information Society', 2007 World Information Society Report: Beyond WSIS, ITU, Geneva, 2007.
ITU-D Secretariat, ITU Study Group Q.22/1 Report on Best Practices for a National Approach to Cybersecurity: A Management Framework for Organizing National Cybersecurity Efforts, Geneva, ITU, January, 2008.
J. Agbonika and A. Musa, 'Delay in the Administration of Criminal Justice in Nigeria: Issues from a Nigerian Viewpoint', Journal of Law, Policy and Globalization, 2014, Vol.26.
J. Graham, B. Amos and T. Plumptre, Governance Principles for Protected Areas in the 21st Century 5 (Ottawa: Institute of Governance, 2003).
L. Kharouni, 'Africa: A New Safe Harbour for Cyber criminals?', Trend Micro Research Paper, USA, Trend Micro Inc, 2013.
L. Ploch, Countering Terrorism in East Africa: The U.S. Response. Congressional Research Service, (2010), R41473.
L. S. and K. Signe, 'Global Cybercrimes and Weak Cybersecurity Threaten Businesses in Africa', Brookings: Africa in Focus (30 May, 2018), available at <https://www.brookings.edu/blog/africa-in-focus/2018/05/30/global-cybercrimes-and-weak-cybersecurity-threaten-businesses-in-africa/>.
M. Bada, B. Von Solms, and I. Agrafiotis, 'Reviewing National Cybersecurity Awareness for Users and Executives in Africa', International Journal on Advances in Security (2019), Vol. No. 1 &2.
M. Dunn, A Comparative Analysis of Cybersecurity Initiatives Worldwide, World Summit on Information Society (WSIS) Thematic Meeting on Cybersecurity, Geneva, ITU: June 2005.
M. Fombad, 'The Context of Justice in Africa: Emerging Trends and Prospects', in Evelyn Edroma (ed), Rethinking the Role of Law and Justice in Africa's Development: An Edited Volume of Discussion Papers, United Nations Development Programme: Addis Ababa, Ethiopia, June, 2013.
M. K. Luka and I. A. Frank, 'The Impacts of ICTs on Banks: A Case Study of the Nigerian Banking Industry', International Journal of Advanced Computer Science and Applications (2012), Vol. 3 (9).
M. Andrianaivo and Kangni Kpodar, 'ICT, Financial Inclusion, and Growth: Evidence from African Countries', IMF Working Paper, WP/11/73 (2011).
M. Lucchetti, Cybercrime Legislation in Africa: Regional and International Standards, African Union/Council of Europe Joint Programme on Cyber Security and Cybercrime for African Diplomats (12 April, 2018: Addis Ababa), available at <https://au.int/sites/default/files/

newsevents/workingdocuments/34122-wd-05.press_cybercrime_legislation_in_africa_12apr2018_matteo.l.pdf>.

M. M. Tamayao, What Is Governance?, available at <https://tamayaosbc.wordpress.com/2014/08/ 21/what-is-governance/>.

M. Ogbonnaya, 'Cybercrime in Nigeria Demands Public-Private Action', Institute for Security Studies-ISS Today, (19 October, 2020), available at <https://www.issafrica.org/iss-today/cybercrime-in-nigeria-demands-public-private-action>.

M. Sarrab, et al, 'Challenges of Computer Crime Investigation in North Africa's Countries', The International Arab Conference of Information Technology, 2013.

M. Shuaibu and L.D. Bernsah, 'An Analysis of the Macroeconomic Impact of Insecurity on Nigeria: A Dynamic Modeling Approach', Journal of Social and Management Sciences, (2016) Vol.2 (1).

M.D.J. Williams, et al, Africa's ICT Infrastructure: Building on the Mobile Revolution, World Bank: Washington DC, 2011.

Miniwatts Marketing Group, 'Internet Usage Statistics for Africa', (31 December, 2020), available at <http://www.internetworldstats.com/stats1.htm>.

N. Allen, 'Africa's Evolving Cyber Threats', African Center for Strategic Studies, (19 January, 2021), available at <https://africacenter.org/spotlight/africa-evloving-cyber-threats/>.

N. K. Chimtom, 'Cameroon's Dilemma in Fighting Cybercrime', African Independent (16 April, 2016), available at <https://www.africanindy.com/business/cameroons-dilemma-in-fighting-cybercrime-5073265>.

N. Kshetri, 'Cybercrime and Cybersecurity in Africa', Journal of Global Information Technology Management (2019), Vol. 22, No.2.

N. Kshetri, 'Cybercrime and Cybersecurity in Sub-Saharan African Economies', in Cybercrime and Cybercrime in the Global South, Palgrave Macmillan, 2013.

N. N. Schia, 'The Cyber Frontier and Digital Pitfalls in the Global South', Third World Quarterly, (2018), Vol. 39, No. 5.

N. Waag –Cowling, 'Living below the Cyber Poverty Line: Strategic Challenges for Africa' Humanitarian Law & Policy (11 June, 2020), available at <https://blogs.icrc.org/law-and-policy/2020/06/11/cyber-poverty-line-africa/>.

Nigerian Communications Commission (NCC), Final Report on Effects of Cyber Crime on Foreign Direct Investment and National Development (NCC: Abuja, 2017).

Nigerian Cybercrimes (Prohibition and Prevention, etc) Act, 2015.

O. Regha, 'Aggressive Consumers Awareness Initiatives: A Proactive &

Consistent Mechanism to Preventing E-fraud' in *Nigerian E-Fraud Forum 2015 Annual Report: Improving and Securing the Cyber Environment*, Central Bank of Nigeria: 2015. *Ognibene v. Citibank* (446 NYS 2d 845 (CIV.Ct.1981).

P. Wallet, Information and Communication Technology (ICT) in Education in Sub-Saharan Africa: A Comparative Analysis of basic e-readiness in Schools (UNESCO Institute for Statistics: Canada, 2015).

R. Bahrini and A. Qaffas, 'Impact of Information and Communication Technology on Economic Growth: Evidence from Developing Countries', Economies (March, 2019) Vol. 7 (21).

R. Butler and M. Butler, 'It Will Take Education, Not Just Legislation, To Take Cybercrime', The Conversation, (10 March, 2016), available at <https://www.theconversation.com/it-will-take-education-not-just-legislation-to-tackle-cybercrime-56030>.

R. Flores, et al, Cybercrime in West Africa: Poised for an Underground Market (Trend Micro and INTERPOL, 2017).

R. Ponelis and M. A. Holmer, 'ICT in Africa: Building a Better Life for all', Information Technology for Development (2015).

Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency.

Rubicon Computer Systems v. United Paints Limited (2000) 2 TCLR 453.

S. Dlamini and C. Mbambo, 'Understanding Policing of Cybercrime in South Africa: The Phenomena, Challenges and Effective Responses', Cogent Social Sciences, (2019) Vol. 5:1.

S. Schjolberg, 'The History of Global Harmonization on Cybercrime Legislation - the Road to Geneva', (2008), available at <http://www.cybercrime law.net/documents/ cybercrime_ history.pdf>.

SADC Model Law on Computer Crime and Cybercrime Version 2.0 Adopted on 02 March 2012.

Serianu Limited, Africa Cyber Security Report 2017: Demystifying Africa's Cyber Security Poverty Line (Serianu Limited: Kenya, 2017).

Serianu Limited, Africa Cybersecurity Report 2016, Kenya: Serianu Limited, 2016.

Serianu Limited, Africa Cybersecurity Report 2018: Kenya (Kenya: Serianu Limited, 2018).

Solutions Consulting, West Africa Cybersecurity Indexing and Readiness Assessment (United States: Solutions Consulting, 2018).

Solutions Consulting, West Africa Cybersecurity Indexing and Readiness Assessment (Solutions Consulting: Florida, United States).

T. J. McIntyre, 'Computer Crime in Ireland: A Critical Assessment of the Substantive Law', Irish Criminal Law Journal, 2005, Vol. 15 (1).

T. Jackson, 'Can Africa Fight Cybercrime and Preserve Human Rights?', BBC News, 10 April, 2015, available at <http://www.bbc.com/news/business-32079748>.

T. Mastile, 'South Africa Loses R.5.7 Billion Annually to Cybercrime', CNBC Africa, 12 February, 2015, available at <http://www.cnbcafrica.com/news/special-report/2014/06/10/safrica-loses-r57-billion-annually-to-cybercrime>.

T. Sewart, 'Time to Drop the Bomb', *Computers & Law,* 2003 *Vol.*14 (4).

T. Soniyi, 'CJN Decries in Criminal Trials', *Thisday*, 18 April, 2016, available at <https://www.thisdaylive.com/index.php/2016/04/18/cjn-decries-delay-in-criminal-trials/amp/>.

T.J. McIntyre, 'Computer Crime in Ireland: A Critical Assessment of the Substantive Law', *Irish Criminal Law Journal*, 2005, Vol. 15 (1).

The Cyber Diplomat, 'Cybercrime in West Africa — An Overview' (18 April, 2020), available at <https://medium.com/@cyberdiplomacy/cybercrime-in-west-africa-an-overview-e3af22ebdb9a>.

Treaty Establishing the Common Market for Eastern and Southern Africa (1994).

U. J. Orji, 'Curbing Advance Fee Fraud in Nigeria: An Analysis of the Regulatory Framework and Contemporary Challenges', International Company and Commercial Law Review, Issue 12, November 2011.

U. J. Orji, 'Examining Missing Cybersecurity Governance Mechanisms in the African Union Convention on Cybersecurity and Personal Data Protection', Computer Law Review International, October, 2014, Issue 5.

U. J. Orji, 'Multilateral Legal Responses to Cybersecurity in Africa: Any Hope for Effective International Cooperation?' in M. Maybaum, et al (eds.), Architectures in Cyberspace- 7th International Conference on Cyber Conflict, NATO CCD COE, Tallinn, Estonia, 2015.

U. J. Orji, 'Protecting Consumers from Cybercrime in the Banking and Financial Sector: An Analysis of the Legal Response in Nigeria', Tilburg Law Review (2019) Vol. 24(1).

U. J. Orji, 'The African Union Convention on Cybersecurity: a Regional Response towards Cyber Stability', Masaryk University Journal of Law and Technology (2018) Vol. 12 (2).

U. J. Orji, Cybersecurity Law and Regulation, The Netherlands, Wolf Legal Publishers, 2012.

U. J. Orji, 'An Inquiry into the Legal Status of ECOWAS Cybercrime Directive and the Implications of its Obligations for Member States' Computer Law & Security Review, 2019, Vol. 35 (6).

U. J. Orji, International Telecommunications Law and Policy (Cambridge

Scholars Publishing: United Kingdom, 2018).

U. J. Orji, 'Regionalizing Cybersecurity Governance in Africa: An Assessment of Responses', in C. Samuel and M. Sharma, (eds.) Securing Cyberspace: International and Asian Perspectives, New Delhi, India: Institute for Defence Studies and Analyses & Pentagon Press, 2016.

'Understanding the Concept of Governance', available at <https://www.gdrc.org/u-gov/governance-understand.html>.

UNODC, Comprehensive Study on Cybercrime (Draft – February 2013), United Nations, New York, 2013.

Vanguard, Federal Government Committing Significant Share of 2017 Budget to North-East – Onyeama (2017), available at <https://www.vanguardngr.com/2017/02/fgcommittingsignificant-share-2017-budget-northeast-onyeama/>.

W. Mcanyana and C. Brindley, Insight into The Cyber Threat Landscape in South Africa (Accenture: South Africa, 2020).

Tools, Techniques and Underground Networks of Yahoo-Boys in Ibadan City, Nigeria

*Usman Adekunle Ojedokun, Ph.D.**
Lecturer
Department of Sociology
University of Ibadan

Ayomide Augustine Ilori
Ph.D. Candidate
Department of Sociology
University of Ibadan

Abstract

Despite the fact that the online criminal activities of Nigerian cyberfraudsters popularly known as the Yahoo-boys has attracted tremendous scholarly attention, little empirical information exists on their operational tools, techniques and underground networks. Hence, this study was motivated by the need to fill this observed gap. Social learning theory was adopted as theoretical guide while in-depth interview was principally deployed for data collection. Snowball sampling technique was utilized for the selection of 11 Yahoo-boys operating in Ibadan city. The results showed that Yahoo-boys who became wealthy through cyber fraud perpetration were being imitated by their peers who saw them as role models. Two major categories of operational tools were generally deployed by the Yahoo-boys for crime commission and illicit cash flows. Underground online forums, foreign criminal contacts and abroad-based criminal associates constituted the major sources of their operational tools and positively reinforced them towards cyber fraud. Yahoo-boys invested huge capital in the procurement of operational tools because they positively defined cyber fraud as a profitable business. There is the need for global law enforcement agencies and relevant international cybercrime-fighting institutions to constantly review and analyze the latest tools and techniques being employed by cyberfraudsters to effectively curtail their illegal activities.

Keywords

Cyberfraudsters, Cybercrime, Cyber fraud, Tools, Techniques, Underground Networks, Yahoo-boys, Nigeria

* Direct correspondence to Usman Adekunle Ojedokun, Ph.D., Lecturer, Department of Sociology, University of Ibadan; uaojedokun@gmail.com.
* http://dx.doi.org/10.36889/IJCJ.2021.003.
* Received 8 March 2021; Revised 19 May 2021; Accepted 20 May 2021; Available online 2 June 2021.
INTERNATIONAL JOURNAL OF CRIMINAL JUSTICE, Vol. 3 Issue 1, June 2021, 99-122

INTRODUCTION

The notoriety of Nigerian cyberfraudsters popularly known as the Yahoo-boys has consistently positioned Nigeria among the major cybercrime hubs in the world. Indeed, different international organizations and law enforcement agencies such as the United Nations Office on Drugs and Crime (UNODC), the International Criminal Police Organization (INTERPOL), the Federal Bureau of Investigation (FBI) amongst others have over time attested to the criminal ingenuity and the devastating transnational socio-economic impacts of Nigerian cyberfraudsters (Aderinto & Ojedokun 2017; Ibrahim 2016; Internet Crime Complaint Centre 2014; This Day, 2016).

Yahooboyism, a term which emerged in Nigeria in the early 2000s, is locally used to describe a criminal subculture of youths involved in cyber fraud perpetration (Adeniran 2008; Ajayi 2019; Ojedokun 2010). The criminal exploits of Yahoo-boys are not only recognized by the federal government of Nigeria to be a serious problem, they have also become a major cause for concern for other cyberspace users worldwide (Ojedokun & Eraye 2012; This Day 2016). In August 2019, FBI arrested a Nigerian cybercrime syndicate in the United States of America that defrauded its victims of approximately $3 billion through fraudulent wire transfers, business email compromise (BEC) frauds, and dating/romance scams (Oladimeji, 2019; Premium Times, 2019). Similarly, the Dubai Police in June 2020 apprehended a suspected cybercriminal gang headed by a Nigerian for allegedly planning and engaging in cyber fraud worth AED 1.6 billion ($435 million) on a global scale (Vanguard, 2020). Furthermore, the Nigeria Deposit Insurance Corporation's (NDIC) 2014 report stated that frauds on the e-payment platform of the Nigerian banking sector increased by 183% between 2013 and 2014 alone (This Day, 2016).

Despite the fact that the online criminal activities of Nigerian cyberfraudsters have attracted tremendous scholarly attention (Jegede, Elegbeleye, Olowookere & Olorunyomi 2016; Ogunleye, Ojedokun & Aderinto 2019; Tade & Aliyu 2011), there is paucity of empirical information on the tools, techniques and underground networks that this group of criminals are relying upon for the facilitation and sustenance of their criminality. Hence, a study of this nature is significant because

it is capable of promoting knowledge and deepening public understanding about a grossly unresearched aspect of cyber-criminality.

Generally, tools, techniques and underground networks constitute important resources for criminal enterprises (Andress & Winterfield 2014; Hutchings & Benham-Hutchings, 2009). Pastrana, Hutchings, Caines and Butterfly (2018) state that cyber-criminality is to a great extent driven by an active underground economy where attack tools and services are not only being traded, but where cyberattacks are also monetized. Similarly, Portnoff et al. (2017) assert that cybercriminals usually rely on underground cyber forums to establish trade relationships and facilitate the exchange of illicit goods and services such as stolen credit card numbers, compromised hosts, and online credentials.

Allodi (2017) claims that the rise of cyber-security challenges coincides with the emergence of underground economy where attack tools and services are easily accessible at low cost or even for free. In their own contribution, Sood and Enbody (2013) identify the three major types of actors in the underground cyber community as including the providers or producers, the advertisers, and the buyers. Pastrana et al. (2018) maintain that the sense of anonymity associated with underground forums as well as the ease of access to attack tools and services which they offer make them attractive to cybercriminals. In the same vein, Leukfeldt, Kleemans and Stol (2017) note that underground forums offer an environment where cybercriminals are able to learn new tricks and plan attacks as well as search for co-offenders with specific knowledge, and procure criminal tools. Some of the items that are most commonly traded in the underground cybermarket include offline and online payment accounts (such as PayPal, cash, Ukash and Pay-Safe-Cards etc.), datasets, credit card numbers, online currencies, compromised accounts, and drugs (Portnoff et al., 2017; Motoyama, McCoy, Levchenko, Savage & Voelker 2011).

Aneke et al. (2020) identify the major cyber-attack techniques and tools of cybercriminals as including botnets (use for spreading malwares automatically), fast flux (use for transferring information to computers sending malwares so as to make it hard to track the originating source), zombie computer (this is a computer system already hacked into that is being used to distribute malicious malwares), denial of service attack (this involves overfilling a computer network or server with lots of data or messages so as to hinder legitimate users from using it),

skimmers (this technique involves using a smart computer device to steal personal credit card information from unsuspecting owners), and social engineering (this is a manipulative way of playing tricks on the minds of potential targets in order to make them give out sensitive and personal information).

Gordon, Hosmer, Siedsma and Rebovich (2002) assert that cyber weapons and tools would continue to pose serious threat to the Internet and all users of network computers as they are mainly used to exploit the weaknesses inherent in the design of computer procedures and protocols. Cárdenas, Radosavac, Grossklags, Chuang and Hoofnagle (2009) observe that though some of the tools that are essential for the perpetration of cybercrime can be procured in the underground market; some tools can be specifically developed and used solely by members of closed criminal groups as a way of gaining competitive advantage over other criminals. Gordon et al. (2002) mention that authors of cyber weapons and tools generally do find it relatively easy to develop and release updated versions of their products because they usually collaborate with other deviant peers in the open-source project environments. Against this background, the central concern of this study was to investigate the tools, techniques and underground networks of Yahoo-boys in Ibadan city, Nigeria.

Theoretical Framework

The propositions of social learning theory as put forward by Ronald L. Akers provided the theoretical guide for this research. Social learning theory is essentially a combination of differential association and behavioral learning theories (Akers & Jennings, 2016). It posits that crime is a learned behavior that results from the interaction of four principal components which are differential association, definitions, differential reinforcement and imitation. Differential association constituent of the theory connotes that people's interaction with others vary in frequency, duration, priority and intensity with the most essential interactions being those involving intimate personal groups such as family and friends. Thus, associations that occur early in life (priority), last longer (duration), take place more often (frequency), and/or involve people with whom the individual is closely attached (intensity) will have a greater effect on an individual's definitions and subsequent behavior (Akers & Sellers, 2013). Definitions entail the meanings, attitudes, values and orientations which people

attach to crime and deviance as well as conforming behavior, while differential reinforcement centers on the balance of the perceived, experienced, or anticipated reward(s) and punishment(s) that would likely accompany or follow the exhibition of a particular kind of behaviour (Akers & Jennings, 2016). Therefore, behaviors that are frequently exhibited and frequently rewarded (and highly reinforced) are those behaviors that individuals are likely to continue to choose to perform (Akers & Jennings, 2016). Imitation involves engaging in a behavior after observing someone else committing a similar act (Holt, Burruss & Bossler, 2012). Thus, social learning theory submits that individuals are more likely to choose criminal behavior over conforming behavior when they differentially associate with those who expose them to deviant patterns, when the deviant behavior is differentially reinforced over conforming behavior, when they are more exposed to deviant compared to conforming models, and when their own definitions favorably dispose them towards committing deviant acts (Akers & Sellers, 2013). In essence, the theory assumes that a dual directional relationship exists between deviance and conformity, because they are both essentially influenced by the process of modelling and reinforcement. Yahoo-boys are not only relying on their offline and online contacts as their main sources of knowledge and information on the techniques for perpetrating cyber fraud, they are also banking on their social networks for the procurement of essential tools and resources used for facilitating their illegal acts on the cyberspace.

Study Area and Study Population

Ibadan city was the location selected for this research. It is a prominent city in Southwestern Nigeria. Ibadan is the capital of Oyo State and has a population size of about 3,565,108 people (World Population Review, 2020). The choice of Ibadan was predicated on the fact that it is among the cities with high record of cyber fraud in Nigeria (Akanle & Shadare, 2019; PM News, 2021). Equally, the officials of the Economic and Financial Crimes Commission (EFCC) which serves as the law enforcement agency saddled with the responsibility of monitoring and investigating financial crimes in Nigeria had arrested and prosecuted youths involved in cyber fraud within Ibadan city at different points in time (Oyewale 2020; The Guardian 2020). The study population was constituted by youths involved in the perpetration of cyber fraud.

METHODOLOGY

This study was exploratory and cross-sectional in design. Data collection lasted over a period of four months between September and December, 2020. Qualitative method was principally deployed for the elicitation of data. Specifically, in-depth interviews involving face-to-face informal chats were conducted with 11 youths involved in the perpetration of cyber fraud via the aid of a voice recorder. Snowball sampling technique was employed for the selection of the respondents. As regards the procedure for data collection, it is pertinent to point out that eliciting data from the Yahoo-boys was particularly challenging because many of them were skeptical about the intention of the researchers because of the increasing monitoring of their activities by EFCC officials. The researchers had to visit major bars widely reputed as relaxation spots of youths involved in cyber fraud perpetration in Ibadan city and contact was successfully established with one of the Yahoo-boys after about four weeks of frequent visits to those locations. After the initial interactions and confidence-building process, this particular contact agreed to be interviewed and also introduced the researchers to two of his associates. Linkage was subsequently established with other respondents through referral facilitated by these initial contacts.

Generally, interviews were conducted with the respondents at afternoon period (between 1:00pm and 4:00pm) in their chosen locations during weekdays and on weekends subject to their availability. The scheduling of the interviews for afternoon period was essentially necessitated by the fact that youths involved in cyber fraud are usually busy on the Internet at night hours so as to be able to connect and interact with some of their potential victims who are resident in countries with different time zones. Thus, they often need to sleep late into the afternoon. Moreover, it was difficult to interact with them in the evening because that was the period of the day they normally used to unwind. Typically, Yahoo-boys prefer not to be ‘disturbed’ while having fun.

As regards data analysis, the generated tape-recorded data were subjected to manual content analysis involving careful transcription, detailed description and interpretation. Specifically, data were thematically analyzed, explored and

interpreted in line with the research objectives. Also, the verbatim quotation of some of the important responses given by the respondents in the course of the interviews was done to further enhance the lucidity of discourse.

Ethical Consideration

The conduct of this research was strictly guided by the international ethical standard for the conduct of social research. The informed consents of the respondents were sought and obtained before their participation. Also, the objectives of the research were clearly and carefully explained to them. Equally, they were informed of their rights to withdraw from further participation in the interview whenever they deemed necessary. Furthermore, none of the respondents was subjected to any form of harm, coercion or intimidation before, during and after data elicitation. Generally, conscious efforts were made at every stage of the research to protect the identity, rights and integrity of the study participants.

RESULTS AND DISCUSSION

In this section, the major results that emanated from this research are thematically presented and discussed. The themes covered included the factors underlying Yahoo-boys' involvement in cyber fraud, their pathways to cyber fraud techniques and skills as well as the types, sources and costs of their operational tools.

Factors Underlying Yahoo-Boys' Involvement in Cyber Fraud

Information was sought from the Yahoo-boys on the reasons underlying their involvement in cyber fraud as a way of understanding the push and pull factors that attracted them to the crime. All of them attributed their involvement in cyber fraud to a similar reason. One of them remarked:

> My motivation mainly comes from some of my guys that are already balling hard (living ostentatious lifestyles) and driving big cars worth between $11795.54 and $13106.16 (N 4,500,000 and N5,000,000). Can you imagine a 19year-old-boy buying a car (Camry Muscle model) worth about $6,553.08 (N2,500,000) through proceeds gained from his hustle (cyber

> fraud)? The boy in question is my friend's younger brother. So, if one sees all the paparazzi and flexing (glamours and glitz) of guys who are into hustle in one's neighborhood every day, one will also want to try it (cyber fraud). That is what we call ginger (inspiration) (IDI/Yahoo-boy/Male/Yoruba/9years in practice/Aluminum Fabricator/Ibadan).

Another respondent said that:

> Every Yahoo-boy in this game is inspired whenever he sees his friend making a big hit from hustling (cyber fraud perpetration). I am usually motivated whenever any of my friends makes huge proceeds. If he makes it big this week, I can also cash-out from my own hustle next week. In essence, I get inspired by the exploits of my guys who are also in the game (cyber fraud). We are sources of inspiration to one another (IDI/Yahoo-boy/Male/Yoruba/6years in practice/Agriculturalist/Ibadan).

Below is another respondent's submission:

> When there is no financial assistance from one's family, one just needs to keep hustling with others to make it. Also, if one has many friends who are into it (cyber fraud) and one decides not to join them in hustling, they will be calling one all sorts of derogatory names. They would see one as being foolish (IDI/Yahoo-boy/Male/Yoruba/7years in practice /Accountant/Ibadan).

It can be established from the above submissions that Yahoo-boys were mainly motivated to engage in cyber fraud by the desire to get rich like their friends and peers who became wealthy through the perpetration of the crime. A few of the respondents also adduced their involvement in the illegal act to lack of financial support from their family members. The implication of this finding is that Yahoo-boys who became wealthy through cyber fraud were being imitated by

their peers who saw them as their role models. Ojedokun and Eraye's (2012) study established that Yahoo-boys are widely known as maintaining a distinctive socio-economic lifestyle which confers a unique identity on them in Nigerian society. Moreover, Ojedokun (2010) and Tade and Aliyu (2011) separately discovered that many youths in Nigeria were attracted to cyber fraud by the desire to get rich and peer pressure. Furthermore, this finding supports the propositions of the differential association, definitions and imitation constituents of social learning theory. Yahoo-boys were mainly motivated to engage in cyber fraud as a result of differentially associating with friends and peers who were also involved in the criminal act themselves and who also attached positive meanings, attitudes, values and orientations (definitions) to cyber fraud perpetration. Equally, they revered their friends and peers who became wealthy through cyber fraud (modelling) and were consequently inspired to imitate their criminal behavior. Skinner and Fream's (1997) study which analyzed computer crime among a sample of college students similarly revealed that associating with peers who indulge in cybercrime was the strongest predictor for perpetrating cybercrime, while definitions that are favorable to adhering to the law are negatively related to perpetrating cybercrime.

Cyber Fraud Techniques and Skills Acquisition Pathways of the Yahoo-Boys

To gain adequate insights into the underground networks of the Yahoo-boys, investigation was conducted into how they acquired the techniques and skills which they usually deploy for the perpetration of fraud on the cyberspace. All the respondents affirmed that they learnt cyber fraud techniques and skills from their friends and peers who were already established cyberfraudsters. In one of the interviews conducted, a Yahoo-boy stated:

> In this game (cyber fraud), you have to learn from someone. Everything about this hustle (cyber fraud) boils down to the connection one has and the area of the hustle which one wants to learn because Gee-boys know that Yahoo Yahoo (cyber fraud) goes beyond what is being done on Facebook, Instagram and so on. So, for a newcomer, the starting point is to learn from a person that would tell you

> what you really need to know because Yahoo Yahoo is not something that you will just decide to go into without being properly tutored. For my own training, I learnt a lot of things from my own boss who is like an area brother to me. I started with the creation and use of United States citizens' Facebook account profiles. There are so many processes to it (cyber fraud). So, one just has to seek information from those who truly know. It is not about what you just know on your own as an individual (IDI/Yah oo- boy/Male/Yoruba/10years in practice/Graduate/Ibadan).

In one of the interviews, a respondent declared:

> I feel the most important thing in this hustle (cyber fraud) is to have someone who is very knowledgeable about it and willing to show one the way. At the training stage, there are certain things one needs to have so as to facilitate a successful learning process. For instance, there are some logs or log-ins that one needs to buy because there are some access-restriction sites that someone residing in Nigeria will not be able to access. It is through these log-ins that one would be able to access such sites. All this process involves constant training and learning. I learnt from my friends (IDI/ Yahoo-boy /Male/Igbo/6years in practice/Undergraduate/Ibadan).

A respondent explained:

> I was introduced into the hustle (cyber fraud) by my childhood friend. He is someone that I look up to because he has made it big. He has always encouraged me to hammer (become rich) like him. However, my parents tried to separate us when they got to know that he is into Gee (cyber fraud) (IDI/Yahoo-boy/Male/Igbo/7years in practice/Un dergraduate/Ibadan).

It can be inferred from the above narratives that learning from social networks (friends and acquaintances) played important role in the respondents' acquisition of cyber fraud techniques and skills. Yahoo-boys attach serious importance to learning criminal techniques and skills from established cyberfraudsters because they recognized the fact that cyber fraud is a complex crime that cannot be successfully perpetrated by a novice who has not been strategically initiated and socialized into its intricacies. This result supports the submission of Leukfeldt (2014) that social relationships is very important for the recruitment and growth of cybercriminal networks. Also, Leukfeldt et al. (2017) have similarly stated that the role which social ties play in the origin and growth of cybercriminal networks cannot be overemphasized. This finding also validates the differential association and imitation aspects of social learning theory. Friends and acquaintances of Yahoo-boys' did not only play prominent roles in their initiation into cyber fraud, but equally constituted the most important nodes for the transmission of ideas, knowledge, skills and techniques associated with cyber fraud. Furthermore, this outcome corresponds with the research of Lee, Hong, Yoon, Peguero and Seok (2018) on correlates of adolescent cyberbullying in South Korea which found that delinquent peer association was positively associated with both cyberbullying perpetration and victimization.

Tools Commonly Used by the Yahoo-Boys for Cyber Fraud Perpetration

Criminals frequently rely on the deployment of certain tools for crime perpetration (Chiu & Leclerc, 2017; Wells & Horney, 2002). Therefore, it was deemed necessary to seek information on the essential tools commonly utilized by the Yahoo-boys. Findings indicated that Yahoo-boys were making use of both hardware and software tools for different purposes. Below is a revelation that was given by one of the respondents:

> For me, the most important tools in this business are one's phone, laptop and the Internet. Also, one needs a very strong VPN (virtual private network). If one needs to interact with people in Europe or South America, one would have to use a VPN to indicate that one is also a resident in such a country. The benefit is that it makes one real and

> legitimizes one's online profile. Also, there are many other types of tools; and their usage depends on the type of hustle (cyber fraud) one is into. For example, people involved in money transfer or account loading need to buy cheque samples and IP (Internet protocol) log-in because it is very important for them to always change their IP codes (IDI/Yahoo-boy/Male/Yoruba/11 years in practice /Self -employed/Ibadan).

Another respondent reasoned in a similar manner:

> When we are talking about tools that we normally use for this hustle, we are talking about VPN. For example, VPN basically is used to change one's location. You know many clients (potential victims) have trust issue. When they discovered that one is a Nigerian, they basically stop interacting with one. So, using a VPN would indicate that one is based in the United States of America; and clients (potential victims) would automatically believe and fall for it. They will basically believe that one is also one of them. In fact, there are some dating sites with very strict access-restriction policy for certain countries. One cannot access them without using a VPN. Sites such as Plenty of Fish (POF), Emily Dates, Match.com. amongst others. Also, there are some dating sites for which one needs to have international telephone numbers to access because they have to send one certain code to enable one to be able to successfully register. Also, we normally buy foreign SIM (subscriber identification module) cards from people willing to sell them (IDI/Yahoo-boy/Igbo/Male/7years in practice/Und ergraduate/Ibadan).

Furthermore, in terms of their illicit financial transactions, one of the interviewees explained the tools they normally use thus:

> Cash App, PayPal, and Zelle are my main tools for cash transfer. Now the ones that is becoming rampant these days among hustlers (Yahoo-boys) is bitcoin and blockchain. The app on which you save your Bitcoin is Paxful. Ethereum is another form of digital currency which one can convert to cash. There are different cryptocurrencies but the one that is high in value compared to the dollar is bitcoin. Some digital currencies are even better than bitcoin but we do not trade in them because few people own them in Nigeria (IDI/Yahoo-boy/Male/Yoruba/11 years in practice/Self-employed/Ibadan).

Also, another respondent emphasized that:

> I cannot use my normal bank account details to receive money from my clients (victims). So, I basically make use of online mobile payment apps that are not traceable like the Cash APP. It is not wise to receive money using my details or passport from the Western Union. Although this is possible, but it is not advisable because one can be easily traced (IDI/Yahoo-boy/Male/Yoruba/9years in practice /Alumi num Fabricator/Ibadan).

The above submissions of the respondents clearly demonstrate that the operational tools of the Yahoo-boys are broadly in two categories which are: (a) tools for facilitating crime commission on the cyberspace (such as laptop, mobile phone, printer, Internet, virtual private network (VPN), Internet protocol (IP) log-ins, and cheque samples) and (b) tools for driving illicit cash flows (such as Bitcoin, Blockchain, Cash App, Ethereum, Paypal, and Zelle). A major deduction that can be made from this finding is that both hardware and software tools being utilized by the Yahoo-boys for cyber fraud perpetration were not originally created and/or designed for illegitimate purposes. Rather, Yahoo-boys are converting them from their primary status as legitimate resources to criminal tools. In February 2021, the Central Bank of Nigeria, the apex monetary authority in Nigeria, banned the use of cryptocurrencies claiming that they are increasingly being employed for money laundering, financial terrorism and other criminal

activities (Komolafe, 2021). The implication of finding this is that criminals would always find a way of exploring the downside of any technological breakthrough to facilitate crime perpetration. This outcome is in line with the observation of Gordon et al. (2002) that cybercriminals are increasingly utilizing tools primarily designed for legitimate usage for the commission of cybercrime. Also, this finding brings to bear the relevance of the concepts of definitions and differential reinforcement aspects of social learning theory. Yahoo-boys were positively oriented towards cyber fraud because they recognized the usefulness and values embedded in the adoption of diverse operational tools. More so, their access to some operational tools which can be employed to deflect the risk of being detected and/or apprehended provided them with negative reinforcement as they aided them to avoid potential punishments that their online criminality attracts. Furthermore, this result is similar to the outcome of Ogunleye, Ojedokun and Aderinto's (2019) study which revealed that female undergraduate cyber fraudsters operating in south-west Nigeria capitalized on the wider interconnectivity and interactive advantages presented by the ubiquity of social media platforms after learning and acquiring essential knowledge and skills on ways to clandestinely deploy information and communication technology (ICT) resources for fraudulent activities from their brothers and boyfriends.

Means Through Which Yahoo-Boys Sourced for their Operational Tools

Studies conducted elsewhere have established that cybercriminals usually procure their attack-tools and other illicit criminal commodities in the underground cyber market (Leukfeldt et al., 2017; Pastrana et al., 2018). Thus, it was considered important to investigate how Yahoo-boys operating in Ibadan city usually source for their operational tools. Nearly all the respondents submitted that they normally procure cyber fraud tools from their international contacts and through underground online forums. One of the interviewees expressed that:

> To get some of these operational tools, one just need to search anonymous (unicc.ru). When one searches for anonymous on Google, one would be able to make right contact with hackers. For example, if one wants to buy a credit card now, one just need to search anonymous. One

> can get these tools at cheap prices all over the world. For example, just type I need so and so in Mexico, then google the anonymous in Mexico. It is a done deal (IDI/Yahoo-boy/ Male/Yoruba/11 years in practice/Self-employed/Ibadan).

A respondent also commented:

> There are some contacts who have turned legit (criminal accomplice) over time. These people normally helped us to get whatever tool and information we need over there in the U.S. There are some clients who have turned legit to the extent that they know the kind of person they are interacting with in terms of nationality and country of residence. If there is a strong connection between one and the person (contact), one can start colluding with him/her to get any vital tools that one needs. For instance, such contact(s) can help one get an American SIM card. He or she would then courier same through the DHL or any other means of delivery to Nigeria. U.S. SIM is very useful, and that is why most Yahoo-boys prefer to use iPhone. iPhone will support such a SIM card in Nigeria (IDI/Yahoo-boy /Male/Yoruba/Agriculturalist/6years in practice/Ibadan).

Another interviewee stated that:

> We do get our vital tools and information from people like us. That is their own area of hustle (cyber fraud). They are hackers - they hack into so many things. For example, they hack to get clients' credit card information. They will then give us the 14 digits at the front side of the card and the CVV (card verification value) number. There are some hackers that normally assist us when we need SSN (social security number) and residents' dates of birth. We do get these tools through online buying and selling. In fact, there are some hackers that can conveniently sell companies'

> accounts information to us. They usually give us details of such accounts, and we will pay them in return. One will then make use of such sensitive information to transfer money from the company whose account had been so compromised to one's client (potential victim) account. It could take up to one week before the affected company detects such a move. By that time, one would have received such a cash from one's client. Of course, he or she (client) would be subsequently arrested (IDI/Yahoo-boy/Male/Yoruba/ 8years in practice/Accountant/Ibadan).

It can be deduced from the above submissions that Yahoo-boys mainly sourced and procured their operational tools from underground online forums, foreign criminal contacts and abroad-based criminal associates. This result does not only demonstrate the increasing organized transnational dimension of cyber fraud, but it equally showcases the way through which cyberfraudsters are exploiting the power of both virtual and social networks to gain access to illicit resources. This outcome is in tandem with Portnoff et al.'s (2017) study which found that cybercriminals were relying on forums not only for the initiation of trade relationships, but also for facilitating the exchange of illicit goods and services. Another major implication of this finding is that the relatively easy means through which tools and resources essential for the perpetration of cyber fraud can be procured from underground online forums and other criminal networks will continue to negatively impact the Nigerian government's efforts at controlling the illegal online activities of the Yahoo-boys. Gordon et al. (2002) have equally asserted that cyber tools and weapons will continue to pose serious threat to the Internet and all users of networked computers. This result also demonstrates the efficacy of social learning theory. Yahoo-boys mainly gained access to their illicit resources from delinquent peers with whom they associated. However, despite the fact that Yahoo-boys' duration and intensity of interactions with their foreign criminal contacts and abroad-based criminal associates played important role in their bonding, they were less significant in their sourcing for operational tools in underground online forums where relationships are mainly transactional and transient. Hollinger's (1993) research on correlates of software piracy and unauthorized account access similarly established that individuals are more likely

to engage in computer crimes as the number of friends they have who also engage in such illegal activities increases.

Cost of Cyber Fraud Operational Tools of the Yahoo-Boys

Respondents were also probed on the cost associated with the procurement of their operational tools as a way of gaining insights into the extent of their financial investment in the illegal act. Generally, all of them submitted that the cost of their operational tools is largely dependent on the type of cyber fraud they intend to perpetrate. One of the Yahoo-boys explained that:

> It (cost of procurement) is dependent on the way you interact with people that have such tools. There are Some tools one does not need to pay for. They will just give one for free. And even if one needs to buy, most tools are not too costly to get. You could purchase a tool of $5 (N2,000.00) or $7 (N3,000.00) to facilitate a hustle that could yield like $100 (N40,000.00) (IDI/Yahoo-boy/Male/Yoruba/11 years in practice/Self-employed/Ibadan).

Also, a respondent mentioned:

> The cost of procurement of tools depends on the area of hustle you are engaging-in. For instance, if one wants to load an account, there are some tools that one can purchase for about $786.36 (N300, 000) or more. If one wants to buy a log-in or a spam, one can purchase either of them for about $786.36 (N300,000). They are costly because they contain all the details that one needs. The only thing that one needs to do is just to shoot the target account. For example, one can only purchase a Wells Fargo account from hackers in the dark web. Although I can buy it for about $786.36 (N300,000), but I can make up to $2621.23 (N1,000, 000) using it (IDI/Yahoo-boy/Male/Yoruba/7 years in practice /Undergraduate/Ibadan).

An interviewee equally said:

> One can get a VPN for $4 (N1,500.00) or $10 (N4,000.00). If one wants to buy a cheque, it is dependent on how genuine it is. A cheque of $20 (N8,000.00) will be more genuine than a cheque of $10 (N4,000.00), a company's account of $100 (N40,000.00) will be more genuine than that of $50 (N20,000.00). At times, one can buy some that are expensive and get scammed. Sellers can still scam one. There are also some Yankee citizens' hacked Facebook accounts that are sold with malwares as operational tools (IDI/Gee boy/Male/Yoruba/Over 7years in practice /Accounta nt /Yoruba/ Ibadan).

It can be established from this result that though the cost of operational tools is largely dependent on the type of cyber fraud to be perpetrated. Yahoo-boys are investing capital in their procurement because they have seen cyber fraud as a profitable business that has the potentials for yielding huge financial gains. Thus, the potential reward is seen as higher than the cost of investment. A major implication of this finding is that Yahoo-boys may not be easily discouraged from perpetrating cyber fraud by the prescribed negative sanctions it attracts because they see the cost of investing in the crime as very cheap when compared with the potential rewards derivable from it. This result affirms the position of Allodi (2017) that the rise of cybersecurity incidents coincides with the development of the underground economy where attack tools and services are easily accessible at low cost or even for free. It equally demonstrates the validity of social learning theory. Yahoo-boys were positively reinforced towards perpetrating cyber fraud because the anticipated rewards which they associated with the deployment of certain operational tools for cyber fraud far outweighs their cost of procurement. Furthermore, this output is in tandem with Shadmanfaat et al.'s (2019) study among University of Guilan undergraduates which found that an individual's sense of personal and social gain from engaging in cyberbullying is directly related to engaging in cyberbullying perpetration.

Limitations of the Study and Suggestions for Future Research

A major limitation of this study lies in the small population size of the Yahoo-boys that were interviewed. Thus, the small size of the study population may negatively impact the overall generalizability of the major findings. Equally, it exclusively focused on male youths involved in the perpetration of cyber fraud. Consequently, the perspectives of their female counterparts on the subject matter were not taken into account. Therefore, future studies focusing on this aspect of cyber-criminality should expand their scope in terms of size of sample and the gender composition of respondents as a way of further enriching the diversity of respondents' submissions. However, in-spite of these identified limitations, this study expands the frontiers of knowledge by providing significant insights into an important aspect of cyber-criminality that had hitherto been a neglected area of research. Equally, it provides an important comparative benchmark that will be beneficial to future studies focusing on the tools, techniques and underground networks of cybercriminals particularly from the viewpoint of social learning theory.

CONCLUSION

The online criminal activities of Yahoo-boys are not only negatively impacting Nigeria in multiples ways, they also constitute serious socio-economic threats to other Internet users worldwide. For this reason, it is expedient to suggest some useful strategies that can be adopted to combat their illegal acts. At the global level, it is important for national governments to design durable and effective strategies through which the use of international online payment systems and digital currencies primarily designed for legitimate financial transactions and monetary exchange purposes can be properly monitored, regulated and secured. This step becomes imperative as a practical means of combatting the criminal activities of cyber-fraudsters that are utilizing these international monetary transactions platforms to perpetrate money laundering and drive illicit cash flows. Also, the dominant role which underground online forums and international criminal networks played on the availability of some operational tools and illicit resources aiding the perpetration of cyber fraud underscores how transnational criminal networks are promoting the occurrence of cybercrime and threatening the online activities of other Internet users. Therefore, it is important for global law enforcement agencies and relevant international cybercrime-fighting institutions to forge strategic alliance and collaboration for the purpose of constantly reviewing and analyzing the latest operational tools and techniques being employed by cyberfraudsters as a way of combatting their criminal activities and the threats posed by the underground cyber economy.

At the national level, it is germane for the National Orientation Agency of Nigeria, the government agency charged with the promotion of values, morals and patriotism among Nigerians to champion the cause for values reorientation among Nigerians by consistently launching massive public campaigns against youth involvement in cyber fraud perpetration while simultaneously promoting the value of hard work. This can be achieved through strategic collaboration and partnership with the mass media and other agents of socialization, particularly family and school as well as religious bodies. Finally, apprehended cyberfraudsters should be promptly prosecuted by law enforcement agents, and the punishments meted out to them in the court of law should be giving as much publicity as possible so as to discourage other youths from engaging in cyber fraud perpetration.

References

Adeniran, A. I. (2008). The Internet and emergence of Yahooboys sub-culture in Nigeria. *International Journal of Cyber Criminology, 12*(2), 368–381.

Aderinto, A. A., & Ojedokun, U. A. (2017). Cyber underground economy in Nigeria. In P. Ndubueze (Ed.), *Cyber criminology and technology-assisted crime control: A reader* (pp. 219-228). Ahmadu Bello University Press, Limited, Zaria.

Ajayi, T. M. (2019). Anti-language, slang and cyber scam subculture among urban youth in southwestern Nigeria. *International Journal of Cyber Criminology, 13*(2), 511-533.

Akanle, O., & Shadare, B. R. (2019). Yahoo-plus in Ibadan: Meaning, characterization and strategies. *International Journal of Cyber Criminology*, *13*(2), 343-357.

Akers, R. L., & Jennings, W. G. (2016). Social learning theory. *The handbook of criminological theory*, 230-240.

Akers, R. L., & Sellers, C. S. (2013). *Criminological theories: Introduction, evaluation, and application* (6th edition). New York: Oxford University Press.

Allodi, L. (2017, October). Economic factors of vulnerability trade and exploitation. *Proceedings of the 2017 ACM SIGSAC conference on computer and communications security* (pp. 1483-1499).

Andress, J., & Winterfeld, S. (2014). *Cyber warfare: techniques, tactics and tools for security practitioners*. Elsevier Inc.

Aneke, S. O., Nweke, C. N., Udanor, I. A…Ezema, M. E. (2020). Towards determining cybercrime technology evolution in Nigeria. *International Journal of Lates Technology in Engineering, Management and Applied Science*, *ix*(iv), 37-43.

Cárdenas, A., Radosavac, S., Grossklags, J., Chuang, J., & Hoofnagle, C. J. (2009). An economic map of cybercrime. Retrieved from https://papers.ssrn.com/soI3/papers.cfm?abstract_id=1997795.

Chiu, Y. N., & Leclerc, B. (2017). An examination of sexual offenses against women by acquaintances: The utility of a script framework for prevention purposes. In: Crime prevention in the 21st century (pp. 59-76). Springer, Cham.

Gordon, G. R., Hosmer, C. D., Siedsma, C., & Rebovich, D. (2002). Assessing technology, methods, and information for committing and combating cybercrime. Retrieved from https://www.ojp.gov/pdffiles1/nij/grants/198421.pdf.

Hollinger, R. C. (1993). Crime by computer: Correlates of software piracy and

unauthorized account access. *Security Journal, 4*, 2-12.

Holt, T. J., Burruss, G. W., & Bossler, A. M. (2012). Social learning and cyber deviance: Examining the importance of a full social learning model in the virtual world. *Journal of Crime and Justice*, *33*(2), 31-61.

Hutchins, C. E., & Benham-Hutchins, M. (2010). Hiding in plain sight: Criminal network analysis. *Computational and Mathematical Organization Theory*, *16*(1), 89-111.

Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, *47*, 44-57.

Internet Crime Complaint Centre. (2014). The internet crime complaint report - 2014. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2014_ IC3 Report.pdf

Jegede, A. E., Elegbeleye, A. O., Olowookere, E. I., & Olorunyomi, B. R. (2016). Gendered alternative to cyber fraud participation: An assessment of technological driven crime in Lagos State, Nigeria. *Gender & Behavior, 14*(3), 7672-7692.

Kayode-Adedeji, D. (2019, August 29). Nigeria: EFCC arrests suspect who 'assisted' Nigerian cyber-crime syndicate in U. S. *Premium Times*. Retrieved from https://www.premiumtimesng.com/news/more-news/349261 -efcc-arrests-sus pect-who-assisted-nigerian-cyber-crime-syndicate-in-u-s.html

Komolafe, B. (2021, February 8). Cryptocurrency ban is to protect Nigerians, financial system– CBN. *Vanguard*, February 8. Retrieved from https://www.vanguardngr.com/2021/02/cryptocurrency-bans-to-protect-nigeria ns-financial-system-cbn/

Lee, J. M., Hong, J. S., Yoon, J., Peguero, A. A., & Seok, H. J. (2018). Correlates of adolescent cyberbullying in South Korea in multiple contexts: A review of the literature and implications for research and school practice. *Deviant Behavior, 39*(3), 293-308.

Leukfeldt, E. R. (2014). Cybercrime and social ties: Phishing in Amsterdam. *Trends in Organized Crime*, *17*, 231–49

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). Origin, growth and criminal capabilities of cybercriminal networks: An international empirical analysis. *Crime, Law and Social Change*, *67*(1), 39-53.

Motoyama, M., McCoy, D., Levchenko, K., Savage, S., & Voelker, G. M. (2011, November). An analysis of underground forums. *Proceedings of the 2011 ACM SIGCOMM conference on Internet measurement conference* (pp. 71-80).

Ojedokun, U. A. (2010). *Cybercrime and changing lifestyle among students of*

some selected universities in south western Nigeria (Unpublished master's thesis). University of Ibadan, Ibadan, Nigeria.

Ojedokun, U. A., & Eraye, M. C. (2012). Socioeconomic lifestyles of the yahoo-boys: A study of perceptions of university students in Nigeria. *International Journal of Cyber Criminology 6*(2), 1001-1013.

Ogunleye, Y. O., Ojedokun, U. A., & Aderinto, A. A. (2019). Pathways and motivations for cyber fraud involvement among female undergraduates of selected universities in south-west Nigeria. *International Journal of Cyber Criminology*, *13*(2), 309-325.

Oladimeji, R. (2019, October 8). Cyber fraud: Court orders Invictus Obi's 280m forfeited. *The Punch*. Retrieved from https://www.punchng.com/cyber-fraud-court-orders-invictus-obis-n280m-forfeited/

Oyewale, W. (2020, October 3). EFCC arrests 10 suspected yahoo boys in Oyo. *The Punch*. Retrieved from https://www.punchng.com/efcc-arrests-10-suspected-yahoo-boys-in-oyo/

Pastrana, S., Hutchings, A., Caines, A., & Buttery, P. (2018, September). Characterizing Eve: Analyzing cybercrime actors in a large underground forum. Proceedings of *international symposium on research in attacks, intrusions, and defenses* (pp. 207-227). Springer, Cham. Retrieved from https://doi.org/10.1007/978-3-030-00470-5_10.

PM News. (2021, January, 20). EFCC arrests seven "Yahoo Yahoo boys" in Ibadan. *PM NEWS*. Retrieved from http://pmnewsnigeria.com/2021/01/20/effc-arrests-seven-yahoo-yahoo-boys-in-ibadan/

Portnoff, R. S., Afroz, S., Durrett, G., Kummerfeld, J. K., Berg-Kirkpatrick, T., McCoy, D., ...& Paxson, V. (2017, April). Tools for automated analysis of cybercriminal markets. *Proceedings of the 26th international conference on world wide web* (pp. 657-666). Retrieved from https://dl.acm.org/doi/abs/10.1145/3038912.3052600.

Shadmanfaat, S., Howell, C. J., Muniz, C. N., Cochran, J. K., & Kabiri, S. (2019).Cyberbullying perpetration: An empirical test of social learning theory in Iran. Deviant Behavior. doi: 10.1080/01639625.2019.1565513.

Skinner, W. F., & Fream, A. M. (1997). A social learning theory analysis of computer crime among college student. *Journal of Research in Crime & Delinquency, 34*, 495-518.

Sood, A. K., & Enbody, R. J. (2013). Crimeware-as-a-service—a survey of commoditized crimeware in the underground market. *International Journal of Critical Infrastructure Protection*, *6*(1), 28-38.

Tade, O., & Aliyu, A. (2011). Social organization of internet fraud among university undergraduates in Nigeria. *International Journal of Cyber Criminology, 5*(2), 860-875.

The Guardian. (2020, March 4). EFCC arrests 'Yahoo' boy with coffin, five others arrested in Ibadan. *The Guardian*. Retrieved from https://guardian.ng/news/efcc-arrests-yahoo-boy-with-coffin-five-others-in-ibadan/

This Day. (2016, April 16). Nigeria loses over N127bn annually through cybercrime. Retrieved from www.thisdaylive.com/index.php/2016/04/18/cyber-security-nigeria-loses-over-n127bn-annually-through-cybercrime/

Wells, W., & Horney, J. (2002). Weapon effects and individual intent to do harm: Influences on the escalation of violence. *Criminology*, *40*(2), 265-296.

World Population Review. (2020). Nigeria population 2020. Retrieved from https://worldpopulationreview.com/countries/nigeria-population

What is Justice Reinvestment? A Review of Policies and Practices

*Richard L. Wentling, Ph.D.**
Assistant Professor
Administration of Justice Department
Pennsylvania State University- New Kensington

Jaeyong Choi, Ph.D.
Assistant Professor
Criminal Justice
West Chester University (PA)

Abstract

Justice reinvestment is a correctional approach to criminal justice, hinging on reducing prison populations while diverting prison-based funding into community programs (Tucker & Cadora, 2003). Justice reinvestment policies were first piloted in 2006 and have since led to federal legislation in the United States (Criminal Justice Reinvestment Act, 2010) and subsequent reauthorizations in 2015 and 2019. Since the passing of the initial legislation, Justice Reinvestment Initiative (JRI) programs have risen to nationwide popularity in the United States, with more than 30 states pursuing reinvestment-related policies. The following paper offers a critical review of the growing popularity of justice reinvestment in the United States to include the most common policies associated with the Justice Reinvestment Initiative and barriers to implementing the JRI approach. State policies and associated grant-based funding strategies are discussed, with recommendations offered for sustaining JRI policies. The current study also reviews other international approaches to justice reinvestment to highlight the widespread use of justice reinvestment.

Keywords

Justice Reinvestment, Community Corrections, Intermediate Sanctions, Prisons

* Direct correspondence to Richard L. Wentling, Ph.D., Assistant Professor, Administration of Justice Department, Pennsylvania State University- New Kensington; e-mail: rwentling@psu.edu.
* http://dx.doi.org/10.36889/IJCJ.2021.004.
* Received 19 March 2021; Revised 2 June 2021; Accepted 3 June 2021; Available online 18 June 2021.
INTERNATIONAL JOURNAL OF CRIMINAL JUSTICE, Vol. 3 Issue 1, June 2021, 123-150

INTRODUCTION

Justice reinvestment began as a criminal justice reform effort to address growing prison populations throughout the United States. Because of the increased use of prisons or jails and corresponding budget increases, calls for change garnered more attention (Austin & Coventry, 2001; Carroll, 2004; Malcolm, 2014; Tucker & Cadora, 2003), shifting the focus of criminal justice towards rehabilitation. With the passing of federal legislation and the corresponding grant funding, a standard definition has risen: a data-driven approach to improve public safety, examine corrections and related criminal justice spending, manage and allocate criminal justice populations more cost-effectively, reinvest savings in strategies that can hold offenders accountable, decrease crime, and strengthen neighborhoods (BJS, 2019a; Clements et al., 2011; Monteiro & Frost, 2015; Wong, 2016). Justice reinvestment was argued to be a solution to these problems (Tucker & Cadora, 2003). The premise of justice reinvestment stems from the investment in the community and community-oriented programs rather than investing in jails or prisons. Using this ideology, justice reinvestment was believed to improve criminal justice practices and programs to reduce overall prison populations and the associated excessive spending. Specifically, high-risk neighborhoods and areas with a greater concentration of crime became the focus of the initial concept to focus more efforts on diversionary programs and reduce formal adjudication.

Tucker & Cadora (2003) introduced justice reinvestment when the criminal justice system was feeling the effects of the previous decade's mass incarceration policies. Justice reinvestment was met with speculation but gained mainstream notoriety piquing both practitioners' and stakeholders' interests within the criminal justice system. The primary objective of the concept was to redirect funding allocated for general criminal justice uses, i.e., prison reconstruction and repairs, and use the budget to increase resources within communities. The original concept was intended to shift funds from traditional spending in the criminal justice system to high-risk or high-crime areas. Placing the focus on localized investments in the community and infrastructure was

believed to reduce the prison populations and corrections-based spending by providing community members more resources.

The justice reinvestment approach came at a pivotal time as both prison populations and criminal justice spending experienced significant increases throughout the country. The total prison population rose from 750,000 in 1985 to 1.7 million in 1997 (Austin & Coventry, 2001). The reliance on prisons continued into the 21st century, with an increase to 2.2 million individuals falling into the category of correctional control, with similar numbers for community supervision growing to a total of 4.5 million (BJS, 2019a). The growing use of corrections was also detailed through federal justice reinvestment legislation presented in 2009 and subsequently passed the following year (*Criminal Justice Reinvestment Act,* 2009). Among the growing concerns for the growth of the carceral state throughout the country were not only the population sizes but also the expenditures associated with the increased use of jails and prisons. The federal legislation argues that corrections-based spending rose from $12.6 million in 1988 to over $52 million in 2008, while incarceration rates also rose to a rate of 1 out of 100 Americans serving time in jails and prisons. Further illustrating the power of the carceral state, the legislation further defines the growing number of individuals experiencing some form of community-based supervision at approximately five million, equating to a rate of 1 out of 45 Americans. These numbers were used as a pivot point to thrust the need for justice reinvestment into the political arena and garner more calls for action.

Since the introduction of justice reinvestment in 2003, justice reinvestment became a leading approach to reducing prison populations and further incentivized legislatures through a federal initiative granting funding outlined by the federal legislation. The following paper offers a critical insight into the policies associated with justice reinvestment funding and the varying methods that states use to meet the JRI grant-based guidelines. There is a limited but growing base of literature related to justice reinvestment and the associated use of JRI funding. This paper furthers the discussion around JRI by presenting the origination and growth in popularity of justice reinvestment with a review of policies associated with justice reinvestment funding.

LITERATURE REVIEW

Development of Justice Reinvestment

Justice reinvestment is often described as using evidence-based practices to serve the public interest. When first introduced, Tucker & Cadora (2003) placed emphasis on reducing prison populations while maintaining aspects of public safety. The concept has since become a malleable policy that can be suited for the needs of the county, state, or jurisdiction that is seeking the use of justice reinvestment funding. Some scholars have argued that the current approach has missed the intended mark of the original intent (Austin et al., 2014). However, with the passing of federal legislation and the corresponding grant funding, a common definition has risen: a data-driven approach to improve public safety, examine corrections and related criminal justice spending, manage and allocate criminal justice populations in a more cost-effective manner, reinvest savings in strategies that can hold offenders accountable, decrease crime, and strengthen neighborhoods (BJS, 2019a; Clements et al., 2011; Monteiro & Frost, 2015; Wong, 2016).

Focusing on the criminogenic effects of specific communities, the reinvestment concept would take the stance of other place-based theories in arguing that certain neighborhoods were producing higher levels of criminal activity. Following the Broken Windows (Wilson & Kelling, 1982) and hot-spots policing (Sherman & Weisburd, 1995) models, justice reinvestment was situated at the crossroads of political discourse by offering the possibility of reduced correctional spending while also decreasing the overall number of those incarcerated throughout the country. Seemingly a tall task but greeted with zest and vigor by many stakeholders in both the criminal justice and public sectors. These “million-dollar blocks” (Story, 2016: Tucker & Cadora, 2003) served as the catalyst for a new way of approaching the carceral state and carving a path forward that could meet the goals of the reinvestment concept. With external support from non-profits, agencies, and various departments, the current justice reinvestment model shows continued promise as both correctional populations and spending decrease across the nation (Doob & Webster, 2014; Petersilia & Cullen, 2015). What is often overlooked, though,

are the consequences of shifting the focus from the prisons and jails meant to house offenders to the communities and neighborhoods where these offenders reside. The use of diversionary approaches for offenders is well-documented and has been used in varying capacities for decades (Wodahl & Garland, 2009). The justice reinvestment model takes a slightly different approach by focusing on diverting funds into community-based, diversionary programs by promoting more informal mechanisms of supervision. Specifically, justice reinvestment seeks to incentivize the reduction in harsh sentencing practices and streamlined parole hearings (LaVigne et al., 2013; Murdock, 2016). By reducing mandatory sentencing strategies (e.g., technical parole violations) offenders are granted subsequent opportunities and not immediately returned to prison after minor violations. One example of the complex relationship between justice reinvestment and diversionary approaches is examined by Latessa and colleagues (2009). As documented by Latessa et al. (2009), community corrections facilities in Pennsylvania had minimal impact on recidivism rates. Specifically, the availability of services and interactions with treatment staff were found to be a contributing factor to the diminished return of rehabilitation in the community setting. The JRI program is designed to increase the effectiveness of community-based programs, and in some cases, revise the more restrictive sentencing practices, which have been noted to increase rates of recidivism which can be exacerbated by ineffective community supervision (see Cullen, Jonson, & Mears, 2016). By using both front and back-end approaches to reforming the administration of justice, JRI shifts the emphasis from more punitive sentencing strategies to shorter, rehabilitative-focused punishments.

During the 2000s, the criminal justice system began seeing profound changes in legislation that would later spur expansive laws such as the Obama administration's Fair Sentencing Act (2010), reducing the disparity in sentencing between crack and powder cocaine and the Sentencing Reform and Corrections Act (2019) which focused on reducing mandatory minimum sentences while expanding treatment in federal prisons. More recently, the Trump Administration signed the First Step Act (2018) expanding the previous reforms of the Sentencing Reform and Corrections Act (2017) to include compassionate release and restricts the use of restraints for pregnant inmates while in labor. There has been no shortage of reform efforts presented as criminal justice policy

(Tonry, 2019). From a broad perspective, these examples of legislation place the impetus of reform on the over-reliance of jails and prisons. States have followed suit with various forms of legislation specific to their needs and jurisdictions, but all with the bi-partisan mantra of reform, echoing that of the federal legislation that often informs state policy.

Difficulties in Implementing Justice Reinvestment Policy

Before states embark upon implementing justice reinvestment, a baseline for both spending and correctional populations needs to be identified. During the original pursuit of justice reinvestment, the Council of State Governments (CSG) and Pew Foundation provided technical assistance for states seeking to implement reinvestment policies. Since the passing of the federal legislation, the Bureau of Justice Assistance (BJA), in partnership with the VERA Institute, have taken on collecting and reporting on the effectiveness of justice reinvestment across the country. At the time of this research, 36 states are pursuing the use of justice reinvestment and JRI funding. Taking a closer look at the requirements set forth by the Bureau of Justice Assistance in conjunction with the CSG, there is a great amount of flexibility for states and jurisdictions to pursue their own individually tailored approach to realizing savings under justice reinvestment practices. However, states must garner commitment from legislative leaders and other authorities within the criminal justice system. This level of participation indicates the importance of stakeholders and how much of an influence they have on the effectiveness and implementation of justice reinvestment.

Although justice reinvestment has garnered much attention, particularly as more states implement programs and policies meeting federal funding criteria, states are incentivized to pursue the justice reinvestment grants afforded through the BJS reinvestment program (BJS, 2019a). With the growing popularity of both politicians and varying stakeholders, it is no surprise that justice reinvestment continues to flourish as a sustainable and meaningful approach to prison-based reform (Brown, Schwartz, & Boseley, 2012; Taxman et al., 2014). There are many informational dashboards,[1] all offering promising results

[1] For examples of the functional dashboards see the Vera Institute of Justice, National Council of State Governments, or the Urban Institute webpages under the justice reinvestment projects.

regarding justice reinvestment and the continued use of the JRI funding. Many examples depict the positive outcomes associated with justice reinvestment. Still, even as one of the original authors states, the purpose of diverting funding into the high-risk communities has been lost to political banter and the push for renewed grant funding (Austin et al., 2014). These critiques and criticisms should be more widely discussed to inform the JRI approach better.

A CLOSER LOOK AT THE ROLE OF JRI

Clear (2011) offered one of the first critiques of justice reinvestment as he noted that an incentive-based initiative may produce more lasting outcomes. Specifically, Clear (2011) shifted the focus from state initiatives to a hot-spots ideology. High-risk communities would be offered incentives for participating at local levels and not state-wide initiatives. Using this ideological basis for criminal justice, individually tailored working groups would need to be further refined to incorporate city-level stakeholders representing the specific community and not just the state-level stakeholders. As Story (2016) argues, the mapping of these hot spots becomes a critical component of realizing justice reinvestment but a facet that has focused solely on racialized areas. Perhaps one of the most challenging aspects of achieving the intended goals and savings of justice reinvestment has been the influence of stakeholder groups and the working groups charged with planning and coordinating the policies. Because of the varying stakeholders and the different possibilities of representation for each state, the justice reinvestment model is treated almost as a one size fits all policy yet is given the flexibility to meet each working group's identified needs.

The use of stakeholders ensures representation when convening for policy implementation or large-scale changes. Still, it may serve to further the divide between the communities in need of reinvestment and the stakeholders who are appropriating the funding. The criminal justice system often relies on politicians and elected officials to act in the best interest of the constituents they represent. Yet, the JRI presents a unique opportunity to meet the data-driven expectation of JRI and use the funding in broad, sweeping policies. Many of

these policies tend to appropriate funding for innovative law enforcement and revised sentencing assessments used in conjunction with sentencing guidelines. In keeping with Clear's (2011) suggestion that stakeholders should be at the local level where the actual programs are designed to make a difference, practitioners and front-line providers should be provided more of a voice when determining the actual needs of the community.

Sabol & Baumann (2020) argue that justice reinvestment and the justice reinvestment initiative created an incentive-heavy push for states to meet the BJS guidelines for eligibility in receiving grant money for corresponding programs. Once the concept became associated with funding through technical assistance provided by external agencies (i.e., BJS, CSG, Urban institute), the general approach then shifted from what was originally intended to reduce prison spending and populations. Instead, it became a means to receive funding to pursue the policies and programs associated with justice reinvestment. The pursuit of the policies through partial implementation and a lack of support from every stakeholder-led some states to fall well short of the intended goals. Yet, the policies and programs continued as the pursuit of the outcome became more important than the path itself. Much of this happened as a result of the legislation authorizing the grant-based programs meeting the BJS criteria. Similarly, the estimated outcomes (both savings and prison populations) were over-stated and led the working groups to continue pursuing these evidence-based programs from the state level (Austin & Coventry, 2014; Clear, 2011; Clements et al., 2011; Sabol & Baumann, 2020). A common theme found in the critical literature is that local-level stakeholders have been overlooked but face the brunt of the success or failure of the policies and programs (see LaVigne et al., 2013). Another aspect presented by Sabol & Baumann (2020) is that although justice reinvestment has shown some problematic returns in investment, the prevailing fact remains that states are continuing to follow federal funding through technical assistance initiatives. Thus, the justice reinvestment initiative has been incredibly successful at enrolling and recruiting states to participate in the data-driven approach.

Tracking the Funding

According to the BJS guidelines, states pursuing grant funding need to demonstrate the use of evidence-based practices that are centered on data-driven approaches (BJS, 2019b). In the fiscal year 2018, the BJS notes that as many as 36 states are using funding based on technical assistance related to JRI, with a total of $5.5 million awarded towards the use of these programs (BJS, 2019c). Washington and Maine received the highest amounts of grant funding ($464,852 and $426,101 respectively), while New York and Indiana ($33,276 and $21,848 respectively) received the lowest. Most states fall in the $100,000-$200,000 range for funding, even while prison rates decline from the 1990s and early 2000s. According to BJS records beginning in 2010, when the federal legislation incentivized justice reinvestment, forty-eight states (including Alaska and Hawaii) have applied for and received grant funding to pursue JRI policies. Twenty of those states receive funding each year. Table 1 presents the annual BJS allotment for grant awards by the highest awarded ten states beginning in 2010 when funding was first made available. The states are listed in alphabetical order and further listed by grant award year, with the highest awarded states provided in table 1. Washington was the highest awarded state during JRI funding, with a total of $1.47 million over nine reported years. The next highest awarded state was Michigan ($1.28 million) followed by Kentucky ($1.23 million), and finally Iowa ($1.06 million), all equaling over $1 million dollars in total funding. The remaining six states all received well over $700,000 in total funding, with Missouri ($793,703) having the lowest average during the time frame.

Table 1. BJS State Grant Awards

Fiscal Year	District of Columbia	Illinois	Iowa	Kentucky	Maryland	Michigan	Missouri	Oregon	Pennsylvania	Washington
2018	150,000	177,035	187,924	228,434	212,927	224,043	66,000	208,069	224,960	464,852
2017	150,000	114,334	152,146	209,738	63,348	208,221	156,298	222,940	209,967	116,339
2016	149,375	101,394	181,040	188,709	206,437	209,966	97,729	61,517	119,080	149,317
2015	60,000	58,676	163,205	189,959	56,444	209,549	210,951	59,900	100,995	184,334
2014	60,000	58,848	83,808	189,140	59,940	208,818	51,412	59,742	59,984	298,131
2013	60,000	78,159	74,935	60,000	73,365	58,246	44,367	56,624	79,288	64,960
2012	60,000	76,978	75,000	60,000	83,097	59,815	59,861	60,277	70,000	57,228
2011	60,000	72,646	75,000	60,000	71,982	59,066	59,861	72,000	73,000	58,177
2010	50,000	68,208	68,094	50,000	85,195	50,000	47,224	105,115	48,050	85,555
Totals	799,375	806,278	1,061,152	1,235,980	912,735	1,287,724	793,703	906,184	985,324	1,478,893

Note. Numbers are listed in dollar amounts.

Funding for the JRI policies remains a crux for state legislators as they navigate various programs and diversionary alternatives to meet the goals for reapplication in the subsequent years. State legislators and working groups pursue grant-based funding to improve their criminal justice systems with the overarching goal of reducing the reliance on prisons and exorbitant spending. Many of these policies follow what can be considered an evidence-based and data-driven framework, ultimately focusing on reforming the justice system. The programs and policies associated with each state must show a promising return to be considered for future funding, which presents a problematic equation. As working groups present the needs of their respective jurisdictions, the associated grant application must show promising results or the possibility of effective strategies regarding the administration of justice. Thus, programs must be presented as being effective and working towards meaningful reform to be continually funded with BJS awards. This pressure could influence some of the decision-making and policy decisions of both practitioners and administrators working within the justice system. Justice reinvestment working groups often reflect state officials, which presents the opportunity for a top-down scenario where front-line practitioners may be pressured to meet the goals of the JRI programs they are implementing. Similarly, prison populations have been

declining since the early 2000s, when the justice reinvestment concept was first introduced, potentially posing a threat to the efficacy of justice reinvestment-associated policies.

Were Prison Populations Already Declining?

Reviewing the common policies associated with justice reinvestment, common themes emerge with each state. Many of these themes focus on initial entry into the system (e.g., sentencing strategies) and recidivism rates. To further explore the impact of justice reinvestment on the custody levels, court commitments, parole violations, and sentences greater than one year are graphed using national prisoner statistics (Department of Justice, 2020). Custody is defined as total inmates in local jails, prisons, private facilities, and centers (to include halfway houses and hospitals) operated by the state. Court commitments are defined as new court sentences within the past year. Parole violations are defined as sentences within the past year for violations while under supervision. Finally, sentences greater than one year refer to the harshness of punishment and are defined as sentences that require punishment of greater than 1 year or 12 months. All numbers were aggregated for both men and women for graphing purposes to offer a visual aid. The variables show trends prior to the federal legislation and the subsequent years leading up to the reauthorization of justice reinvestment. Figure 1 shows nationwide incarceration trends beginning in 2006 when justice reinvestment was first piloted as a criminal justice policy in Connecticut.

Trends reveal rates of recommitment and custody levels for men were decreasing prior to the federal legislation, which incentivized the use of justice reinvestment. Overall, custody rates decreased from 1,289,485 in 2006 to 1,228,171 in 2015, with 2008 producing the highest level at 1,303,505. Other rates remained relatively stable as both recommitments to court and parole violations presented little change through 2006-2015. However, when graphing the changes for new sentences based on parole violations, data show a decrease beginning in 2009 (45,213) and continuing to the lowest levels in 2015 (25,181). Female offenders showed similar trends as reported custody levels, commitments, and sentences greater than one year decreased from 2006 to 2012. Figure 2 shows that in the years following 2012, trends increased

nationwide, with only rates of parole violations decreasing. These variables are graphed in ascending order, as shown in Figures 1 & 2.

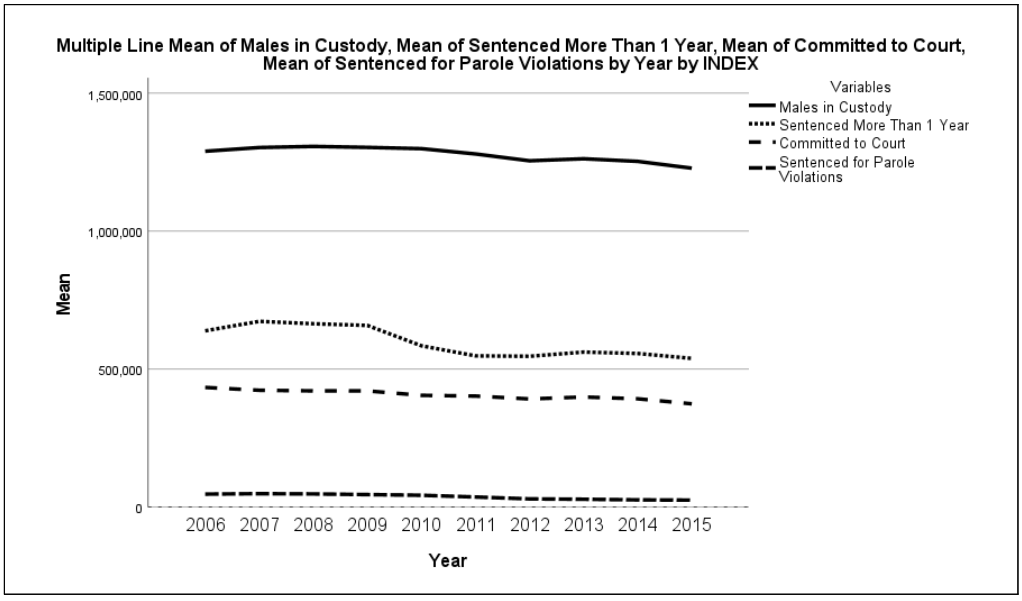

Figure 1. Nationwide rates for male offenders

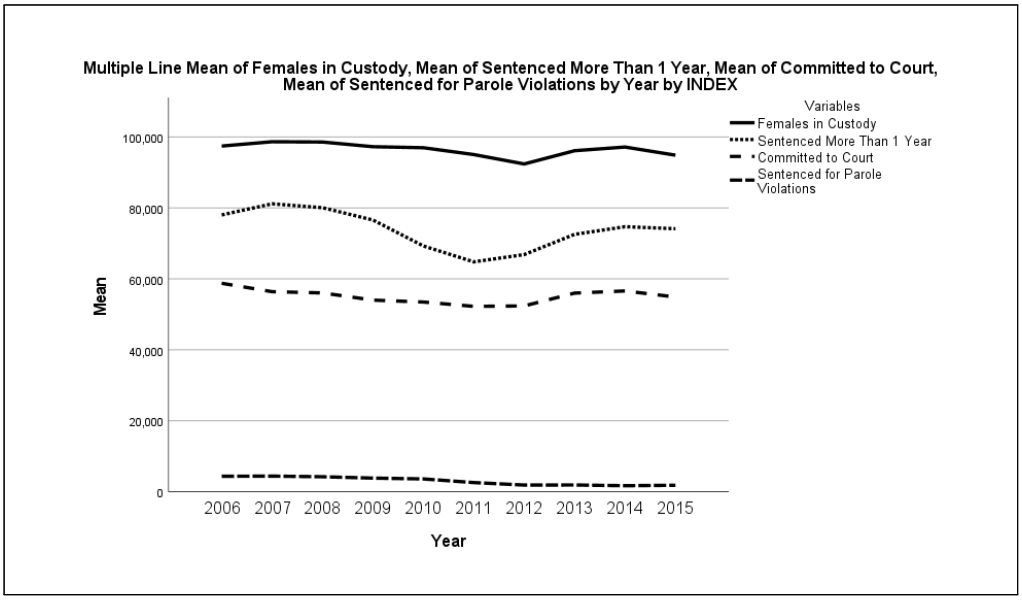

Figure 2. Nationwide rates of female offenders

With the primary focus of justice reinvestment being to reduce prison populations while diverting funding to community-based programs, many argue that justice reinvestment has offered promising results through reduced parole revocation (Fabelo, 2010), re-imagined structured sentencing strategies (Murdock, 2016) and greater availability to correctional-programming (Taxman et al., 2014). As one of the overarching goals being to reduce prison populations, JRI can be touted as a success. However, these trends appear to be decreasing before the federal legislation and incentivized grant funding associated with the initiative. Justice reinvestment may have helped with the declining populations, but it should not be credited as the sole cause for the declining numbers. Although the JRI federal program was helping to increase the efficacy of community-programs, there are multiple explanations that could influence prison populations and crime rates. For example, Murdock (2016) notes the previous attempts in state-based sentencing strategies in the name of reform which were implemented in the 1990s. Similarly, other reform efforts aligned with JRI may have influenced the declining prison populations and reduced correctional spending prior to the federal incentives (Clear, 2011). Many factors influence the effectiveness of JRI as states continue pursuing criminal justice reform. The success of JRI is a complex topic that is not easily understood considering that many states and jurisdictions can pursue varying approaches to evidence-based policy, which makes them eligible for the JRI funding. For some jurisdictions, the focus becomes public-facing dashboards depicting the trends in correctional control and prison populations (Clement, Schwarzfeld, & Thompson, 2011). Using the interactive dashboards provided by external agencies and individual state agencies, JRI shows promising returns for the investment. These dashboards show the current and projected populations, funding diverted from the use of these policies, and other jurisdictional information relevant to the use of JRI as a means of transparency and public awareness. One of the overlooked aspects of these dashboards is that maintaining the statistics and creating public-facing websites is considered eligible for funding under the JRI (BJS, 2019a), potentially influencing the need to show successful outcomes of jurisdictional policies.

Table 2 presents a list of states using what can be considered back-end policies associated with justice reinvestment. Back-end policies are designed to

reduce the volume of violations parolees/probationers face while under supervision. Namely, technical violations and general conditions are often altered to reduce the sentence if an offender does commit a violation. Back-end approaches also include the use of short-minimum sentencing for violations that rely on community corrections centers as opposed to reincarceration (Bergstrom & Bucklen, 2016). According to data from Pew Foundation (2019), the most popular back-end policies were related to streamlining the parole process to reduce the time an eligible offender waits for a hearing and subsequent release. Following the parole efforts, states also placed emphasis on early-release credits allowing for more offenders to become eligible for release earlier in their sentence.

Table 2. States using "Back-End" policies

Release Strategies: Streamline Parole Process and Eligibility for Parole	Release Strategies: Expanding Good-Time Credits and Earned-Time Credits
Alabama	Alaska
Alaska	Georgia
Arkansas	Kansas* (2007)
Georgia	Louisiana
Hawaii	Maryland
Idaho	Mississippi
Kansas	Nevada* (2007)
Kentucky	North Carolina
Louisiana	Ohio
Maryland	Oregon
Michigan	Rhode Island
Mississippi	South Carolina
Montana	Utah
Nebraska	
New Hampshire	
Rhode Island	
South Carolina* (2010)	
South Dakota	
Utah	

Source: PEW Charitable Trust: 35 States Using Justice Reinvestment.
Note. * = Indicates the first state to pass legislation with associated year.

Table 3 presents states that are using front-end justice reinvestment policies. The front-end of the justice reinvestment approach shifts the emphasis from offenders going back to jails or prisons and tries to prevent them from incarceration altogether. The front-end policies are often the second wave of legislation as states implement their tailored justice reinvestment approach. The front-end policies focus on sentencing strategies and the discretionary powers afforded to judges during the trial's sentencing phase. States using front-end policies focus their efforts on revising the codified statutes and definitions for low-level crimes, particularly drug and property offenses. Similarly, mandatory sentencing strategies are often a key factor for continually high prison populations (Petersilia & Cullen, 2015; Tonry, 2014). The states listed in Table 3 are pursuing legislation to reduce or revise the use of mandatory sentencing strategies and rely more heavily on discretionary guidelines.

Table 3. States using "Front-End" policies

Sentencing Strategies: Re-classify Low Level Crimes: Drugs and/or Property Offenses	Sentencing Strategies: Enhancements and/or Presumptive Guidelines	Sentencing Strategies: Mandatory Minimum Policies
Alabama	Alabama	Alaska
Alaska	Alaska	Georgia
Arkansas	Georgia	Hawaii
Georgia	Hawaii	Louisiana
Hawaii	Kentucky	Maryland
Kentucky	Louisiana	Montana
Louisiana	Mississippi	Oregon
Maryland	Montana	South Carolina (2010)*
Mississippi	Nebraska	
Montana	North Dakota	
Nebraska	Ohio	
North Carolina	Oregon	
North Dakota	South Carolina (2010)*	
Ohio	Utah	
Oregon		
Rhode Island		
South Carolina (2010)*		
South Dakota		
Utah		

Source: PEW Charitable Trust: 35 States Using Justice Reinvestment.
Note. * = Indicates the first state to pass legislation with associated year.

The final policy associated with justice reinvestment is the reliance on community corrections facilities and improving treatment plans for individual offenders (Bergstrom & Bucklen, 2016; Taxman et al., 2014). Specifically, states adhering to justice reinvestment from the community corrections aspect recognize the need for appropriate assessment and development of specific rehabilitation goals for each offender and not simply a general approach where each type of offender is grouped together. For these states, the goals become developing risk-needs assessments and ensuring that the agreed-upon measurement tool meets the needs outlined by the working group. Other popular policies stem from the recognition of mental health and behavioral needs in a correctional population. Thus, states have adopted legislation that introduces or improves upon the in-patient/out-patient treatment resources and availability to these resources. Table 4 shows the various legislative approaches to justice reinvestment in a community-corrections setting.

Table 4. Community Corrections Policies

Risk Needs Assessments	Behavioral and Mental Health Policies	Graduated Sentencing for Parole/Probation Violation
Alabama	Alabama	Alabama
Alaska	Alaska	Alaska
Arkansas	Connecticut	Arkansas
Connecticut (2008)	Delaware	Delaware
Delaware	Georgia	Georgia
Georgia	Hawaii	Hawaii
Hawaii	Idaho	Idaho
Idaho	Kansas* (2007)	Kansas
Illinois	Kentucky	Kentucky
Kentucky	Louisiana	Louisiana
Louisiana	Michigan	Maryland
Maryland	Mississippi	Mississippi
Michigan	Montana	Montana
Mississippi	Nebraska	Nebraska
Montana	Nevada* (2007)	Nevada* (2007)
Nebraska	North Carolina	North Carolina
North Carolina	North Dakota	North Dakota
North Dakota	Ohio	Oregon
Ohio	Oregon	Pennsylvania
Oregon	Pennsylvania	South Carolina
Rhode Island* (2008)	Rhode Island	South Dakota
South Carolina	South Dakota	Texas* (2007)
South Dakota	Texas* (2007)	Utah
Utah	Utah	West Virginia
West Virginia	Vermont	
	West Virginia	
	Wisconsin	

Source: PEW Charitable Trust: 35 States Using Justice Reinvestment.
Note. * = Indicates the first state to pass legislation with associated year.

To date, 36 states are using some form of justice reinvestment legislation (CSG, 2019), with additional states pursuing related funding. As justice reinvestment policies continue receiving attention, and more states are applying for funding, the initial goals seemingly have been met. One aspect that seems not to receive much focus, however, is the reinvestment aspect of the approach. For jurisdictions to receive justice reinvestment funding through federally grant-based incentives, the legislature must adopt and present policies adhering to data-driven, evidence-based policies associated with the BJS funded initiative (BJS, 2019b).

INTERNATIONAL PERSPECTIVES ON JUSTICE REINVESTMENT

Justice Reinvestment is a global phenomenon observed across different countries, including the United Kingdom and Australia (Homel, 2014; Willis & Kapira, 2018). In a report written for the New South Wales Parliament, Roth (2016) offers a review of justice reinvestment and details the successes that have occurred thus far with American states and local jurisdictions. Applying justice reinvestment to Aboriginal populations, the New South Wales (NSW) approach seeks to reduce the high rates of incarceration, particularly with younger generations of the Aboriginal population (Willis & Kapira, 2018). One initiative is coined the Maranguka and emphasizes a small indigenous community that experiences high rates of imprisonment. The Maranguka justice reinvestment approach focuses on building trust within the community and relying on data-driven outcomes to reduce the incarceration rate (Roth, 2016). Another justice reinvestment approach used in Australia is being utilized in the community of Cowra. The Cowra approach to justice reinvestment aims to reduce rates of imprisonment by creating more meaningful lives and abstaining from criminal acts (Roth, 2016). Other approaches are being used throughout Australia, all of which focus on specific communities and reduce the funding and resources used for imprisonment. Criticism for the use of justice reinvestment in Australia is the lack of definitions and the specific allocations for funding generated from savings (Brown et al., 2012). Austin and Coventry

(2014) note considerable disproportionate incarceration rates between indigenous populations and nonindigenous populations. This point is juxtaposed to the United States incarceration rate and the current prison population's varying demographics. Austin and Coventry (2014) find that the incarceration in Australia is approximately 1/6 the rate of the incarceration rate in the United States. Although many aspects of policing and expenditures remain comparable between the two countries, Austin and Coventry (2014) pose the argument that Australia does not rely on incarceration as a punishment to the extent of the United States.

England and Wales have also adopted the use of justice reinvestment with a focus on diversionary programs and community-based services. In a report presented to Parliament by the Ministry of Justice (2010), the focus for justice reinvestment would be decentralizing the current criminal justice method and moving towards a more individualized approach (Allen, 2011; Homel, 2014; Ministry of Justice, 2010). Payment by results method would be adopted in which the reinvestment would incentivize the reduction of prison and jail populations. This approach coincides with the cost-benefit aspect of justice reinvestment and offers the freedom for local jurisdictions to specifically tailor their approach to their population's needs. Similarly, a focus on youthful offenders and the development of diversionary programs was also implemented through the payment by results method (Ministry of Justice, 2010). The popularity of justice reinvestment has continued to spread across the globe with various governments, such as England, Wales, and Australia, adopting the data-driven, cost-effective reform movement. Austin and Coventry (2014) note that the rise in popularity of justice reinvestment practices has spread into other nations such as Ireland, Canada, and New Zealand.

DISCUSSION

The popularity of justice reinvestment has become a sticking point for its success. Specifically, concerning the JRI funding, states show important declines in both correctional populations and the subsequent spending on jails/prisons (Sabol & Baumann, 2020; NCSL, 2019). With over 30 states using justice reinvestment in various policies, the JRI program is producing the intended outcomes that it was designed to do: create a path toward meaningful criminal justice reform. The impact and overall influence of the JRI program may be somewhat overstated, though. As correctional populations began declining in the 2000s, the justice reinvestment approach seemed to offer the best of both worlds by maintaining public safety while also reducing prison populations and using the diverted funding for high-risk communities. The current use of the program may not be entirely in line with that initial goal as the diverted funding seems to focus on criminal justice strategies and not community-based programs, which was the original allure of the effort.

The justice reinvestment push has led to numerous legislative changes across the country as states such as Arizona implement policies to increase treatment for probationers and parolees (Safe Communities Act, 2008) while other states seek to streamline the parole process and improve effective placement (Bergstrom & Bucklen, 2016; Fabelo, 2010; Murdock, 2016). Non-contiguous states have pursued justice reinvestment (Armstrong, 2016) as the concept spreads throughout the world to countries like England and Australia (Allen, 2011). The theoretical framework is situated in a common goal but implementing the policies and pursuing JRI funding varies greatly to include a divergence from the community-funded approach of the original concept.

We propose that the JRI programs can benefit by incorporating crime mapping or geospatial analyses. Criminologists have shown that the use of geographic information systems (GIS) mapping technology is useful in identifying and understanding crime patterns (Brantingham & Brantingham, 1999; Eck, Chainey, Cameron, & Wilson, 2005; Ratcliffe & McCullagh, 1999). Scholars have pointed out unique spatial distributions of incarceration in communities (e.g., high-incarceration communities) and some potential factors associated with

the phenomena (e.g., employment rates) (Clear, 2011; Homel, 2014; Tucker & Cadora, 2003). However, systematic understanding of geospatial patterns involving the areas marked by high incarceration areas is very limited. These findings can provide the groundwork for justice reinvestment in a community-corrections setting. Presently, many states and jurisdictions provide public-facing dashboards that show the efforts of the justice reinvestment initiative. However, few of these dashboards focus on the high crime areas as originally suggested by Tucker & Cadora (2003).

Barriers to Justice Reinvestment

The JRI movement has led many states to note the funding and availability for technical assistance to submit for federal funding through the initiative. Although many programs and policies are tied to incentive-based funding throughout the criminal justice system, none has risen to the popularity and widespread use quite like justice reinvestment. Sabol & Baumann (2020) note that states continue pursuing the evidence-based programs throughout the initiative, yet budgets have remained modest throughout the last decade, even declining in some states. Similar trends occurred in prison populations as states like California were ordered to reduce prison populations due to extreme over-crowding (Brown v. Plata, 2011), yet most of the population were moved to county jails. Crime rates were also decreasing across the nation as justice reinvestment rose to prominence creating a situation in which justice reinvestment may not be able to take full responsibility for the claims of reducing prison populations. The prison populations may have only been influenced marginally by the methods found through each working group. With prison populations decreasing prior to the use of JRI and budgets remaining stable from year to year, the JRI approach may have been introduced during a time when positive results were occurring without the incentivized programs. The use of JRI funding to facilitate evidence-based programs may not have caused the goals of justice reinvestment, but these goals seem to have been in motion before federal legislation (Criminal Justice Reinvestment Act, 2010).

Each state is permitted the flexibility in creating and maintaining a working group; however, each working group may consist of varying levels of legislators, court officials, and/or practitioners who are then labeled stakeholders

(Bergstrom & Bucklen, 2016; BJS, 2019a; CSG, 2012). Thus, the title of stakeholder could be used to fit a myriad of individuals who are directly influenced by the policies and practices of JRI. This becomes problematic because justice reinvestment is often credited as being a local-level solution. Stakeholders and the members of the working groups may also serve as a barrier to effectiveness in some regards. LaVigne and colleagues (2013) offered planning guides for local-level implementation, and Clear (2011) argues for incentivizing the communities using JRI effectively rather than a broad, over-arching approach. Yet, many of the working group members are comprised of state-level officials or executives. To meet the needs of the outcomes associated with justice reinvestment, working groups should solicit more participation from practitioners and executives at the county levels. Using this approach will likely lead to lengthier discussions of practical ways of meeting the BJS definition for funding. Still, it will likely also produce a more effective approach with more holistic policies that reduce the possibility of competing grants or programs.

During the rise of justice reinvestment and the corresponding federal initiative, other legislative changes were underway throughout the country. Namely, federal legislation curbing the sentencing disparity dramatically impacted drug offenders with the Fair Sentencing Act (2010). Varying forms of legislation were signed into law intended to directly impact reducing prison populations (e.g., First Step Act, 2018; Sentencing Reform and Corrections Act, 2017). States were also passing jurisdiction-specific legislation such as Pennsylvania with the signing of the Clean Slate Act (2018), which allowed the expungement of records for low-level offenders if they did not commit a new offense within the previous ten years. Similar approaches are happening at the county level with programs like the Safety and Justice Challenge, allowing incentive-based funding for counties seeking meaningful approaches to reducing prison and jail populations through the MacArthur Foundation. A similar goal is justice reinvestment. Currently, the MacArthur Foundation funds 52 cities or counties to understand better the use of the correctional system (Garduque, 2020). Many of the sites receiving funding are co-located in states using justice reinvestment as well.

CONCLUSION

Prisons and jails are overcrowded, leading to risky and dangerous situations throughout correctional institutions nationwide. Justice reinvestment and the associated funding are designed to curb the correctional populations while emphasizing on maintaining public safety through incentivized programs. Although there are many reasons to support JRI programs, some caution should be taken when describing the sustainability and effectiveness of the approach. With the growing number of states using JRI, and the varying ways that states can choose to implement the policies or programs, many areas of the initiative remain relatively unknown even with the development of user-friendly dashboards and public access to specific data. This theoretical analysis of JRI policies shows that most states are relying on similar methods to achieve reduced prison populations. Although the programs and policies are rooted in the empirical literature, the prison populations appear to have been decreasing before the federal legislation. A positive aspect of correctional reform, and a goal of JRI, is reducing the need for correctional institutions in a traditional sense and instead focusing on community-oriented programs. Justice reinvestment is built upon the simple notion of reducing prison populations while maintaining public safety. The similarity in approaches across jurisdictions suggests the effectiveness of various policies associated with JRI, yet prison populations and crime rates were declining prior to the use of justice reinvestment. After all, if revised sentencing strategies, improved parole efficiency, and more accurate offender assessments lead to lower prison populations, states should emphasize these programs nationwide. More research is needed in the wake of JRI policies to determine the sustainability of the approaches and how much impact the associated grant funding has on implementing the programs. Although this review lacks a statistical analysis, it does push the critical literature of justice reinvestment forward as more information becomes available. Future studies should focus on an analytical cost-benefit of the funding associated with this research and determine where the allotted funding is going.

We suggest that there are several ways to evaluate the effectiveness of the

JRI programs. First, we can use a quasi-experimental research design to tease out the influences of confounding variables (Bunting, Staton, Winston, & Pangburn, 2019; Shadish, Cook, & Campbell, 2002). Many different statistical models (e.g., time series analysis) enable researchers to consider time trends to identify the effects of variables of interests. Second, researchers can evaluate individual correctional programs based on a randomized experiment (Ayoub, 2020; Petersilia, 1989). For instance, if diverted funds can be spent on implementing a particular community-based diversionary program, we can divide the community into smaller units and randomly choose units to implement the community-based program and compare the outcomes (e.g., recidivism rates). Third, we can consider other outcome variables to evaluate the success of the JRI programs (Hyatt & Han, 2018; Link, Ward, & Stansfield, 2019). For example, the percentage of individuals participating in community diversionary programs can be one outcome variable. If more people are participating in community diversionary programs since the JRI programs are implemented, it may signal the positive impact of the JRI legislature on corrections. Relatedly, subjective and objective outcomes from the participation in the programs are critical. Policymakers should keep track of the recidivism rates among those who participate in the programs. Also, understanding how participants feel about the programs can be very important because it is related to the future of the JRI programs.

According to the current fiscal year summaries, the use of JRI programs and incentive-based grant funding is not likely to dissipate. With a relatively stable budget of $25 million made available each year (DOJ, 2019), JRI will likely continue as an approach to reducing prison populations as states continue the pursuit of the funding. Reports from the most recent program summary indicate that states have generated savings as high as $491 million and a total of over $1 billion nationwide (DOJ, 2019). The outcomes for JRI present an opportunity for substantial funding to be made available through alternative criminal justice avenues as reliance continues shifting towards rehabilitation and community-oriented programs. As JRI continues gaining momentum and as more states adopt the policies associated with justice reinvestment, the prison populations will likely continue decreasing, just as they were before justice reinvestment legislation.

Note

1. There has not been landmark or major legislative changes from the Biden administration.

References

Allen, R. (2011). Justice reinvestment and the use of imprisonment: Policy reflections from England and Wales. *Criminology & Public Policy, 10*(3), 617-627.

Armstrong, B. (2016). Justice reinvestment report. *Alaska Justice Forum, 32*(4), 4-6.

Ayoub, L. H. (2020). The impact of reentry court on recidivism: a randomized controlled trial in Harlem, New York. *Journal of Experimental Criminology, 16*(1), 101-117.

Aos, S., Miller, M., & Drake, E. (2006). Evidence-based public policy options to reduce future prison construction, criminal justice costs, and crime rates. *Federal Sentencing Reporter, 19*, 275–290.

Ariel, B., Weinborn, C., & Sherman, L.W. (2016). "Soft" policing at hot spots-do police community support officers work? A randomized controlled trial. *Journal of Experimental Criminology, 12,* 277-317.

Austin, J., Cadora, E., Clear, T.R., Dansky, K., Greene, J., Gupta, V., Mauer, M., Porter, N., Tucker, S., Young, M.C. (2014). Ending mass incarceration: Charting a new justice reinvestment. *The Sentencing Project.* Retrieved from https://www.sentencingproject.org/wp-content/uploads/2015/12/Ending-Mass-Incarceration-Charting-a-New-Justice-Reinvestment.pdf

Austin, J., & Coventry, G. (2014). A critical analysis of justice reinvestment in the United States and Australia. *Victims & Offenders, 9,* 126-148.

Austin, J., & Coventry, G. (2001). *Emerging issues on privatized prisons*. Washington, DC: US Department of Justice, Office of Justice Programs.

Brantingham, P. L., & Brantingham, P. J. (1999). A theoretical model of crime hot spot generation. *Studies on Crime & Crime Prevention, 8*(1), 7–26.

Brown, D., Schwartz, M. & Boseley, L. (2012). The promise of justice reinvestment. *Alternative Law Journal* 37(2), 96-102.

Bunting, A.M., Staton, M., Winston, E., & Pangburn, K. (2019). Beyond the employment dichotomy: An examination of recidivism and days remaining in the community by post-release employment status. *International Journal of Offender Therapy and Comparative Criminology, 63*(5), 712-733.

Bureau of Justice Statistics. (2019a). *Justice reinvestment initiative.* Retrieved

from https://www.bja.gov/programs/justicereinvestment/index.html.
Bureau of Justice Statistics. (2019b). *What is JRI?* Retrieved from https://www.bja.gov/programs/justicereinvestment/what_is_jri.html.
Bureau of Justice Statistics. (2019c). State profiles. Retrieved from https://www.bjs.gov/index.cfm?ty=tp&tid=481.
Carroll, L. (2004). Prison siting, rural development, racism, and justice reinvestment. *Criminology & Public Policy, 3*(3), 481-488.
Clean Slate Act. (2018). PL 402, No. 56, HB 1419. Clean Slate Act. Retrieved from https://www.legis.state.pa.us
Clear, T. (2011). A private-sector, incentives-based model for justice reinvestment. *Criminology & Public Policy, 10*(3), 585-608.
Clement, M., Schwarzfield, M., & Thompson, M. (2011). *The national summit on justice reinvestment and public safety: Addressing recidivism, crime, and corrections spending.* Report prepared for The Council of State Governments. Retrieved from https://www.bja.gov/publications/csg_justicereinvestmentsummitreport.pdf.
Criminal Justice Reinvestment Act of 2009. (2010). 111th Cong., 1st Sess. Retrieved from https://www.govtrack.us/congress/bills/111/s2772.
Cook, T. D., Campbell, D. T., & Shadish, W. (2002). *Experimental and quasi-experimental designs for generalized causal inference*. Boston, MA: Houghton Mifflin.
Council of State Governments. (2019a). *Connecticut.* Retrieved from https://csgjusticecenter.org/jr/ct/.
Council of State Governments. (2019b). *Pennsylvania.* Retrieved from https://csgjusticecenter.org/jr/pa/.
Council of State Governments. (2019c). *Justice reinvestment in Pennsylvania: Policy framework*. Retrieved from https://csgjusticecenter.org/wp-content/JR-in-Pennsylvania.pdf.
Council of State Governments. (2012). *Justice reinvestment in Pennsylvania: Final summary & policy options for consideration.* Retrieved from http://www.cor.pa.gov/General%20Information/Documents/Justice%20Reinvestment%20Initiative/JRI%20May%2023%202012%20Presentation.pdf.
Cullen, F.T., Jonson, C.L., & Mears, D.P. (2016). Reinventing community corrections. *Crime & Justice, 46*(1), 27-93.
Department of Justice. (2019). *Office of justice programs: FY 2020 program summaries.* Retrieved from https://www.justice.gov/jmd/page/file/1160581/download
Department of Justice. (21 January 2020). Office of Justice Programs. Bureau of Justice Statistics. National Prisoner Statistics, 1978-2015. Ann Arbor, MI: Inter-university Consortium for Political and Social Research

[distributor], 2017-01-05. https://doi.org/10.3886/ICPSR36657.v1

Doob, A.N., & Webster, C.M. (2014). Creating the will to change: The challenges of decarceration in the United States. *Criminology & Public Policy, 13*(4), 547-559.

Eck, J., Chainey, S., Cameron, J., & Wilson, R. (2005). Mapping crime: Understanding hotspots. U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, 1-79.

Fabelo, T. (2010). Texas justice reinvestment: Be more like Texas? *Justice Research & Policy 12*(1), 113-131.

First Step Act. (2020). S. 3747 — 115th Congress: First Step Act of 2018. Retrieved from https://www.govtrack.us/congress/bills/115/s3747

Fox, C., Albertson, K., & Warburton, F. (2011). Justice reinvestment: Can it deliver more for less? *The Howard Journal, 50*(2), 119-136.

Fox, C., Albertson, K., & Wong, K. (2013). *Justice reinvestment: Can the criminal justice system deliver more for less?* New York, NY: Routledge.

Garduque, L. (2020). *About the challenge.* Retrieved from http://www.safetyandjusticechallenge.org/about-the-challenge/.

Homel, R. (2014). Justice reinvestment as a global phenomenon. *Victims & Offenders, 9*(1), 6-12.

Hyatt, J.M., & Han, S.H. (2018). Expanding the focus on correctional evaluations beyond recidivism: The impact of halfway houses on public safety. *Journal of Experimental Criminology, 14*, 187-211.

Kleiman, M.A.R. (2011). Justice reinvestment in community supervision. *Criminology & Public Policy, 10*(3), 651-659.

LaVigne, N., Davies, E., Lachman, P., & Neusteter, S.R. (2013). Justice reinvestment at the local level: Planning and implementation guide (2 eds). *Urban Institute.* Retrieved from https://www.urban.org/policy-centers/justice-policy-center/projects/justice-reinvestment-local-level.

Link, N.W., Ward, J.T., & Stansfield, R. (2019). Consequences of mental and physical health for reentry and recidivism: Toward a health-based model of desistance. *Criminology, 57*(3), 544-573.

Malcolm, J.G. (2014). Criminal justice reform at the crossroads. *Texas Review of Law & Politics, 20*(2), 249-293.

Maruna, S. (2011). Lessons for justice reinvestment from restorative justice and the justice model experience: Some tips for an 8-year-old prodigy. *Criminology & Public Policy, 10*(3), 661-669.

Monteiro, C.E., & Frost, N.A. (2015). Altering trajectories through community-based justice reinvestment. *Criminology & Public Policy, 14*(3), 455-462.

Murdock, R. (2016). The justice reinvestment act in North Carolina and its impact on sentencing.
Federal Sentencing Reporter, 29(1), 39-46.

National Conference of State Legislators. (2019). Justice reinvestment state resources. Retrieved from http://www.ncsl.org/research/civil-and-criminal-justice/justicereinvestment.aspx.

Pennsylvania Commission on Crime and Delinquency. (2017). *Current JRI in Pennsylvania (2016)*. Retrieved from http://www.pccd.pa.gov/

Petersilia, J., & Cullen, F.T. (2015). Liberal but not stupid: Meeting the promise of downsizing prisons. *Stanford Journal of Criminal Law and Policy, 2*, 1-43.

Petersilia, J. (1989). Implementing randomized experiments: Lessons from BJA's intensive supervision project. *Evaluation Review, 13*(5), 435-458.

Pew Center on the States. (2019). 35 states using justice reinvestment. Retrieved from https://www.pewtrusts.org/-/media/assets/2018/07/pspp_reform_matrix.pdf.

Pew Center on the States. (2011). *The impact of Arizona's probation reforms.* Retrieved from http://www.pewtrusts.org/en/research-and-analysis/issue-briefs/2011/05/07/the-impact-of-arizonas-probation-reforms.

Ratcliffe, J. H., & McCullagh, M. J. (1999). Hotbeds of crime and the search for spatial accuracy. *Journal of geographical systems*, *1*(4), 385-398.

Roth, L. (2016). *Justice reinvestment*: New South Wales Parliamentary Research Service.

Sabol, W.J. & Baumann, M.L. (2020). Justice reinvestment: Vision and practice. *Annual Review of Criminology, 3,* doi 10.1146/annurev-criminol-011419-041407.

Safe Communities Act. 48th state legislature, 2nd Sess., Arizona, (2008). Retrieved from http://www.azcourts.gov/apsd/Safe-Communities-Act.

Sentencing Reform and Corrections Act. (2017). 115th Con., S. 1917.

Sherman, L. W., & Weisburd, D. (1995). General deterrent effects of police patrol in crime "hot spots": A randomized, controlled trial. *Justice quarterly*, *12*(4), 625-648.

Story, B. (2016). The prison in the city: Tracking the neoliberal life of the "million dollar block". *Theoretical Criminology,20*(3), 257-276.

Taxman, F.S. (2016). Justice reinvestment: Extending the framework to non-justice efforts.
Federal Sentencing Reporter, 29(1), 52-57.

Taxman, F.S., Pattavina, A., & Caudy, M. (2014). Justice reinvestment in the United States: An empirical assessment of the potential impact of

increased correctional programming on recidivism. *Victims and Offenders, 9*(1), 50-75.

Tonry, M. (2019). Fifty years of American sentencing reform: Nine lessons. *Crime and Justice, 48*(1), 1-34.

Tonry, M. (2014). Remodeling American sentencing: A ten-step blueprint for moving past mass incarceration. *Criminology & Public Policy, 13*(4), 503-533.

Tucker, S. B., & Cadora, E. (2003). Justice reinvestment. *IDEAS for an Open Society, 3*(3), 2-5.

Urban Institute. (2013). *Justice reinvestment at the local level: Planning and implementation guide* (2nd ed). Washington, D.C. Retrieved from: https://www.urban.org/sites/default/files/publication/24076/412930-Justice-Reinvestment-at-the-Local-Level-Planning-and-Implementation-Guide-Second-Edition.PDF

Urban Institute. (2010). *Justice reinvestment at the local level: Planning and implementation guide.* Washington, D.C. Retrieved from: https://www.urban.org/research/publication/justice-reinvestment-local-level-planning-and-implementation-guide.

West, S.L., & O'Neal, K.K. (2004). Project D.A.R.E. outcome effectiveness revisited (Drug Abuse Resistance Education). *The American Journal of Public Health, 94*(6), 1027-1030.

Wilson, J. Q., & Kelling, G. L. (1982). Broken windows. *Atlantic monthly*, *249*(3), 29-38.

Willis, M., & Kapira, M. (2018). *Justice reinvestment in Australia: A review of the literature*: Australian Institute of Criminology.

Wodahl, E.J., & Garland, B. (2009). The evolution of community corrections: The enduring influence of the prison. *The Prison Journal, 89S*(1), 81S-104S.

Wong, K. (2016). Justice reinvestment: "Motherhood and apple pie?" Matching ambition to capacity and capability. *Federal Sentencing Reporter, 29*(58), 1-16.

International Journal of Criminal Justice

114 Taebong-no, Seocho-gu, Seoul, 06764, Republic of Korea
https://www.kic.re.kr/international/

Printed in Seoul, Korea
30 June, 2021

ISSN 2713-5152

CALL FOR PAPERS

International Journal of Criminal Justice

AIM AND SCOPE

The International Journal of Criminal Justice (IJCJ), a biannual and peer-reviewed English journal published by Korean Institute of Criminology (KIC), facilitates comprehensive analysis and evidence-based research on crime trends in order to make a contribution to national policies for crime prevention and criminal justice policies.

The IJCJ will share academic and practical views from home and abroad and play a pivotal role as an international academic forum for domestic and foreign criminal polices.

SUBMISSION DETAILS

- Manuscripts should be written in English and should be no more than 10,000 words in MS word.
- Please provide an abstract which should be no more than 200 words in length and a maximum of 5 key words.
- All papers should identify all authors and provide their contact information such as phone numbers, full postal addresses, email addresses, affiliations and so on.
- Authors should ensure that they have written entirely original works, and should not publish manuscripts describing essentially the same research in more than one journal.
- Honorarium (USD 2,000 or KRW 2,000,000) will be paid when papers are accepted for publication.
- All manuscripts must be submitted to the managing editor at ijcj@kic.re.kr.

AREAS

International Journal of Criminal Justice (IJCJ) invites papers from many different realms of criminology and criminal justice at both regional and global levels. Any issues related to criminology and criminal justice will be welcomed such as:

Community Sanction, Corrections, Corruption & White Collar Crime, Crime Prevention & Protection, Crime Trends, Crime & Deviance, Criminal Investigation, Criminal Law & Policy, Criminal Procedure, Cybercrime, Drug, Terrorism & Organized Crime, Economic & Corporate Crime, Information, Technology & Forensic Science, Juvenile Delinquency, Juvenile Justice, Penology, Police & Policing, Violent Crime.

International Journal of Criminal Justice

KIC Korean Institute of Criminology

09
9 772713 515003
ISSN 2713-5152