SOCIETY REGISTER

*Original Article*

# Quantitatively examining the interaction between cybercrime and physical crime

SOCIETY REGISTER
2023 / 7(3): 7–20
ISSN: 2544–5502
DOI: 10.14746/sr.2023.7.3.01

OPEN ACCESS

**Daniel Adrian Doss[1] & Daniel Scherr[2]**

[1] University of Tennessee, 433 W Madison St, Pulaski, TN 38478, Pulaski, USA. ORCID: 0000-0002-3393-0488, Email: ddoss8@tennessee.edu

[2] University of Tennessee, 433 W Madison St, Pulaski, TN 38478, Pulaski, USA. ORCID: 0000-0003-1222-5779, Email: dscherr@tennessee.edu

ABSTRACT: This study examined the differences and relationships between reported incidents of cybercrime and physical crime within U.S. society nationally. The examined period encompassed the years between 2001 and 2020. The study outcomes showed that a relationship existed between reported incidents of cybercrime and reported incidents of physical crime ($p = 0.00$; $\alpha = 0.05$). More specifically, it appeared that relationships existed between the reported incidents of cybercrime and the reported incidents of physical crimes representing robbery rate ($p = 0.01$; $\alpha = 0.05$), burglary rate ($p = 0.00$; $\alpha = 0.05$), and larceny theft rate ($p = 0.00$; $\alpha = 0.05$). It also appeared that a difference ($p = 0.00$; $\alpha = 0.05$) existed between reported incidents of cybercrime and physical crime wherein greater quantities of physical crime were exhibited societally during the examined period.

KEYWORDS: crime and criminology, cybercrime, cybersecurity, cyberspace, sociology

## INTRODUCTION

Within a society, crime was defined through its relevant legislative processes and the expressing and codifying of the resulting legislative content whereby the corresponding law was made enforceable by appropriate government authority (Leider, 2021). From a foundational perspective, cybercrime adhered to an analogous definition, and it consisted of the illegal transactions that occurred in cyberspace

(Doss, et al., 2022). Cybercrime, like terrorism, lacked a universal definition, but instead retained basic characteristics across its various perspectives (Curtis & Oxburgh, 2022). The U.S. federal government's perspective and definition of cybercrime varied depending on the focus of the agency (Bryant & Bryant, 2022).

Cyberspace is an intangible entity that affects tangible reality (Brenner, 2009). It is the nebulous, intangible, borderless, and dynamic reality generated by the various connections, uses, and interactions of technological devices (Doss, et al., 2022). Myriads of transactions occur continuously in cyberspace to satisfy some human needs and wants, either legally or illegally (Oosterman & Yates, 2022). Vojinovic (2022) indicated that 59% of polled Americans reported they had experienced cybercrime or were victimized by a hacker; 70% of small businesses were completely unprepared for cyberattacks; and that cybercrime damages were about $6 trillion in 2022. Cveticanin (2023) indicated that by 2027, society will expend about $10 billion annually on cybersecurity.

The Federal Bureau of Investigation (FBI) served as the principal investigate agency for cybercrimes and intrusions in the United States (Pesch-Cronin & Marion, 2016). The main, federal effort was facilitated by the National Cyber Investigative Joint Task Force (NCIJF), consisting about three dozen law enforcement and intelligence agencies (McElreath, et al., 2021). This effort complemented other partnerships with government agencies, private sector partners, foreign partners, and academia to identify and close gaps in networks worldwide (McElreath, et al., 2021). The FBI also operated the Internet Crime Complaint Center (IC3), which collected reports of cybercrime from the public for investigation and action (Federal Bureau of Investigation, n.d.).

Discussions about crime rates, victimization, trends, and threats were prevalent across media platforms, both traditional and social (Waldron, et al., 2009). Over the last several decades, however, the crime discussion increasingly incorporated cybercrime alongside physical or traditional crimes to the point where some organizations became more concerned with cybercrime than physical crime (Kshetri, 2010). This notion mirrored the emergence and expansion of the use of connected devices and individuals using the Internet (Ilbiz & Kaunert, 2023). According to the International Telecommunications Union (ITU), 91% of the United States and 59% of the world connected to the Internet (ITU, 2022). The prevalence of connected devices grew exponentially since their introduction in the 1970s from approximately 16 million in 1995 to almost 5.5 billion in 2022 (Internet World Stats, 2022).

The concept of a universally interconnected world was neither new nor particularly novel. Decades ago, visions ensued of the world transforming into a 'Global Village' and connection based on the rise of mass media in the 1960s (Dixon, 2009). Going further back, Nikola Tesla, outlined his vision for an interconnected populace and the positive benefits of wireless energy and connection for humanity during an interview with *Colliers* in 1926 (Kennedy, 1926). While the concepts of an interconnected world are not new, many of the types and varieties of modern cybercrime may have been unimaginable in the days of Tesla or the envisioning of a global village. As the Internet emerged and proliferated, physical crime was often mimicked or complemented within cyberspace whereby a straightforward question became relevant: What was the

intersection between cybercrime and physical crime?

## MOTIVATION FOR CYBER MALFEASANCE

People may inadvertently facilitate opportunities for victimization. For instance, when traveling out of town, someone may openly post photographs via social media indicating their absence from a residence or office. Within the Internet, tools may be obtained for cracking passwords to email, social media, employment, or other accounts wherein criminals may obtain knowledge that facilitates some type of theft crime. Additionally, the theft of a cellular telephone may provide an array of information assets that would be opportunistic for criminals to access virtual bank accounts or to break into someone's home or office.

Tesla predicted and described the implementation of the cellular phone concept some five decades before its invention and unveiling in 1973 (Launiainen, 2018). Tesla's technological vision emphasized positive impacts of the connection and not how the technology could have been used harmfully (Launiainen, 2018). As users relied increasingly on their connected devices for their daily lives and were inattentive to security needs, the comfort and convenience of cellular devices provided a false sense of security for transactions and behaviors (Koch, 2007). The ability to connect to an open wireless network at a restaurant, hotel, or public space provided free access to the Internet without much reliance upon physical location. Users may have been unaware of the need for security on their devices or the risks they undertook by using access points to conduct banking transactions, log into work or other confidential systems, or otherwise open up their personal data to those that wished to use it for their own purposes (Rawat & Ghafoor, 2019).

Humans often placed themselves at risk for increased criminal offending through their activities, as proposed by Felson and Cohen (1980) in *Human Ecology and Crime: A Routine Activity Approach*. Felson and Cohen (1980) built upon Hawley's human ecological theory (1950) as it related to criminal activity and behaviors and developed a Routine Activities Theory (RAT). Felson and Cohen (1980) found, in part, the determining factors for whether criminal activity occurred in a given situation depended on three factors: a motivated perpetrator, a suitable target, and the presence (or lack of) guardianship. This particular theory did not attempt to explain the rationale or motivation behind criminal activity, but assumed a motivated individual prepared to commit the crime in a specific scenario. Without that type of individual, or either of the other two legs of the RAT, the situation decomposed and became incomplete, like a stool missing a leg. The target was a human or an object, and the object needed to have value in the eyes of the perpetrator thereby leaving victims potentially blind to dangers. The issue of guardianship (or lack thereof) centered on whether controls or protections existed that could either prevent the successful completion of a criminal act or make the perpetrator question the outcomes. Guardianship took the form of law enforcement presence, cameras, others in the area that may intervene, or actions and preventative measures taken by the target to mitigate risks. The target had several specific characteristics critical to this calculus, including value, visibility, access, and

inertia (Felson & Cohen, 1980).

While the RAT dealt with criminal activities in the physical world, it was applicable in cyberspace (Bossler & Holt, 2007; Choi, 2008; Holt & Bossler, 2009; Kigerl, 2021; Leukfeldt & Yar, 2016). Just as individuals became comfortable with routines and familiarity in the physical world, the same behavior also occurred in the virtual world. Cyberspace exhibited activities and behaviors that paralleled their counterparts in the physical world, including crime. As the world became more interconnected, individuals spent more time in the virtual realm, created virtual presences, and interacted increasingly in cyberspace—so did criminals. Society became comfortable with and reliant upon technology to complete daily tasks and attributed ease and efficiency with safety and security. The lack of understanding of what information was contained online (big data, metadata, cookies and browsing history, connections and information shared by friends from private profiles, and so on) limited user ability to understand their exposure and vulnerability online. In the physical world, the requirements for the three major elements to exist in the same location limited exposure and vulnerability. In the virtual world, however, information and exposure were constantly available, opening users up to attacks and losses continually. The same lack of understanding provided challenges for users to also understand guardianship and access needs as well as how to meet their requirements.

## CYBERSPACE AND THE INFLUENCING OF PHYSICAL REALITY

The rapid expansion of cyberspace and the increasing and extensive use of the Internet by individuals, businesses, and government agencies influenced not only actions and behaviors in the virtual realm, but life in the physical world. The effect of change ushered by the proliferation and use of cyberspace pervaded societies globally. Everyday activities traditionally handled face-to-face, such as banking, shopping, reading the newspaper, interacting with family and friends, and many others, became activities that many performed online. Print media decreased dramatically and forced the closure of various newspapers and magazines or caused them to adapt and move content online. Industries also adjusted to new behaviors and attitudes or risked being left behind thereby altering the dynamics of the economy and daily life.

The emerging of the Internet of Things (IoT) also further integrated the physical world with cyberspace. Through the IoT, many everyday items in homes were connected to the Internet. It included not only electronics traditionally associated with connection, such as phones, watches, security systems, and televisions, but also a host of others, including refrigerators, coffee makers, toasters, and dishwashers (Levin, 2013). Some of these smart devices required tangible user action or manipulation, while others users were controlled intangibly by speech (Naik & Patel, 2023). The track record for security in the IoT was uneven, at best. Security was an afterthought for IoT devices, and resulted in a number of high-profile attacks and breaches (Klosowski, 2020). With devices tracking or able to access personal data and monitoring the environment with audio, visual, or both, there was significant opportunity for victimization (De Cremer, Nguyen, & Simkin, 2017).

History showed the potential of intangible software to cause harm in physical reality for intentional purposes. For instance, an early use of malware to cause some type of physical damage was demonstrated in 1982 when President Ronald Reagan approved a Central Intelligence Agency (CIA) operation for sabotaging the Soviet Union's economy via clandestine technology transfers that rigged software to destroy a natural gas pipeline in Siberia (Hoffman, 2004). The use of malware was strongly demonstrated during the Stuxnet attack in 2010 with the attack on and destruction of an Iranian nuclear facility wherein the world realized the destructive power of cyberspace (Collins & McCombie, 2012). In the ensuing years, a variety of actions in cyberspace yielded physical consequences. These included attacks that shut down or impeded local governments (Nir, 2022), school systems (Reed, 2023), and infrastructure (Sanger, Krauss, & Perlroth, 2021) thereby impacting the daily lives of many within society.

As the world integrated and cyber components were incorporated into daily life, both citizen and criminal behaviors changed. There were certain crimes that did not translate exactly to the cyber realm. Murder, burglary, and some other crimes required some manner of physical interaction, but may have been supplemented with cyber means (e.g., communication, surveillance of a target, and so on). Many other crimes had opportunities for commission online, but the nature of the crime and enforcement varied significantly. In cases of fraud or theft, the fundamental goal of cybercrime was the same as physical crime: to acquire something of value belonging to another (Department of Justice, n.d.). The form and function of cybercrime varied depending on the offense, but the end result was the same—financial gain for the offender (Department of Justice, n.d.). These types of crimes included not only financial theft, but also non-delivery or nonpayment incidents, espionage, romance schemes, intellectual property theft, and ransomware (Back, 2019).

The rapid adoption of e-commerce reduced foot traffic in traditional retail, forcing criminals to adapt to find their targets. Many businesses and agencies embraced ecommerce and web-based applications in the years leading up to the COVID-19 pandemic, but repeated lockdowns and impacts of the pandemic accelerated the move to electronic commerce from more traditional retail outlets thereby increasing online sales (Whalley, Stocker, & Lehr, 2023). According to the U.S. Census Bureau, e-commerce surged 30.3% overall from 2019 to 2020, with a 35.2% increase in electronic shopping and mail orders to $888.5 billion (U.S. Census, 2022a). From a high of almost 17% of the total retail sales during the pandemic, e-commerce represented almost 15% of the total retail sales in the United States (U.S. Census Bureau, 2022b). The increase in retail sales led to increased crime and victimization online, including $337 million in non-payment or non-delivery scams and $173 million in credit card fraud reported to the IC3 in 2021 (FBI, 2022).

## DESIGN AND METHODOLOGY

This study examined the relationship and difference between reported incidents of cybercrime and the reported incidents of physical crime for the period spanning the years between 2001 and 2020. This research examined the following questions: What

was the relationship between annually reported physical crime events versus annually reported cybercrime events? What was the relationship between reported physical crime events of murder and nonnegligent manslaughter; robbery; aggravated assault; burglary; larceny theft; and motor vehicle theft versus reported cybercrime events? What was the difference between annually reported physical crime events versus annually reported cybercrime events? The corresponding hypotheses were stated as follows:

$H_{01}$: No statistically significant relationship existed between annually reported aggregated physical crime event quantities versus annually reported cybercrime incident quantities.

$H_{02}$: No statistically significant relationship existed between annually reported physical crime quantities of murder and nonnegligent manslaughter; robbery; aggravated assault; burglary; larceny theft; and motor vehicle theft and annually reported cybercrime incident quantities.

$H_{03}$: No statistically significant difference existed between annually reported aggregated physical crime incident quantities versus annually reported cybercrime event quantities.

The first and second hypotheses used regression as the mathematical tool for data analysis to examine aggregated, cumulative values of reported cybercrime incidents versus reported values of physical crime incidents. Using the p-value approach, the regression testing of both hypotheses incorporated an alpha value of 0.05 ($\alpha = 0.05$).

The third hypothesis examined differences between the reported incidents of cybercrime and physical crime. Using ANOVA and an alpha value of 0.05 ($\alpha = 0.05$; $p < 0.05$), the third hypothesis considered whether a statistically significant difference existed between the reported incidents of cybercrime and physical crime. The Omega-Squared method was used to show effect size corresponding to statistical significance. An analysis of the means was used to determine size differences between the reported incidents of cybercrime and physical crime throughout the examined period.

The data sets for the study were obtained from the Federal Bureau of Investigation (FBI). Specifically, the FBI data sources were the Uniform Crime Reports (UCR) and the annual cybercrime reports published by the Internet Crime Complaint Center (IC3). The UCR data consisted of annually reported incidents reflecting the aggregated physical crime quantities of murder and nonnegligent manslaughter; robbery; aggravated assault; burglary; larceny theft; and motor vehicle theft. A redefining of sex crimes occurred during 2013. Therefore, sex crimes were excluded from this study because crimes reported after 2013 did not correspond to incidents reported beforehand in terms of fundamental definition. The definitions of murder and nonnegligent manslaughter; robbery; aggravated assault; burglary; larceny theft; and motor vehicle theft were unchanged and static throughout the period examined within this study. Although the IC3 data contained annually aggregated quantities of reported cybercrime incidents, no delineation of any specific cybercrime type (e.g., phishing, theft, and so on) was indicated in the data. Therefore, only the aggregated incidents of re-

ported cybercrime were used within the study.

Contrasting and comparing the examined incident quantities of cybercrime and physical crime necessitated the use of a ratio basis for analysis to ensure the presence of a common unit of measurement. Specifically, each annually aggregated value for both cybercrime and physical crime was converted to a ratio that reflected the quantity of reported incidents per 100,000 national population. Doing so provided a congruent basis for analyzing reported incidents with respect to population fluctuations over time. The annual United States national population data were obtained from World Bank data sets.

## FINDINGS

### Data Demographics

Performing the mathematics of regression and ANOVA necessitated the use of a common unit of measurement between the data sets representing cybercrime and physical crime. Table 1 shows the generated annual incidents of cybercrime representing a per 100,000 population value for the years spanning 2001 through 2020.

| Year | Cybercrime Complaints Filed | National Population | Cybercrime Incidents per 100,000 Individuals |
|---|---|---|---|
| 2001 | 49,711 | 284,968,955 | 17.44 |
| 2002 | 75,063 | 287,625,193 | 26.10 |
| 2003 | 124,509 | 290,107,933 | 42.92 |
| 2004 | 207,449 | 292,805,298 | 70.85 |
| 2005 | 231,493 | 295,516,599 | 78.33 |
| 2006 | 207,492 | 298,379,912 | 69.54 |
| 2007 | 206,884 | 301,231,207 | 68.68 |
| 2008 | 275,284 | 304,093,966 | 90.53 |
| 2009 | 336,655 | 306,771,529 | 109.74 |
| 2010 | 303,809 | 309,327,143 | 98.22 |
| 2011 | 314,246 | 311,583,481 | 100.85 |
| 2012 | 289,874 | 313,877,662 | 92.35 |
| 2013 | 262,813 | 316,059,947 | 83.15 |
| 2014 | 269,422 | 318,386,329 | 84.62 |
| 2015 | 288,012 | 320,738,994 | 89.80 |
| 2016 | 298,728 | 323,071,755 | 92.46 |
| 2017 | 301,580 | 325,122,128 | 92.76 |
| 2018 | 351,937 | 326,838,199 | 107.68 |
| 2019 | 467,361 | 328,329,953 | 142.34 |
| 2020 | 791,790 | 331,501,080 | 238.85 |

Table 1. Cybercrime Data Set
Source: own elaboration

The expression of physical crime incidents also necessitated the use of a per 100,000 population ratio to facilitate mathematical analysis. Obtained from the FBI Uniform

Crime Report data sets, using the per 100,000 population values, Table 2 shows the physical crime data for the period spanning the years between 2001 and 2020.

| Year | Murder and nonnegligent manslaughter rate | Robbery rate | Aggravated assault rate | Burglary rate | Larceny-theft rate | Motor vehicle theft rate |
|---|---|---|---|---|---|---|
| 2001 | 5.60 | 148.50 | 318.60 | 741.80 | 2,485.70 | 430.50 |
| 2002 | 5.60 | 146.10 | 309.50 | 747.00 | 2,450.70 | 432.90 |
| 2003 | 5.70 | 142.50 | 295.40 | 741.00 | 2,416.50 | 433.70 |
| 2004 | 5.50 | 136.70 | 288.60 | 730.30 | 2,362.30 | 421.50 |
| 2005 | 5.60 | 140.80 | 290.80 | 726.90 | 2,287.80 | 416.80 |
| 2006 | 5.80 | 150.00 | 292.00 | 733.10 | 2,213.20 | 400.20 |
| 2007 | 5.70 | 148.30 | 287.20 | 726.10 | 2,185.40 | 364.90 |
| 2008 | 5.40 | 145.90 | 277.50 | 733.00 | 2,166.10 | 315.40 |
| 2009 | 5.00 | 133.10 | 264.70 | 717.70 | 2,064.50 | 259.20 |
| 2010 | 4.80 | 119.30 | 252.80 | 701.00 | 2,005.80 | 239.10 |
| 2011 | 4.70 | 113.90 | 241.50 | 701.30 | 1,974.10 | 230.00 |
| 2012 | 4.70 | 113.10 | 242.80 | 672.20 | 1,965.40 | 230.40 |
| 2013 | 4.50 | 109.00 | 229.60 | 610.50 | 1,901.90 | 221.30 |
| 2014 | 4.50 | 101.30 | 229.20 | 537.20 | 1,821.50 | 215.40 |
| 2015 | 4.90 | 102.20 | 238.10 | 494.70 | 1,783.60 | 222.20 |
| 2016 | 5.40 | 102.90 | 248.30 | 468.90 | 1,745.40 | 237.30 |
| 2017 | 5.30 | 98.60 | 249.20 | 429.70 | 1,695.50 | 237.70 |
| 2018 | 5.00 | 86.10 | 248.20 | 378.00 | 1,601.60 | 230.20 |
| 2019 | 5.10 | 81.80 | 250.40 | 340.50 | 1,569.20 | 220.80 |
| 2020 | 6.50 | 73.90 | 279.70 | 314.20 | 1,398.00 | 246.00 |

Table 2. Physical Crime Data Set
Source: own elaboration

Measures of central tendency and dispersion were used to examine the demographic characteristics of the data sets representing both cybercrime and physical crime. Table 3 shows the characteristics of cybercrime whereas Table 4 shows the characteristics of physical crime.

| Category | Cybercrime Complaints Filed | National Population | Cybercrime Incidents per 100,000 Individuals |
|---|---|---|---|
| Mean | 237,824.94 | 305,862,825.35 | 76.96 |
| Median | 269,422.00 | 306,771,529.00 | 84.62 |
| S.D. | 84,242.28 | 12,831,792.60 | 25.89 |
| Var | 7.10E+09 | 1.65E+14 | 670.06 |

Table 3. Cybercrime: Central Tendency and Dispersion
Source: own elaboration

| Category | Murder and nonnegligent manslaughter rate | Robbery rate | Aggravated assault rate | Burglary rate | Larceny-theft rate | Motor vehicle theft rate |
|---|---|---|---|---|---|---|
| Mean | 5.27 | 119.70 | 266.71 | 612.26 | 2,004.71 | 300.28 |
| Median | 5.35 | 116.60 | 258.75 | 701.15 | 1,989.95 | 242.55 |
| S.D. | 0.510186 | 24.71907 | 27.15682 | 152.5481 | 315.5783 | 89.40008 |
| Var | 0.260289 | 611.0326 | 737.4931 | 23270.91 | 99589.66 | 7992.374 |

Table 4. Physical Crime Tendency and Dispersion
Source: own elaboration

## Findings of the First Hypothesis

The first hypothesis, $H_{01}$, examined whether a statistically significant relationship existed between annually reported aggregated physical crime incident quantities versus annually reported aggregated cybercrime event quantities. The regression outcome showed that physical crime explained 29.99% of the variation in cybercrime [$R^2 = 0.59$; ($F(1,18) = 26.18$, $p = 0.00$)]. These results were significant at the $p < 0.05$ level.

## Findings of the Second Hypothesis

The second hypothesis, $H_{02}$, examined whether a statistically significant relationship existed between annually reported physical crimes quantities of murder and nonnegligent manslaughter; robbery; aggravated assault; burglary; larceny theft; and motor vehicle theft versus annually reported cybercrimes. The hypothesis testing outcome revealed a statistically significant relationship [$R^2 = 0.92$; ($F(6,13) = 25.77$, $p < 0.05$)] existed between the reported incidents of robbery rate ($\beta = -1.7$; $p = 0.01$; $\alpha = 0.05$), burglary rate ($\beta = 0.52$; $p = 0.00$; $\alpha = 0.05$), and larceny theft rate ($\beta = -0.31$; $p = 0.00$; $\alpha = 0.05$) and the examined quantities of cybercrime thereby rejecting the null hypothesis.

## Findings of the Third Hypothesis

The third hypothesis, $H_{03}$, examined whether a statistically significant difference existed between annually reported aggregated cybercrime incident quantities versus annually reported physical crime event quantities. The hypothesis testing outcome revealed a statistically significant difference ($p = 0.00$; $\alpha = 0.05$; $\omega^2 = 0.94$) between annually reported aggregated cybercrime incident quantities versus annually reported physical crime event quantities thereby rejecting the null hypothesis. Comparing the means between the reported incidents of cybercrime ($M = 89.86$) and physical crime ($M = 3{,}308.91$) showed a greater prevalence of physical crime throughout the examined period.

## CONCLUSIONS, IMPLICATIONS, AND RECOMMENDATIONS

The study explored two decades of national crime data spanning period between 2001 and 2020. The study outcomes showed that a relationship existed between reported incidents of cybercrime and reported incidents of physical crime. More specifically, it appeared that relationships existed between the reported incidents of cybercrime and the reported incidents of physical crimes representing robbery, burglary, and larceny theft. All three categories represented some type of property crime within the context of theft. Essentially, all three types of crime involved someone taking something from another without permission to satisfy some intended purpose. Certainly, real and personal properties exist in tangible reality, and not cyberspace. However, given the findings, it may be that criminals may have used some form of electronic device or system to facilitate some aspects of crime in physical reality.

It also appeared that a difference existed between reported incidents of cybercrime and physical crime wherein greater quantities of physical crime were exhibited societally during the examined period. In other words, it appeared that cybercrime rates had neither met nor surpassed physical crime rates societally. The fact cybercrime did not meet or exceed physical crimes during the chosen time is instructive, but the data collected for the study provides additional details and projections looking forward. Looking at the data collected, with respect to events per 100,000 population, the rate of physical crime dwarfed cybercrime at the beginning of the data set, with rates for robbery (148.5), aggravated assault (318.6), and larceny theft (2,485.7) versus cybercrime (17.62). Respectively, at the end of the examined period, the same categories were robbery (73.9), aggravated assault (279.7), and larceny theft (1,398) versus cybercrime (241.16). It appeared that crime moved into cyberspace.

The FBI data contained in the study was aggregated from law enforcement agencies nationally using similar definitions of crime and with structured reporting. The cybercrime numbers reported herein derived from citizen reports of crimes based on personal experience and understanding, with potentially limited knowledge of how or where to report cybercrimes. The dark figure of crime, that volume of criminal activity between the amount reported or captured and that conducted, was a limiting factor in this analysis. However, the data showed a significant increase in the volume of reported cybercrime, especially during the two years of the Covid pandemic (2019-2020) provided in the study. It was unclear whether the increase in incidents was because of greater commission of crimes, better reporting, pandemic effect, or some combination thereof.

Without a clear process to report and capture cybercrime across the country, the true nature of the maturing cybercrime problem remains ambiguous. As additional data emerges, trends can be identified and monitored, but how significant the problem is, how to address it, and the necessary prioritization will remain guesswork, at best, for now. The reporting structure and methodology for cybercrime should be evaluated, along with taking a detailed look at the rates for the different types of cybercrime, and how this information is collected or used at the different levels of government.

One of the largest questions coming out of this study was how well known and uti-

lized was the IC3 reporting tool. The IC3 captured increasingly more cybercrime data over the 20 years included in the study, but there was not another measure to corroborate the numbers support the data. The reliance on the public to report these crimes, often without interaction with law enforcement, represented a potential gap in the reporting. A national standard or recommendation for how and when to report cybercrime, along with increased communication to the public, could improve the capture of data. Working with stakeholders at the different levels of government to create a system to at least capture the reports and data from local law enforcement to and through the federal level for cybercrime could also be beneficial. This could also tie in with additional investigation on types and rates of cybercrime at state and regional levels, which could help drive efforts in those locations.

Although this study examined a variety of property crimes, it did not address crimes of passion. In other words, it lacked any examination of sex crimes. Future studies may examine the relationship and differences between reported incidents of cybercrime and physical crimes of passion. Future studies may examine recidivism within the context of cybercrime. At the time of this authorship, in general, U.S. society exhibited about a 75% recidivism rate (Beeler, 2022). Although such a recidivism rate reflected physical crime incidents historically, virtual crime was a relatively new phenomenon in contemporary times. Interestingly, this study incorporated two decades of cybercrime data. McElreath, et al., (2022) indicated that about two decades of observations were necessary for examining events from the perspectives of policy analysis and historical contexts. Given such notions, from such perspectives, future studies may examine sentencing policy and recidivism contexts of cybercrime.

**FUNDING:** This research received no external funding.

**CONFLICT OF INTEREST:** The authors declare no conflict of interest.

**ACKNOWLEDGEMENTS:** We would like to thank Almighty God for the research opportunity. Also, thanks to the University of Tennessee system for the necessary research resources and the data sources for their respective uses of open data sets.

## REFERENCES

Back, S. (2019). *The cybercrime triangle: An empirical assessment of offender, victim, and place*. Miami, FL: Florida International University.

Beeler, A. (2022). Inmate seminaries: How they have positively impacted corrections. *Corrections Today, 2022*, 34-42.

Brenner, S. (2009). *Cyberthreats: The emerging fault lines of the nation state*. New York, NY: Oxford University Press.

Bryant, R. & Bryant, S. (2014). *Policing digital crime*. New York, NY: Routledge.

Bossler, A. M., & Holt, T. J. (2007, November 14). *Examining the utility of routine activities theory for cybercrime.* Paper presented at the annual meeting of the American

Society of Criminology, Atlanta Marriott.
Choi, K. S. (2008). Computer crime victimization and integrated theory: An empirical assessment. *International Journal of Cyber Criminology, 2*, 308-333.
Collins, S. & McCombie, S. (2012). Stuxnet: The emergence of a new cyber weapon and its implications. *Journal of Policing, Intelligence, and Counter Terrorism 7*(1), 80-91.
Computer Fraud and Abuse Act of 1986, 100 Stat. 1213.
Curtis, J. & Oxburgh, G. (2022). Understanding cybercrime in 'real world' policing and law enforcement. *The Police Journal: Theory, Practice, and Principles, 0*(0). https://doi.org/10.1177/0032258X221107584
Cveticanin, N. (2023). *Hacking statistics to give you nightmares*. Retrieved from https://dataprot.net/statistics/hacking-statistics/
Cybersecurity and Infrastructure Security Agency. (2018). *Combating Cyber Crime*. Retrieved from https://www.cisa.gov/combating-cyber-crime
De Cremer, D., Nguyen, B., & Simkin, L. (2017). The integrity challenge of the Internet-of-Things (IoT): On understanding its dark side. *Journal of Marketing Management, 33,* 1-2.
De Padirac, B. (2018). *International dimensions of cyberspace law*. New York, NY: Routledge.
Department of Justice. (n.d.). *Computer crime and intellectual property section (CCIPS)*. Retrieved from: https://www.justice.gov/criminal-ccips
Department of Justice. (n.d.). *Prosecuting computer crimes*. Retrieved from https://www.justice.gov/criminal/file/442156/download
Dixon, V.K. (2009). Understanding the implications of a global village. *Inquiries, 1*(11), 1-2.
Doss, D.A., Etter, G., Rials, W., McElreath, D., Gokaraju, B., & Standish, H. (2022). Examining the effects of the Federal Information Sharing Modernization Act of 2014 and the Cybersecurity Information Sharing Act of 2015: What were the impacts toward reducing cybercrime incidents. *Journal of Gang Research, 29*(3), 1-23.
Encyclopedia Britannica. (n.d.) *Cybercrime*. Retrieved from https://www.britannica.com/topic/cybercrime
European Union Agency for Law Enforcement Cooperation. (2021). *Internet Organised Crime Threat Assessment 2021*. Retrieved from https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf
Federal Bureau of Investigation. (n.d.). *What We Investigate: Cyber*. Retrieved from https://www.fbi.gov/investigate/cyber
Federal Bureau of Investigation. (2022). *Internet Crime Report: 2021*. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
Felson, M. & Cohen, L. (1980). Human ecology and crime: A routine activity approach. *Human Ecology, 8*(4), 389-406.
Henderson, H. (2014). *A to Z of computer scientists*. New York, NY: Facts on File.
Hoffman, D.E. (2004). *CIA slipped bugs to Soviets*. Retrieved from https://www.nbc-

news.com/id/wbna4394002
Holt, T. J. & Bossler, A. M. (2009). Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. *Deviant Behavior, 30*, 1-25.
Ilbiz, E. & Kaunert, C. (2023). *The sharing economy for tackling cybercrime*. New York, NY: Springer.
International Telecommunications Union (2022). *ITU Datahub: Individuals using the Internet*. Retrieved from https://datahub.itu.int/data/?e=USA&c=701&i=11624
Internet World Stats. (2022). *Internet Growth Statistics*: *Today's road to e-Commerce and Global Trade*. Retrieved from https://www.internetworldstats.com/emarketing.htm
Kennedy, J. (1926, January 30). *An Interview with Nikola Tesla*. Collier's Magazine.
Kigerl, A. (2021). Routine activity theory and malware, fraud, and spam at the national level. *Crime Law and Social Change, 76*(4).
Koch, C. (2007). You plan to fight cyber crime. *CIO, 2007*, 34-40.
Kritzinger, E. & Von Solms, S. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security, 29*(8), 840-847.
Kshetri, N. (2010). *The global cybercrime industry*. New York, NY: Springer.
Klosowski, T. (2021). *We asked appliance manufacturers how long they'll keep connected devices secure. Many couldn't tell us*. Retrieved from https://www.nytimes.com/wirecutter/blog/how-long-connected-devices-secure/
Launiainen, P. (2018). *A brief history of everything wireless: How invisible waves have changed the world*. Cham, Switzerland: Springer.
Leider, R. (2021). The modern common law of crime. *Journal of Criminal Law and Criminology, 111*(2), 407-499.
Leukfeldt, E. & Yar, M. (2016) Applying Routine Activity Theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263-280.
Levin, A. (2013). *9 Household Products That May Be Spying on You: Could you coffee machine be spying on you?* Retrieved from https://abcnews.go.com/Business/household-products-spying/story?id=19974898
McElreath, D., DioGuardi, S., & Doss, D. (2022). Pre-crime prediction: Does it have value? Is it inherently racist? *International Journal of Service Science, Management, Engineering, and Technology, 13*(1), 1-17.
McElreath, D., Doss, D., Russo, B., Etter, G., Van Slyke, J., Skinner, J., Corey, M., Jensen, C., Wigginton, M., & Nations, R. (2021). *Introduction homeland security*. (3rd ed.). Boca Raton, FL: CRC Press.
Naik, K. & Patel, S. (2023). An open source smart home management system based on IOT. *Wireless Networks, 29*, 989-995.
Nir, S. (2022). *How a cyberattack plunged a long island county into the 1990s*. Retrieved from https://www.nytimes.com/2022/11/28/nyregion/suffolk-county-cyber-attack.html
Office of the Attorney General. (2014). *Intake and Charging Policy for Computer Crime Matters*. Retrieved from https://www.justice.gov/criminal-ccips/file/904941/download

Oosterman, N. & Yates D. (2021). *Crime and art sociological and criminological perspectives of crimes in the art world*. Cham, Switzerland: Springer.

Pesch-Cronin, K. & Marion, N. (2016). *Critical infrastructure protection, risk management, and resilience: A policy perspective*. Boca Raton, FL: CRC Press.

Rawat, D. & Ghafoor, K. (2019). *Smart cities cybersecurity and privacy*. Cambridge, MA: Elsevier.

Reed, J. (2032). *More school closings coast-to-coast due to ransomware*. Retrieved from https://securityintelligence.com/news/schools-closing-due-to-ransomware/

Sanger, D., Krauss, C., & Perlroth, N. (2021). *Cyberattack Forces a Shutdown of a Top U.S. Pipeline*. Retrieved from https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html

United States Census Bureau. (2022a). *E-Commerce Sales Surged During the Pandemic*. Retrieved from https://www.census.gov/library/stories/2022/04/ecommerce-sales-surged-during-pandemic.html

United States Census Bureau. (2022b). *Quarterly Retail E-Commerce Sales: 3d Quarter 2022*. Retrieved from https://www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf

Waldron, R., Quarles, C., McElreath, D., Walron, M., & Milstein, D. (2009). *The criminal justice system*. (5th ed.). Tulsa, OK: K&M Publishers.

Whalley, J., Stocker, V., & Lehr, W. (2023). *Beyond the pandemic*. Bingley, UK: Emerald Publishing.

World Bank. (2022). *Databank: Population estimates and projections*. Retrieved from:https://databank.worldbank.org/source/population-estimates-and-projections

Visger, M. (2022). *The international law sovereignty debate and development of international norms on peacetime cyber operations*. Retrieved from https://www.lawfareblog.com/international-law-sovereignty-debate-and-development-international-norms-peacetime-cyber-operations

Vojinovic, I. (2022). *More than 70 cybercrime statistics—A $6 trillion problem*. Retrieved from https://dataprot.net/statistics/cybercrime-statistics/

**BIOGRAPHICAL NOTE**

Daniel Adrian Doss is associate professor of cybersecurity at the University of Tennessee—Southern.

Dan Scherr is assistant professor of criminal justice at the University of Tennessee—Southern.



ARTICLE HISTORY: Received 2023-07-15 / Accepted 2023-09-24