International Annals of Criminology (2022), **60**, 220–240
doi:10.1017/cri.2022.12

ARTICLE

The Value of Criminological Theories in Explaining Cybersecurity in South African Smart Cities

François Paul Cornelius, Shandré Kim Jansen van Rensburg and Sarika Kader*

Department of Criminology and Security Science, University of South Africa, Tshwane, South Africa
*Corresponding Author: Sarika Kader, Department of Criminology and Security Science, University of South Africa, Tshwane, South Africa. E-mail: sewpes@unisa.ac.za

(Submitted 18 May 2022; revised 28 June 2022; accepted 20 July 2022; first published online 26 August 2022)

Abstract
The development of smart cities in South Africa has the potential to enrich quality of life, encourage economic growth and reduce the human ecological footprint. It can advance and elevate service delivery in urban areas by applying various information and communication technologies. However, despite the countless benefits available, smart cities are at risk for major cybersecurity breaches that can produce devastating consequences. Criminological theories provide a foundation for understanding and explaining the criminal activity. Advancements in computer technologies and increased use of electronic devices and the Internet have resulted in crimes committed in cyberspace. As such, criminology scholars have been forced to think differently about how crimes are committed in cyberspace and how theoretical perspectives can be advanced to explain these non-traditional crimes. This article contends that criminological theories can inform cybersecurity risks in smart cities. This paper is based on theoretical findings through a qualitative inquiry, and the data were analysed thematically. The authors illustrate the value of social learning theory, neutralization theory, code of the street theory, space transition theory, actor-network theory and integrated model theory in explaining cybersecurity risks in smart cities.

Keywords cybercrime, criminological theories, smart cities, cybersecurity, cybersecurity risks

INTRODUCTION

Smart cities promise to vastly improve and optimize urban service delivery by applying various information and communication technologies (ICT) (Karvonen, Cugurullo, and Caprotti 2019). Furthermore, smart cities' key goals are to improve citizens' quality of life, promote economic growth and reduce the human ecological footprint through sustainability (Deloitte 2015). Regarding global population figures, 55% of the world's current population now lives in urban city areas, likely to grow to 68% by the year 2050 (United Nations 2018). In South Africa, the implementation of smart city initiatives has been limited to mere elements of a smart city, mainly installing smart electricity meters and limited smart city ICT projects (Foster 2020). However, plans for developing South Africa's first ground-up built new smart city in the region, titled "The Lanseria Airport City", are underway (BusinessTech 2020). The new smart city is also one of 19 "Mega City" projects, including constructing multiple mixed-use smart city developments in the province (Gauteng Department of Human Settlements 2018). Despite the various benefits of smart cities, cybersecurity risks remain significant and could have catastrophic implications (Barlow and Levy-Bencheton 2019).

Criminological theories form the basis of understanding and explaining the reasons behind why individuals commit a crime (Newburn 2017). From theories, a substantial amount of empirical research has been conducted to increase knowledge of the motivations and other factors behind the causation of crime (Akers, Sellers, and Jennings 2016). Moreover, the rise in popularity and usability of computer technology and the Internet has led to the growth of crimes such as online fraud, hacking and the distribution of malicious malware (Holt and Bossler 2017).

This newfound "cyberspace" influenced the ideological perspectives of criminologists and forced researchers to start deliberating on how much "cybercrime" diverged from traditional crime (Grabosky 2001; Wall 1998). Grabosky (2001) claimed that the fundamental motivations to commit a crime (financial gain, power) are relevant to traditional theories and that technology was now a new avenue to conduct a crime. Wall (1998) acknowledged that certain real-world crimes have direct comparisons to cybercrimes (online fraud) but argued that there are also certain cybercrimes (hacking, distribution of malicious malware) that traditional theories could not adequately support. Wall (1998) motivates this notation that cybercrimes depend on an individual's ability to gain knowledge on the function and exploitation of a specific computer or Internet technology. As a result, Jaishankar (2007a:2) conceptualized cybercriminology as "the study of causation of crimes that occur in cyberspace and its impact in the physical space". He argues that cybercriminology is a multidisciplinary field that includes researchers from various fields such as criminology, victimology, sociology, psychology and computer science.

This paper argues that criminological theories inform cybersecurity risks in smart cities. The theoretical underpinning of this article encompasses theories evolving from the positivist school of thought and taking on a subcultural perspective on cybercrimes. Additionally, this paper intends to showcase how selected criminological theories can be used to explain cybercrimes in smart cities. Subsequently, the paper contributes to the body of knowledge related to the theories (Crawford 2020).

Traditional theory, subcultural theory, new theoretical paradigms and an integrated model of multiple theoretical perspectives enlighten this paper. Therefore, the following theories are used to contextualize cybercrimes in smart cities:

- Social learning theory
- Neutralization theory
- Code of the street theory
- Space transition theory
- Actor-network theory (ANT)
- Integrated model theory

https://doi.org/10.1017/cri.2022.12 Published online by Cambridge University Press

OVERVIEW OF SMART CITIES

The concept of a smart city has been around for many years. Although adoption has been slow, the potential is evident in various city sectors (Allam 2021). Smart cities consist of highly sophisticated forms of technology and require the partnership of numerous local and international stakeholders (Ferreira 2021). In sum, a smart city is a complex "system of systems, of both traditional systems, such as critical infrastructure as well as new ones resulting from emerging technologies, such as virtualisation, sensor networks, and others". Furthermore, three fundamental elements driving smart city initiatives consist of physical, social and technological infrastructures (British Standards Institution 2014:3; International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) 2015:2).

Merely a decade ago, the concept of a smart city seemed like a utopian fantasy driven by unrealistic technological advancements. However, over the last few years, smart urbanization has formed a significant part of numerous urban projects in cities around the globe (Karvonen et al. 2019). The rise of the Internet of Things (IoT) technology has significantly enabled the development and feasibility of a smart city. IoT is, however, just one of the many technologies that are allowing the smart city concept to become a reality (Allam 2021). Other modern technologies, such as broadband Internet connections, artificial intelligence and ICT systems, have fundamentally changed how cities function and ultimately form the critical infrastructure of smart cities (Pelton and Singh 2018). Global population figures show that 55% of the world's current population now live in urban city areas, likely to grow to 68% by the year 2050 (United Nations 2018). The planet is therefore fast becoming urbanized. Digital social market studies indicate that the continuing trend of urbanization will have a significant impact on the socio-economic environment within cities (White and Marchet 2021).

Smart cities aim to improve citizens' quality of life and the efficiency of public services by optimizing the digital integration of the IoT and ICT systems with the current city infrastructure to create a fair and sustainable operational system (Akhuseyinoglu and Joshi 2020). Additionally, many smart IoT components, such as sensors, cameras and other related devices, are deployed throughout a smart city in places such as houses, roads and buildings. These technologies generate massive amounts of "big data" and allow cities to gain valuable insights into their operations (Lozada, Arias-Pérez, and Perdomo-Charry 2019). The use of ICT systems and IoT technologies enables the increased efficiency of energy grids, enhanced service delivery, and improved communications and transportation in smart cities (Ghosal and Halder 2018). Furthermore, smart cities have the potential to improve planning strategies, enhance economic development, reduce pollution, lower energy consumption and implement a faster, more efficient infrastructure. As a result, commuting time will be reduced due to better transportation systems and a decrease in traffic accidents (Pelton and Singh 2018). Moreover, smart cities will enhance the safety of citizens with the assistance of IoT-connected devices to identify, prevent and minimize the impact of security risks. The reporting of crimes and other security issues will be improved with the increased reliance on IoT-connected devices such as closed-circuit television (CCTV) video surveillance systems, mobile applications and interactive kiosks (Le-Dang and Le-Ngoc 2018).

https://doi.org/10.1017/cri.2022.12 Published online by Cambridge University Press

Cybersecurity in smart cities has become increasingly important as the new era of digitalization and hyper-connectivity has created a wide range of new cybersecurity risks. Cybersecurity risks may have a profound impact on the functionality and feasibility of smart cities (Pandey, Peasley, and Kelkar 2019). Cybersecurity risks refer to the level of exposure to harm within an organization that could result in a loss-occurring event due to a breach or attacks on the information system, technical infrastructure or technological devices (RSA Security 2019). Cyber-threats have been growing yearly, and recent trends in cybersecurity statistics reveal a considerable increase in cyberattacks targeting data and physical assets (World Economic Forum 2018).

CYBERCRIME AND ITS IMPACT ON CYBERSECURITY OF SMART CITIES

Major global smart city cybersecurity incidents include a global ransomware cyberattack that was distributed to 150 countries, encrypting over 300,000 computers resulting in an £92 million loss of income to the National Health Service of the United Kingdom (Woollaston-Webber 2017). Singapore experienced the country's worst-ever data breach when hackers stole the personal healthcare profiles of 1.5 million patients (Tham 2018). In terms of cyber-warfare, the critical infrastructure of Ukraine was attacked by Russian hackers, which resulted in massive power outages, leading to blackouts in regions of the country (Kovacs 2019). Recently, the largest fuel pipeline in the United States fell victim to a significant ransomware attack that forced the shutdown of operations for approximately one week, resulting in fuel panic-buying and countless fuel stations running out of supplies (Milman 2021).

It has become increasingly difficult to prevent cyberattacks such as ransomware, data breaches and cyberterrorism (Pelton and Singh 2018). As a result, smart cities have the potential to become lucrative targets for cybercriminals, cyberterrorists and hackers capable of crippling a city's operations through ransomware and other forms of cyberattacks (KPMG 2019).

In 2012, R42 million was stolen during a cyber-fraud incident at the South African Postbank. The cyber-fraud incident was carried out during the Christmas season when a Postbank employee fraudulently utilized the computer of a colleague who was on leave (Swart and Wa Africa 2012). In 2012, the "Red October" cyber-espionage campaign was first detected. The campaign is believed to be a Russian state-sponsored operation (FireEye 2014) that utilized malware to steal sensitive information from many governments and private organizations worldwide (Valeriano and Maness 2015). In South Africa, attackers sent an infected document via e-mail to numerous embassies, claiming to be from the Department of International Relations and Cooperation (ESET 2016).

Moreover, the South African Police Service (SAPS) fell victim to a data breach that exposed information related to approximately 16,000 whistle-blowers and victims. The cyberattack was politically motivated, as the hacking group "Anonymous" claimed that the data breach was in response to the killings of striking mineworkers at the Marikana mine by members of the SAPS (Roane 2013; Tubbs 2013). In July 2018, the hacktivist group "Black Team X" attacked

https://doi.org/10.1017/cri.2022.12 Published online by Cambridge University Press

and defaced the South African Presidency's website. The socio-politically motivated attack prevented access to the website (Sicetsha 2018) in response to South Africa's support of the independent state of Western Sahara, which Morocco claims to be a part of their country (Nxumalo 2018). In 2015, the adultery website Ashley Madison was hacked, and the personal information of 175,000 South African users was leaked online (Vermeulen 2015). The hackers claimed that the privacy breach was intended to expose companies' morally dubious business model and their users, and their attempts were aimed at shutting the website down (Lee 2015).

In October 2019, multiple South African banks were targeted by a distributed denial of service (DDoS) attack (Moyo 2019). The South African Banking Risk Information Centre confirmed the incidents and stated that the attacks were financially motivated and initiated by a ransom note delivered by e-mail to publicly available staff e-mail addresses (South African Banking Risk Information Centre 2019). Experian South Africa announced that it was investigating a major data breach that exposed the personal information of 24 million South Africans and 793,749 local businesses (South African Banking Risk Information Centre 2020). The data breach is believed to be financially motivated, as the data records are potentially worth millions of rands (Hosken 2020).

Furthermore, the COVID-19 pandemic has created increased risks for smart cities, businesses and individuals as they adapt to a revised operating model in the "new ordinary world" (Khan et al. 2021). Kaspersky (2020) reported that cyberattacks soared in 2020 as South Africans increased their reliance on the Internet due to factors caused by the COVID-19 pandemic. Thus, the "new normal" concerning the role of digital technologies will probably create lucrative ground for cybercriminals to carry out a variety of cyberattacks at the present time and beyond (Mimecast 2021).

GOAL OF THE STUDY

This article is based on a more extensive study conducted by the first author (Cornelius 2022). It accentuates the value of criminological theories to cybersecurity in smart cities. Thus, it is directed by the following research question: How can criminological theories inform cybersecurity in smart cities?

RESEARCH METHODOLOGY

Research Approach

The paper adopted a qualitative approach, contributing to a comprehensive and rich understanding of the phenomenon under study (Leavy 2017). The research study was exploratory as it examined a problem that had not been studied thoroughly (Patton 2015). Due to the novelty of the phenomenon, a phenomenological research strategy was used. Phenomenological research is exploratory, intending to understand people's perceptions, perspectives and experiences in a particular situation in the real world (Schurink, Schurink, and Fouché 2021). The paper uses a conceptual approach in its research design because it is problem-focused and meticulously unpacks the research question. Thus, this conceptual paper endeavours to link

https://doi.org/10.1017/cri.2022.12 Published online by Cambridge University Press

traditional and contemporary criminological theories in exciting ways. Consequently, it provides introspection across disciplines, proposes multilevel perceptions, and expands the reader's scope of thinking and reasoning regarding South African smart cities (Gilson and Goldberg 2015).

FINDINGS AND DISCUSSION

The paper's findings are premised on three main contributions: traditional, new, and integrated criminological theories that inform cybersecurity in smart cities.

Traditional Criminological Theories Value Cybersecurity in South African Smart Cities

Social Learning Theory

Within the positivist perspective, social learning theory has been proved over the last five decades to be one of the most popular theories utilized by criminologists. The theory, developed by Akers (1998), has been used in countless studies to describe various criminal activities. The origins of the theory date back to the 1960s. It is considered an extension of Sutherland's (1947) differential association theory. Sutherland (1947) argued that individuals gain an understanding of criminal behaviour through time spent with influential criminal groups. Akers (1998) expanded on that notion by arguing that the learning method of any behaviour, especially crime, includes the following four key components: (1) differential association; (2) favourable definitions; (3) differential reinforcement; and (4) imitation.

In terms of cybercrimes, the four key components can also be effectively used to explain the motives behind such criminal behaviour (Stalans and Donner 2018). Differential association refers to social exchanges with others who offer motives, reasoning and supportive attitudes to commit cybercrime. Favourable definitions of committing cybercrimes refer to an individual's attitude created from social interactions with deviant peers who support criminal behaviour (Akers 1998). Favourable attitudes refer to an individual's defiant mindset that the criminal act that they are committing is not immoral and not harmful to others. This reasoning allows individuals to feel that they are not accountable for the subsequent harm caused by their actions (Hinduja and Ingram 2008). Differential reinforcement refers to positive (rewards of cybercrimes) and negative reinforcements (being arrested by the authorities). Lastly, imitation/modelling refers to observing other individuals involved in criminal behaviour, including cybercrimes, and subsequently emulating such behaviour (Akers 1998). From a South African perspective, Akers' (1998) four key components can also be effectively used to explain the motives behind cybersecurity risks faced by South Africa's smart cities.

The differential association could refer to online social exchanges, reasoning and supportive attitudes that result in individuals committing cybercrime in South African smart cities. The use of social media in South Africa is on the rise and, every day, more people are socializing online. In 2019, there were approximately 22.89 million social network users in South Africa, projected to grow to 26.81 million in 2025 (Statista 2021). Many dedicated websites, website forums

https://doi.org/10.1017/cri.2022.12 Published online by Cambridge University Press

and social media groups support subculture groups, enabling them to share information and support the various forms of cybercrime deviance (Stalans and Donner 2018). Cybercrime activities in the form of cyberterrorism can be cultivated on websites and social media groups. These "virtual communities of hate" allow individuals to engage with others who may share similar beliefs and nefarious motives and, as such, support Akers' (1998) differential association component within social learning theory. Research studies have found that hackers appear to function in a global subculture, which exchanges ideas and techniques on how to successfully commit cybercrimes (Holt 2009; Holt et al. 2012). Hackers reported maintaining regular peer relationships with other hackers, either online, offline or both (Decary-Hetu, Morselli, and Leman-Langlois 2012; Holt 2009; Holt and Kilger 2008). Multiple studies have utilized the social learning theory to indicate its ability to explain cybercrimes (Morris and Blackburn 2009; Navarro and Marcum 2019; Skinner and Fream 1997). Therefore, the social exchanges, reasoning and support that individuals experience online could be the driving force behind cybercrimes committed in potential South African smart cities.

Favourable definitions could refer to an individual's change of attitude created by continued visits to websites and social media groups that support and encourage online criminal behaviour in South Africa (Akers 1998). The pro-criminal attitude cultivated in such groups could be the driving force behind cybercrimes committed in South African smart cities. Examples include financially motivated (see South African Postbank), politically motivated (see SAPS, South African Presidency), cyber-espionage (see Red October) or privacy breaches (see Ashley Madison) cybercrimes.

Differential reinforcement could refer to the positive reinforcements from the rewards of cybercrimes that could encourage individuals to start or continue to commit cybercrimes in South African smart cities. The rewards and lower consequences of online crimes outweigh the much higher likelihood of being caught in real-world crimes (Stalans and Donner 2018). The lucrative opportunities for financial rewards are a major driving factor in committing crimes online rather than in the real world. The positive reinforcements from the rewards of cybercrimes could be the driving force behind cybercrimes committed in South African smart cities.

Imitation applies to individuals in South Africa who observe the successes and financial rewards achieved by their online peers involved in cybercrimes and could subsequently start to emulate such behaviour. This could be an individual's first and foremost motivation to start criminal activities in South African intelligent cities (Holt and Bossler 2017). The successful execution of previous cybercriminal incidents in South African cities could motivate individuals to start to emulate such behaviour.

Social learning theory can explain the rise of cybersecurity incidents in South Africa over the last few years. In 2019, South Africa saw a sharp increase in cyberattacks. Internet service providers, utilities, e-commerce platforms and customers were severely affected. Furthermore, social learning theory can also be used to explain the rise in hacking incidents in South Africa over the last few years. Therefore, social learning can explain why cyberattacks in South African cities are committed and continue to rise.

https://doi.org/10.1017/cri.2022.12 Published online by Cambridge University Press

Subculture Theories

Social learning theory emphasizes that peer relationships and individual perceptions of crime contribute significantly to criminal behaviour. However, the theory fails to address criminal behaviour's influence on individuals (Holt and Bossler 2017). Researchers utilizing a subcultural perspective have broadened knowledge and placed in perspective the aspects that individuals account for when they commit crimes. Research has been widespread, ranging from gang membership (Miller 1958; Short 1968) to digital piracy (Cooper and Harrison 2001). Subcultural theories were developed to explain the societal structures that create oppositional subgroups in society (Stalans and Donner 2018). In a criminological and sociological context, subcultures are any group whose values, attitudes and behaviours are at odds with society's universal laws and values (Brake 1980; Kornblum 1997). Researchers have conducted numerous studies to examine the subcultural values, norms and practices of digital pirates, hackers, online fraudsters and accomplices in the online illicit sex trade (Holt 2007; Holt and Copes 2010; Holt, Freilich, and Chermak 2017; Stalans and Finn 2016).

Neutralization Theory

Sykes and Matza (1957) argued that individuals are constantly aware of the obligation to abide by the law. Individuals who commit crimes need to engage in cognitive activity to neutralize their guilt. They developed five techniques to explain how individuals "neutralize" themselves to temporarily lift their guilt and allow individuals to "drift" into committing crimes (Stalans and Donner 2018). The techniques are denial of responsibility, denial of injury, denial of the victim, condemnation of the condemners and appeal to higher loyalties. In his study, Morris (2010) utilized the theory and concluded that neutralization in combination with the influence of deviant peers was directly linked to hacking.

Additionally, the neutralization of individuals created a shared value of secrecy in the hackers' subculture. All the members of the hacking group did not want to get caught, so the group created methods like "spot the fed" warnings at hacking conventions to warn other hackers of the presence of undercover law enforcement (Stalans and Donner 2018). Moreover, the study found that hackers were inspired by their shared values in the subculture. However, targeting victims for malicious hacking attacks was based on religious and political agendas (Holt et al. 2017).

Smart cities in South Africa face severe cybersecurity risks due to neutralized hackers carrying out malicious cyberattacks. The hackers' moral disengagement with society, caused by neutralization, enables them to neutralize their guilt and engage in cybercrimes within a smart city's cyberspace. The five techniques outlined by Sykes and Matza (1957) are reviewed in light of their practical implications for cybersecurity risks, especially potential hacking incidents in South African smart cities:

- *Denial of responsibility*: Individuals may deny responsibility for their behaviour due to disengagement from society and, as a result, detach their sense of responsibility from their moral standards to commit cybercrime. The disconnect created by the Internet enables hackers and other individuals to lose any sense of responsibility. Individuals would possibly not have had the courage to carry out cybercrimes in the "real world".

- *Denial of injury:* One of the key components in social learning theory is "favourable attitudes", which maintains that some individuals create a defiant mindset that the criminal act they are engaged in is not immoral and encourages reasoning on why the cybercrime is not harmful to others. If a hacker perceives the cybersecurity breach that he/she is committing will not harm anyone, then he/she inadvertently denies that there are any affected victims present (Hinduja and Ingram 2008). The attacker could feel that their attack will only affect wealthy organizations, affluent institutions or government agencies, denying that specific individuals will be affected.
- *Denial of the victim:* Criminals often claim that the victim is deserving of the harm or is partly responsible for the harm (Stalans and Donner 2018). This may motivate criminals to engage in cybercrime because the attacker believes "they deserve it". Hackers often view themselves as a Robin Hood type of character by stealing (hacking) from the rich and giving to the poor (hacking community) (Maurushat 2019).
- *Condemnation of the condemners:* Individuals that commit cybercrimes claim that their behaviour is not wrong because those who disapprove of their behaviour engage in more unlawful activities (Stalans and Donner 2018). Hacktivists could claim that their actions of website defacement are far less destructive than that of the person or organization they are attacking. Furthermore, empirical studies have shown that in many cases, hackers blame their victims for not having good cybersecurity skills or anti-virus software to prevent them from being victims (Cross, Richards, and Smith 2016; Taylor 1999).
- *Appeal to higher loyalties:* Individuals attempt to justify themselves by claiming that their actions are motivated by other more important values. Individuals believe that their actions will benefit their friends, peers or the hacking community and feel the need to protect themselves (Schmalleger 2019). The influence of peer relations is key to introducing individuals to the techniques of neutralization to justify their immoral values and criminal behaviours in cyberspace (Bossler and Burruss 2011). Hackers maintain peer relations with other hackers online or offline and often need to prove their loyalty to each other (Holt and Kilger 2012). These beliefs are a neutralization technique to justify their criminal behaviours in cyberspace.

Over the last few decades, traditional subcultural theories have been applied to studies to explain cybercrime and deviance (Holt and Bossler 2017). The code of the street theory has proven to be effective in explaining the causes behind specific cybercrimes. The theory and its application to cybersecurity in South African smart cities are reviewed.

Code of the Street Theory

The code of the street theory was developed by Anderson (1999). The theory argues that a set of informal or "street" rules govern interpersonal relations in depreciated inner-city neighbourhoods struggling with joblessness, racism, poverty, alienation

https://doi.org/10.1017/cri.2022.12 Published online by Cambridge University Press

and mistrust of the police. These neighbourhoods are often characterized by a lack of public resources, poor service delivery and a history of racial segregation. Adverse socio-economic situations force youths to choose between believing in traditional values or the "code of the street" values which consist of illegal behaviours to get ahead in life (Stalans and Donner 2018). The theory was utilized in numerous studies (Stewart and Simons 2010), which found that individuals' loyalty to "street values" is linked to numerous violent crimes.

Henson, Swartz, and Reyns (2017) applied the code of the street theory to their empirical research to indicate how theory can explain crime in cyberspace. In their study, Henson et al. (2017) found that when youths started adopting online street-oriented beliefs, it related to online offending. Street-oriented beliefs were supported and shared on platforms such as social media and specific web forums. In another study, Holt (2007) examined the subculture of hackers using interviews with active hackers by examining data from public web forums from Defcon 2004, the largest annual hacker convention in the United States. Holt (2007) identified five general "normative orders" related to hackers. Notably, the establishment of identity within the subcategories of hackers who have shared values on violating laws is similar to that of street-oriented beliefs.

Furthermore, a study by Adeniran (2011) on the notorious Nigerian "yahoo boys" highlighted the group's use of the Internet to conduct online criminal activities, including fraud, money laundering and hacking. Poverty, unemployment and deteriorating social lifestyle standards lead to the development of the "yahoo boys" subculture (Adeniran 2011). Interestingly, the hostile socio-economic environment was similar to the environment that led to the creation of the "code of the street" values.

The code of the street theory has proven to be relevant, especially in poverty-stricken areas of the world. The subculture that gave rise to the origins of "street culture" and the online application of the values system by the Nigerian "yahoo boys" both have deep roots in poverty, unemployment and deteriorating social lifestyle standards (Adeniran 2011). South Africa faces similar socio-economic misfortunes. The unemployment rate for the fourth quarter of 2020 escalated to 32.5%, putting the number of unemployed people at 7.2 million (Stats SA 2020). Furthermore, youth unemployment, individuals aged 25–34 years, recorded the highest unemployment rate of 41.2% (Stats SA 2020). Young South African work-seekers are turning to online platforms to enhance their digital literacy to increase their chances of achieving work opportunities (Matli and Ngoepe 2020). Youth unemployment is expected to drive an increased reliance on criminality as a source of income in both the online and offline spheres.

Furthermore, opportunities for cybercrimes have increased due to uncertainty created by the COVID-19 pandemic (Mahadevan 2020). The unemployed youth in South Africa can therefore take advantage of the increased cybercrime opportunities created by the COVID-19 pandemic and turn to a life of crime on the "streets" of cyberspace. The potential "street code culture" among the unemployed youth coupled with the many specialized forums and "how-to-do" websites could breed a substantial community of hackers and other cybercriminals in South Africa. This envisioned increase in skilled cybercriminals in South Africa could pose a significant risk to its IoT-interconnected smart cities.

https://doi.org/10.1017/cri.2022.12 Published online by Cambridge University Press

New Theoretical Paradigms and Their Value to Cybersecurity in South African Smart Cities

Empirical studies have shown that traditional theories can advance knowledge of cybercrimes. However, these theoretical frameworks have clear limitations and shortcomings in their limited applicability for certain cybercrimes. As a result, there is immense value in developing new theoretical paradigms that integrate online and offline criminal behaviour more comprehensively (Holt and Bossler 2017). Furthermore, studies have shown that theoretical integration, or combining individual frameworks into a single model, could prove valuable in better understanding specific crimes (Bossler and Burruss 2011; Higgins and Marcum 2011).

The subsequent section will discuss space transition theory, ANT and integrated models in terms of their applicability to cybersecurity in smart cities.

Space Transition Theory

Space transition theory is viewed as one of the newer theories in criminology that have been designed to distinctively address the ever-growing phenomenon of cybercrimes (Holt and Bossler 2017). Developed in 2007 by Jaishankar (2007b), space transition theory attempts to explain the causation of crimes in cyberspace. He deemed it necessary to create a different theory on cybercrimes due to the inability of traditional criminological theories to suitably deliver a comprehensive explanation of the phenomenon of cybercrimes (Jaishankar 2008). Space transition theory is defined as the movement of an individual from one space to another (physical space to cyberspace) and argues that individuals conduct themselves differently when moving from one space to another.

Jaishankar (2007b) offers seven fundamental propositions regarding the behaviour of individuals when they engage online and offline:

- Individuals who control their need to conduct crime in the real world to protect their reputation could tend to engage in crimes in cyberspace.
- Cybercriminals may find it more appealing to engage in cybercrime due to the ability to use multiple identities, keep their location secret, and the absence of deterrence factors in cyberspace.
- Crimes in cyberspace are prone to move into physical space and vice versa.
- Individuals could have the opportunity to cease their criminal activities due to the temporary nature of the Internet and its disengagement from the real world.
- The Internet enables strangers to form online partnerships to plan and commit crimes in the real world and, conversely, allows real-world partnerships to engage in cybercrimes.
- Closed societies could harvest higher levels of online crime than open societies because of the oppressive nature of such regimes.
- The feeling of disengagement from the real world created by the Internet could allow individuals to disengage from their real-world societal norms and values and start engaging in cybercrime.

https://doi.org/10.1017/cri.2022.12 Published online by Cambridge University Press

Space transition theory offers a critical understanding of the behaviour of criminals in cyberspace (Al-Ali, Nimrat, and Benzaid 2018).

The COVID-19 pandemic has expanded the global cyber-landscape by forcing industries and governments to implement a massive and uncoordinated strategic shift to working remotely and relying heavily on the Internet to stay operational and conduct business (Wiggen 2020). Due to nationwide lockdowns, work-from-home offices in public and private sectors required industries to increase electronic transactions, shift offline data to online databases, and use unproved software to communicate sensitive information (Mahadevan 2020). Subsequently, millions of malware and other attacks were experienced between January and August of 2020 (Kaspersky 2020). The COVID-19 pandemic has increased risks for smart cities, businesses and individuals as they adapt to a revised operating model in the "new normal" world. Space transition theory can therefore be utilized to explain the causations of cybercrimes created by the increased movement of individuals from offline spaces to cyberspace due to the COVID-19 pandemic. Additionally, the rise of more sophisticated smart cities in South Africa will only increase and amplify cybercrime opportunities.

Actor-Network Theory

ANT is a theoretical and methodological approach to social theory that claims everything in the social and natural worlds exists through a relationship of continuously shifting networks (Latour 2005). This approach was adopted by van der Wagen and Pieters (2015), who argued that the ANT could be explicitly applied to their study on the cybercrimes committed by botnets. They further argue that the ANT could take a social constructionist approach to focus on the role technologies have on specific criminal actions, especially where the technology does not require constant human input to carry out continuous cybercrimes. A botnet attack is a new type of "cyborg crime", carried out by a combination of human and non-human criminal actions. The ANT is therefore used to draw a parallel perspective on human and non-human interactions in hybrid cybercriminal networks (van der Wagen and Pieters 2015). Van der Wagen and Pieter's (2015) application of the ANT opened a platform for scholars to start the debate over the concept that technological innovations are non-rational actors rather than tools that can be used to commit complex forms of cybercrime. This notion would lead to better insights into empirical research studies (Holt and Bossler 2017). Furthermore, van der Wagen and Pieters (2015) suggest that the ANT framework would not only be applicable for studying botnets but could also be utilized for understanding how technology affects other forms of cybercrime. Hence, the selection of the ANT framework for application to this paper.

One complex botnet case from the Netherlands was examined for their research study to demonstrate their argument. The study concluded that the human "actor" was not always entirely in control of the deployed technology, as the "botherder" (individual responsible for controlling the botnet) could not consistently predict how the botnet network would interact and carry out actions. Van der Wagen and Pieters (2015) motivated that without the ANT, their analysis and conclusion would have overstated the influence of the human as a rational "actor" managing the botnet network.

https://doi.org/10.1017/cri.2022.12 Published online by Cambridge University Press

As global smart cities have increased their reliance on technology, cybersecurity incidents have increased in sophistication. As a result, more complex forms of cybercrime will be experienced in smart cities. Therefore, smart cities around the globe and in South Africa are at risk for sophisticated cyberattacks like botnet attacks and ransomware. According to ANT, everything in the social and natural worlds exists through a relationship of continuously shifting networks. The theory is used to explain the parallel perspectives that exist between human and non-human interactions within a hybrid cybercriminal network. Furthermore, the ANT explains the causes behind such hybrid cybercriminal networks carrying out sophisticated cyberattacks on smart cities.

TOWARDS AN INTEGRATED CRIMINOLOGICAL THEORETICAL FRAMEWORK

Numerous cybercrime criminologists (Higgins and Marcum 2011; Holt and Bossler 2014) have promoted the use of integrated models in cybercrime studies. Integrated models can be referred to as integrating several theoretical perspectives into one model to better understand criminal behaviour in cyberspace (Stalans and Donner 2018). Criminal behaviour is multifaceted and cannot be interpreted merely by a single viewpoint. Therefore, theoretical integration in cybercrime could deliver comprehensive insight into why individuals engage in online criminal behaviour (Akers et al. 2016). Thus, an integrated model consists of social learning theory, street code and space transition theory.

Social learning theory can explain the rise of cybersecurity and hacking incidents in South Africa over the last few years. In the last few years, South Africa has seen a sharp increase in cyberattacks on all business fronts (Mcanyana, Brindley, and Seedat 2020). The four critical components of Akers' (1998) social learning theory, i.e. (1) differential association (supportive attitudes to commit cybercrime); (2) favourable definitions (criminal attitude gained from deviant online social interactions); (3) differential reinforcement (financial rewards to cybercrimes); and (4) imitation (emulating criminal behaviour), can effectively be used to explain the motives behind cybercrimes in South African smart cities. Social learning theory can be applied to the rise in the number of individuals that have access to the Internet and can now visit deviant websites, forums and social media sites. This could empower individuals with the required technical skills and support to carry out cybercrimes in South African smart cities. The code of the street theory can be used to explain street-oriented beliefs as the values that can be used to commit cybercrimes (Henson et al. 2017) in South African smart cities. The code of the street theory has proven to be relevant, especially in poverty-stricken areas of the world (Adeniran 2011). Space transition theory can explain why individuals conduct themselves differently when moving from the physical, real-world space to cyberspace and why this could lead to them committing cybercrimes. Moving an individual's current offline-based experience to an increased online experience will only increase opportunities for cybercrimes in South African smart cities.

All three theories can be combined to explain the current cybercriminological uptake in South Africa: social learning theory (growing number of empowered, cyber-skilled individuals with deviant peers); the code of the street theory

https://doi.org/10.1017/cri.2022.12 Published online by Cambridge University Press

(unemployed individuals with online street values and increased opportunities for cybercrimes due to the COVID-19 pandemic); and space transition theory (individual behaviour change from the real world to cyberspace).

Social learning theory-related incidents in South African cities include politically motivated cybercrimes, which include hacktivism through web defacement. Code of the street theory in a South African smart city context refers to the unemployed youth who could turn to online crime as a worthwhile opportunity for financial reward rather than attempting crime in the real world. The adverse socio-economic situation could be the driving force behind creating an online "code of the street" culture amongst youth seeking the rewards of cybercrimes in South African smart cities. Moreover, space transition theory in a South African smart city context refers to the disconnect created by the Internet that enables individuals to lose any sense of responsibility and behave in a manner they would not have done offline or in the real world.

CONCLUSION

Criminological theories play a significant role in explaining why individuals commit a crime. This article accentuated the value of criminological theories in explaining cybersecurity risks in smart cities. The authors illustrated how theoretical perspectives from traditional criminological theories, subculture theories and new theoretical paradigms could be combined into an integrated criminological theoretical framework as a valuable resource to provide a comprehensive understanding of cybercrimes in South African smart cities. This understanding contributes constructive insights to explain cybersecurity risks in smart cities and the planning and implementation of cybersecurity goals in South African smart cities.

Acknowledgements. The authors would like to acknowledge all the participants who participated in the larger study on which this article is premised and the Editorial Office of the *International Annals of Criminology* for the assistance in its publication.

References

Adeniran, Adebusuyi I. 2011. "Café Culture and Heresy of Yahooboyism in Nigeria." Pp. 3–12 in *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*, edited by K. Jaishankar. Boca Raton, FL: Taylor & Francis.

Akers, Ronald L. 1998. *Social Learning and Social Structure: A General Theory of Crime and Deviance*. Boston, MA: Northeastern University Press.

Akers, Ronald L., Christine S. Sellers, and Wesley G. Jennings. 2016. *Criminological Theories: Introduction, Evaluation, and Application*, 7th ed. Oxford: Oxford University Press.

Akhuseyinoglu, Nuray B. and James Joshi. 2020. "Access Control Approaches for Smart Cities." Pp. 1–40 *in IoT Technologies in Smart-Cities: From Sensors to Big Data, Security and Trust*, edited by F. Al-Tudjman and M. Imran. Stevenage: Institution of Engineering and Technology.

Al-Ali, Abdelrahman A., Amer Nimrat, and Chafika Benzaid. 2018. "Combating Cyber Victimisation: Cybercrime Prevention." Pp. 325–39 in *Cyber Criminology*, edited by H. Jahankhani. Cham, Switzerland: Springer.

Allam, Zaheer. 2021. *The Rise of Autonomous Smart Cities: Technology, Economic Performance, and Climate Resilience*. London: Palgrave Macmillan.

Anderson, Elijah. 1999. *Code of the Street: Decency, Violence, and the Moral Life of the Inner City*. New York: W. W. Norton & Company.

https://doi.org/10.1017/cri.2022.12 Published online by Cambridge University Press

Barlow, Mike and Cornelia Levy-Bencheton. 2019. *Smart Cities, Smart Future: Showcasing Tomorrow*. Hoboken, NJ: John Wiley & Sons.

Bossler, Adam M. and George W. Burruss. 2011. "The General Theory of Crime and Computer Hacking: Low Self-Control Hackers?" Pp. 38–67 in *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, edited by T. J. Holt and B. H. Schell. Hershey, PA: Business Science Reference.

Brake, Mike. 1980. *The Sociology of Youth Cultures and Youth Subcultures*. London: Routledge and Kegan Paul.

British Standards Institution. 2014. "PAS 180 Smart Cities – Terminology." BSI, retrieved 9 July 2020 (https://www.bsigroup.com/en-GB/smart-cities/Smart-Cities-Standards-and-Publication/PAS-180-smart-cities-terminology/).

BusinessTech. 2020. "Ramaphosa Has a Plan for a New 'Smart City' in Gauteng." 14 February 2020, retrieved 15 February 2021 (https://businesstech.co.za/news/technology/374270/ramaphosa-has-a-plan-for-a-new-smart-city-in-gauteng/).

Cooper, Jon and Daniel M. Harrison. 2001. "The Social Organization of Audio Piracy on the Internet." *Media, Culture, and Society* 23(1):71–89.

Cornelius, François Paul. 2022. *Cyber Security Risks in Smart Cities: A South African Perspective*. Unpublished MA Dissertation, University of South Africa, Pretoria.

Crawford, Linda M. 2020. "Conceptual and Theoretical Frameworks in Research." Pp. 35–48 in *Research Design and Methods: An Applied Guide for the Scholar–Practitioner*, edited by G. J. Burkholder, K. A. Cox, L. M. Crawford, J. H. Hitchcock, and M. Q. Patton. Thousand Oaks, CA: Sage.

Cross, Cassandra, Kelly M. Richards, and Russel G. Smith. 2016. "The Reporting Experiences and Support Needs of Victims of Online Fraud." *Trends and Issues in Crime and Criminal Justice* 518(1):1–14.

Decary-Hetu, David, Carlo Morselli, and Stéphane Leman-Langlois. 2012. "Welcome to the Scene: A Study of Social Organization and Recognition Among Warez Hackers." *Journal of Research in Crime and Delinquency* 49(3):359–82.

Deloitte. 2015. "Smart Cities: How Rapid Advances in Technology are Reshaping our Economy and Society." Retrieved 28 October 2020 (https://www2.deloitte.com/tr/en/pages/public-sector/articles/smart-cities.html).

ESET. 2016. "En Route with Sednit: Part I: Approaching the Target." Version 1.0. Retrieved 18 May 2021 (https://www.welivesecurity.com/wp-content/uploads/2016/10/eset-sednit-part1.pdf).

Ferreira, Maria I. A. (ed.). 2021. *How Smart is Your City?: Technological Innovation, Ethics, and Inclusiveness*. Cham, Switzerland: Springer.

FireEye. 2014. "APT28: A Window into Russia's Cyber Espionage Operations?" Retrieved 18 May 2021 (https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf).

Foster, Kevin. 2020. "Smarten Up: Paths to Bottom-Up Smart Cities and the Risks of Top-Down Smart Governance." Pp. 23–8 in *South African Cities Network: Smart Cities Paper Series: Smart Governance in South African Cities*. The South African Cities Network (SACN). Retrieved 27 April 2021. (https://www.sacities.net/wp-content/uploads/2020/10/Smart_Cities_Papers_Volume_1_Final-Draft.pdf).

Gauteng Department of Human Settlements. 2018. "Gauteng Infrastructure Funding Summit: Mega Projects." Retrieved 25 October 2020 (https://www.gpf.org.za/wp-content/uploads/2018/04/MEGA-Projects-Booklet-V7-ilovepdf-compressed.pdf).

Ghosal, Amrita and Subir Halder. 2018. "Building Intelligent Systems for Smart Cities: Issues, Challenges, and Approaches." Pp. 107–25 in *Smart Cities: Development and Governance Frameworks*, edited by Z. Mahmood. Cham, Switzerland: Springer.

Gilson, Lucy L. and Caren B. Goldberg. 2015. "Editors' Comment: So, What is a Conceptual Paper?" *Group & Organization Management* 50(2):127–30.

Grabosky, Peter N. 2001. "Virtual Criminality: Old Wine in New Bottles?" *Social and Legal Studies* 10(2):243–9.

Henson, Billy, Kristin Swartz, and Bradford W. Reyns. 2017. "#Respect: Applying Anderson's Code of the Street to the Online Context." *Deviant Behavior* 38(7):768–80.

Higgins, George E. and Catherine D. Marcum. 2011. *Digital Piracy: An Integrated Theoretical Approach*. Raleigh, NC: Carolina Academic Press.

Hinduja, Sameer and Jason R. Ingram. 2008. "Self-Control and Ethical Beliefs on the Social Learning of Intellectual Property Theft." *Western Criminology Review* 9(2):52–72.

https://doi.org/10.1017/cri.2022.12 Published online by Cambridge University Press

Holt, Thomas J. 2007. "Subcultural Evolution? Examining the Influence of On- and Offline Experiences on Deviant Subcultures." *Deviant Behavior* 28(2):171–98.

Holt, Thomas J. 2009. "Lone Hacks or Group Cracks: Examining the Social Organization of Computer Hackers." Pp. 336–55 in *Crimes of the Internet*, edited by F. Smalleger and M. Pittaro. Upper Saddle River, NJ: Pearson Prentice Hall.

Holt, Thomas J. and Adam M. Bossler. 2014. "An Assessment of the Current State of Cybercrime Scholarship." *Deviant Behavior* 35(1):20–40.

Holt, Thomas J. and Adam M. Bossler. 2017. *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*. London: Routledge.

Holt, Thomas J. and Heith Copes. 2010. "Transferring Subcultural Knowledge Online: Practices and Beliefs of Digital Pirates." *Deviant Behavior* 31(7):625–54.

Holt, Thomas J., Joshua D. Freilich, and Steven M. Chermak. 2017. "Exploring the Subculture of Ideologically Motivated Cyber-Attackers." *Journal of Contemporary Criminal Justice* 33(3):212–33.

Holt, Thomas J. and Max Kilger. 2008. "Techcrafters and Makecrafters: A Comparison of Two Populations of Hackers." Pp. 67–78 in *2008 WOMBAT Workshop on Information Security Threats Data Collection and Sharing (WISTDCS)*. Amsterdam, the Netherlands: IEEE Computer Society.

Holt, Thomas J. and Max Kilger. 2012. "Know Your Enemy: The Social Dynamics of Hacking." *The Honeynet Project*, 29 May 2012, retrieved 4 April 2021 (https://www.honeynet.org/papers/kye-kyt/know-your-enemy-the-social-dynamics-of-hacking/).

Holt, Thomas J., Deborah Strumsky, Olga Smirnova, and Max Kilger. 2012. "Examining the Social Networks of Malware Writers and Hackers." *International Journal of Cyber Criminology* 6(1):891–903.

Hosken, Graeme. 2020. "Data from Huge Experian Breach Found on the Internet." *TimesLIVE*, 13 September 2020, retrieved 30 April 2021 (https://www.timeslive.co.za/sunday-times/news/2020-09-13-data-from-huge-experian-breach-found-on-the-internet/).

International Organization for Standardization and International Electrotechnical Commission (ISO/IEC). 2015. "Smart Cities: Preliminary Report 2014." Retrieved 24 February 2021 (https://www.iso.org/files/live/sites/isoorg/files/developing_standards/docs/en/smart_cities_report-jtc1.pdf).

Jaishankar, Karuppannan. 2007a. "Editorial. Cyber Criminology: Evolving a Novel Discipline with a New Journal." *International Journal of Cyber Criminology* 1(1):1–6.

Jaishankar, Karuppannan. 2007b. "Establishing a Theory of Cyber-Crimes." *International Journal of Cyber Criminology* 1(2):7–9.

Jaishankar, Karuppannan. 2008. "Space Transition Theory of Cyber-Crimes." Pp. 283–301 in *Crimes of the Internet*, edited by F. Schmallager and M. Pittaro. Upper Saddle River, NJ: Prentice Hall.

Karvonen, Andrew, Federico Cugurullo, and Federico Caprotti (eds). 2019. *Inside Smart Cities: Place, Politics and Urban Innovation*. London: Routledge.

Kaspersky. 2020. "Kaspersky Security Bulletin 2020. Statistics." Retrieved 23 February 2021 (https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2020_en.pdf).

Khan, Iman, Muhammad N. Iftikhar, Saleem H. Ali, and Shua Khalid. 2021. "Cities and COVID-19: Navigating the New Normal." *Global Sustainability* 4(12):1–6. Retrieved 5 May 2021 (https://www.cambridge.org/core/services/aop-cambridge-core/content/view/4096D1C809023C58527C59A9E1BB1DD3/S2059479821000107a.pdf/div-class-title-cities-and-covid-19-navigating-the-new-normal-div.pdf).

Kornblum, William. 1997. *Sociology in a Changing World*, 4th ed. Fort Worth, TX: Harcourt Brace and Company.

Kovacs, Eduard. 2019. "Russian Hackers Behind Ukraine Power Outage May Have Sought More Damage." *SecurityWeek*, 13 September 2019, retrieved 1 November 2020 (https://www.securityweek.com/russian-hackers-behind-ukraine-power-outage-may-have-sought-more-damage).

KPMG. 2019. "Cybersecurity in Smart Cities." Retrieved 11 October 2019 (https://home.kpmg/in/en/home/insights/2019/02/cybersecurity-smartcities.html).

Latour, Bruno. 2005. *Reassembling the Social: An Introduction to Actor-Network Theory*. Oxford: Oxford University Press.

Leavy, Patricia. 2017. *Research Design: Quantitative, Qualitative, Mixed Methods, Arts-Based, and Community-Based Participatory Research Approaches*. New York: The Guilford Press.

Le-Dang, Quang and Tho Le-Ngoc. 2018. "Internet of Things (IoT) Infrastructures for Smart Cities." Pp. 1–30 in *Handbook of Smart Cities Software Services and Cyber Infrastructure*, edited by M. Maheswaran and E. Baddi. Cham, Switzerland: Springer.

https://doi.org/10.1017/cri.2022.12 Published online by Cambridge University Press

Lee, Timothy B. 2015. “The Ashley Madison Hack, Explained.” *Vox*, 19 August 2015, retrieved 15 May 2021 (https://www.vox.com/2015/7/20/9007039/ashley-madison-hack-explained).

Lozada, Nelson, Jose Arias-Pérez, and Geovanny Perdomo-Charry. 2019. “Big Data Analytics Capability and Co-Innovation: An Empirical Study.” *Heliyon* 5(10):1–7.

Mahadevan, Prem. 2020. “Cybercrime: Threats During the Covid-19 Pandemic.” Geneva, Switzerland: Global Initiative. Retrieved 4 April 2021 (https://globalinitiative.net/analysis/cybercrime-covid-19/).

Matli, Walter and Mpho Ngoepe. 2020. “Capitalizing on Digital Literacy Skills for Capacity Development of People Who Are Not in Education, Employment or Training in South Africa.” *African Journal of Science, Technology, Innovation, and Development* 12(2):129–39.

Maurushat, Alana. 2019. *Ethical Hacking*. Ottawa, Ontario: University of Ottawa.

Mcanyana, Wandile, Clive Brindley, and Yusof Seedat. 2020. “Cyberthreat Landscape in South Africa.” Retrieved 20 September 2021 (https://www.accenture.com/_acnmedia/PDF-125/Accenture-Insight-Into-The-Threat-Landscape-Of-South-Africa-V5.pdf).

Miller, Walter. B. 1958. “Lower Class Culture as a Generating Milieu of Gang Delinquency.” *Journal of Social Issues* 14(3):5–19.

Milman, Oliver. 2021. “Largest US Pipeline Restarts Operations After Hack Shut It Down for Nearly a Week.” *The Guardian*, 12 May 2021, retrieved 26 May 2021 (https://www.theguardian.com/us-news/2021/may/12/us-fuel-shortages-pipeline-hack-drivers).

Mimecast. 2021.“What 2021 Holds for Cybersecurity in South Africa.” *BusinessTech*, 8 February 2021, retrieved 10 August 2021 (https://businesstech.co.za/news/industry-news/466148/what-2021-holds-for-cybersecurity-in-south-africa/).

Morris, Robert G. 2010. “Computer Hacking and the Techniques of Neutralization: An Empirical Assessment.” Pp. 1–17 in *Corporate Hacking and Technology-Driven Crime: Social Dynamics and Implications*, edited by T. J. Holt and B. Schell. New York: Information Science Reference.

Morris, Robert G. and Ashley G. Blackburn. 2009. “Cracking the Code: An Empirical Exploration of Social Learning Theory and Computer Crime.” *Journal of Crime and Justice* 32(1):1–34.

Moyo, Admire. 2019. “Bad Day for SA’s Cyber Security as Banks Suffer DDoS Attacks.” *ITWeb*, 25 October 2019, retrieved 30 April 2021 (https://www.itweb.co.za/content/LPp6V7r4OVzqDKQz).

Navarro, Jordana N. and Catherine D. Marcum. 2019. “Deviant Instruction: The Applicability of Social Learning Theory to Understanding Cybercrime.” Pp 1–20 in *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, edited by T. Holt and Adam Bossler. Cham, Switzerland: Palgrave Macmillan.

Newburn, Tim. 2017. *Criminology*, 3rd ed. London: Routledge.

Nxumalo, Mphathi. 2018. “SA Presidency Website Hacked.” *IOL*, 11 July 2008, retrieved 19 May 2021 (https://www.iol.co.za/dailynews/news/sa-presidency-website-hacked-15950026).

Pandey, Piyush, Sean Peasley, and Mahesh Kelkar. 2019. “Making Smart Cities Cybersecure: Ways to Address Distinct Risks in an Increasingly Connected Urban Future.” *Deloitte Insights*, 11 April 2019, retrieved 10 August 2020 (https://www2.deloitte.com/us/en/insights/focus/smart-city/making-smart-cities-cyber-secure.html).

Patton, Michael Q. 2015. *Qualitative Research and Evaluation Methods*, 4th ed. Thousand Oaks, CA: Sage.

Pelton, Joseph N. and Indu B. Singh. 2018. *Smart Cities of Today and Tomorrow: Better Technology, Infrastructure, and Security*. Cham, Switzerland: Springer.

Roane, Brendan. 2013. “SAPS Website Hacked.” *The Star*, 22 May 2013, retrieved 19 May 2021 (https://www.iol.co.za/news/saps-website-hacked-1520042).

RSA Security. 2019. “Digital Risk Report.” September 2019, retrieved 30 May 2020 (https://www.rsa.com/content/dam/en/white-paper/rsa-digital-risk-report-2019.pdf).

Schmalleger, Frank. 2019. *Criminology Today: An Integrative Introduction*. New York: Pearson.

Schurink, Willem J., Evanthe M. Schurink, and Christa B. Fouché. 2021. “Thematic Inquiry in Qualitative Research.” Pp. 289–310 in *Research at Grass Roots: For the Social Sciences and Human Service Professions*, edited by C. B. Fouché, H. Strydom, and W. J. H. Roestenburg. Pretoria: Van Schaik.

Short, James F. 1968. *Gang Delinquency and Delinquent Subcultures*. Oxford: Harper and Row.

Sicetsha, Andile. 2018. “Hack Alert: The Presidency’s Website Has Just Been Hacked.” *The South African*, 7 July 2018, retrieved 13 May 2021 (https://www.thesouthafrican.com/news/hack-alert-the-presidencys-website-has-just-been-hacked/).

https://doi.org/10.1017/cri.2022.12 Published online by Cambridge University Press

Skinner, William F. and Anne M. Fream. 1997. "A Social Learning Theory Analysis of Computer Crime Among College Students." *Journal of Research in Crime and Delinquency* 34(4):495–518.

South African Banking Risk Information Centre. 2019. "South African Banks Resilient in the Face of Latest DDoS Attacks." *SABRIC*, 23 October 2019, retrieved 30 April 2021 (https://www.sabric.co.za/media-and-news/press-releases/south-african-banks-resilient-in-the-face-of-latest-ddos-attacks/).

South African Banking Risk Information Centre. 2020. "Experian Data Breach." *SABRIC*, retrieved 16 December 2020 (https://www.sabric.co.za/media-and-news/press-releases/experian-data-breach/).

Stalans, Loretta J. and Christopher M. Donner. 2018. "Explaining Why Cybercrime Occurs: Criminological and Psychological Theories." Pp. 25–45 in *Cyber Criminology*, edited by H. Jahankhani. Cham, Switzerland: Springer.

Stalans, Loretta J. and Mary A. Finn. 2016. "Consulting Legal Experts in the Real and Virtual World: Pimps' and Johns' Cultural Schemas About Strategies to Avoid Arrest and Conviction." *Deviant Behavior* 37(6):644–64.

Statista. 2021. "South Africa Number of Social Network Users 2017–2025." 28 January 2021, retrieved 4 April 2021 (https://www.statista.com/statistics/972776/number-of-social-network-users-in-south-africa/#:~:text=This%20statistic%20shows%20the%20number,26.81%20million%20users%20in%202025).

Stats SA. 2020. "Quarterly Labour Force Survey (QLFS) Q4:2020." Retrieved 4 April 2021 (http://www.statssa.gov.za/publications/P0211/Presentation%20QLFS%20Q4_2020.pdf).

Stewart, Eric A. and Ronald L. Simons. 2010. "Race, Code of the Street, and Violent Delinquency: A Multilevel Investigation of Neighborhood Street Culture and Individual Norms of Violence." *Criminology* 48(2):569–605.

Sutherland, Edwin H. 1947. *Principles of Criminology*, 4th ed. Philadelphia, PA: Lippincott.

Swart, Werner and Mzilikazi Wa Afrika. 2012. "It Was a Happy New Year's Day for the Gang Who Pulled Off the R42m Postbank Heist." *TimesLIVE*, 15 January 2012, retrieved 14 May 2021 (https://www.timeslive.co.za/news/south-africa/2012-01-15-it-was-a-happy-new-years-day-for-gang-who-pulled-offr42m-postbank-heist/).

Sykes, Gresham M. and David Matza. 1957. "Techniques of Neutralization: A Theory of Delinquency." *American Sociological Review* 22(6):664–70.

Taylor, Paul A. 1999. *Hackers: Crime in the Digital Sublime*. London: Routledge.

Tham, Irene. 2018. "Personal Info of 1.5m SingHealth Patients, Including PM Lee, Stolen in Singapore's Worst Cyber Attack." 21 July 2018, retrieved 1 November 2020 (https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most).

Tubbs, Bonnie. 2013. "SAPS Hack Spells Negligence." *ITWeb*, 22 May 2013, retrieved 19 May 2021 (https://www.itweb.co.za/content/nG98YdqL2yx7X2PD).

United Nations. 2018. "68% of the World Population Projected to Live in Urban Areas by 2050, Says UN." New York: United Nations. Retrieved 9 October 2019 (https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html).

Valeriano, Brandon and Ryan C. Maness. 2015. *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. New York: Oxford University Press.

Van der Wagen, Wytske and Wolter Pieters. 2015. "From Cybercrime to Cyborg: Botnets as Hybrid Criminal Actor-Networks." *British Journal of Criminology* 55(3):578–95.

Vermeulen, Jan. 2015. "Ashley Madison Hack List: South African Details." *MyBroadband*, 21 August 2015, retrieved 15 May 2021 (https://mybroadband.co.za/news/security/135972-ashley-madison-hack-list-south-african-details.html).

Wall, David S. 1998. "Catching Cybercriminals: Policing the Internet." *International Review of Law, Computers, and Technology* 12(2):201–18.

White, Thomas and Francesco Marchet. 2021. "Digital Social Markets: Exploring the Opportunities and Impacts of Gamification and Reward Mechanisms in Citizen Engagement and Smart City Services." Pp 103–44 in *How Smart is Your City?: Technological Innovation, Ethics, and Inclusiveness*, edited by M. I. A. Ferreira. Cham, Switzerland: Springer.

Wiggen, Johannes. 2020. "The Impact of COVID-19 on Cyber Crime and State-Sponsored Cyber Activities." *Konrad Adenauer Stiftung*, June 2020, retrieved 10 April 2021 (https://www.jstor.org/stable/resrep25300?seq=1#metadata_info_tab_contents).

https://doi.org/10.1017/cri.2022.12 Published online by Cambridge University Press

Woollaston-Webber, Victoria. 2017. "WannaCry Ransomware: What is It and How to Protect Yourself." *Wired*, 22 May 2017, retrieved 4 November 2020 (https://www.wired.co.uk/article/wannacry-ransomware-virus-patch).

World Economic Forum. 2018. *The Global Risks Report 2018*, 13th ed. Retrieved 9 August 2020 (https://www3.weforum.org/docs/WEF_GRR18_Report.pdf).

TRANSLATED ABSTRACTS

Abstracto

El desarrollo de ciudades inteligentes en Sudáfrica tiene el potencial de enriquecer la calidad de vida, fomentar el crecimiento económico y reducir la huella ecológica humana. Puede avanzar y elevar la prestación de servicios en áreas urbanas mediante la aplicación de diversas Tecnologías de la Información y la Comunicación. Sin embargo, a pesar de los innumerables beneficios disponibles, las ciudades inteligentes corren el riesgo de sufrir importantes brechas de seguridad cibernética que pueden tener consecuencias devastadoras. Las teorías criminológicas proporcionan una base para comprender y explicar la actividad delictiva. Los avances en las tecnologías informáticas y el mayor uso de dispositivos electrónicos e Internet han resultado en delitos cometidos en el ciberespacio. Como tal, los estudiosos de la criminología se vieron obligados a pensar de manera diferente sobre cómo se cometen los delitos en el ciberespacio y cómo se pueden avanzar las perspectivas teóricas para explicar estos delitos no tradicionales. Este artículo sostiene que las teorías criminológicas pueden informar los riesgos de seguridad cibernética en las ciudades inteligentes. Este artículo se basa en hallazgos teóricos a través de una investigación cualitativa, y los datos fueron analizados temáticamente. Los autores ilustran el valor de la teoría del aprendizaje social, de la neutralización, del código de la calle, de la transición espacial, del actor-red y la del modelo integrado para explicar los riesgos de ciberseguridad en las ciudades inteligentes.

Palabras clave ciberdelincuencia, teorías criminológicas, ciudades inteligentes, la seguridad cibernética, riesgos de ciberseguridad

https://doi.org/10.1017/cri.2022.12 Published online by Cambridge University Press

Abstrait

Le développement de villes intelligentes en Afrique du Sud a le potentiel d'enrichir la qualité de vie, d'encourager la croissance économique et de réduire l'empreinte écologique humaine. Il peut faire progresser et élever la prestation de services dans les zones urbaines en appliquant diverses technologies de l'information et de la communication. Cependant, malgré les innombrables avantages disponibles, les villes intelligentes sont exposées à des failles majeures de cybersécurité qui peuvent avoir des conséquences dévastatrices. Les théories criminologiques fournissent une base pour comprendre et expliquer l'activité criminelle. Les progrès des technologies informatiques et l'utilisation accrue d'appareils électroniques et d'Internet ont entraîné des crimes commis dans le cyberespace. En tant que tels, les chercheurs en criminologie ont été contraints de penser différemment sur la façon dont les crimes sont commis dans le cyberespace et sur la manière dont les perspectives théoriques peuvent être avancées pour expliquer ces crimes non traditionnels. Cet article soutient que les théories criminologiques peuvent éclairer les risques de cybersécurité dans les villes intelligentes. Cet article est basé sur des découvertes théoriques à travers une enquête qualitative, et les données ont été analysées thématiquement. Les auteurs illustrent la valeur de la théorie de l'apprentissage social, de la théorie de la neutralisation, de la théorie du code de la rue, de la théorie de la transition spatiale, de la théorie des acteurs-réseaux et de la théorie des modèles intégrés pour expliquer les risques de cybersécurité dans les villes intelligentes.

Mots-clés cybercriminalite, théories criminologiques, villes intelligentes, la cybersécurité, risques de cybersécurité

抽象的

南非智慧城市的发展具有丰富生活质量、鼓励经济增长和减少人类生态足迹的潜力。它可以通过应用各种信息和通信技术来推进和提升城市地区的服务提供。然而, 尽管有无数的好处, 智慧城市仍面临可能产生毁灭性后果的重大网络安全漏洞的风险。犯罪学理论为理解和解释犯罪活动提供了基础。计算机技术的进步以及电子设备和互联网的使用增加导致网络空间犯罪。因此, 犯罪学学者被迫以不同的方式思考网络空间中的犯罪行为以及如何推进理论视角来解释这些非传统犯罪。本文认为, 犯罪学理论可以为智慧城市的网络安全风险提供信息。本文基于定性调查的理论发现, 并对数据进行了主题分析。作者阐述了社会学习理论、中和理论、街道代码理论、空间转换理论、行动者网络理论和集成模型理论在解释智慧城市网络安全风险中的价值。

关键词：网络犯罪，犯罪学理论，智慧城市，网络安全;网络安全风险

https://doi.org/10.1017/cri.2022.12 Published online by Cambridge University Press

الملخص

إن تطوير المدن الذكية في جنوب إفريقيا لديه القدرة على إثراء نوعية الحياة ، وتشجيع النمو الاقتصادي ، وتقليل البصمة البيئية البشرية. يمكن أن تقدم وترتقي بتقديم الخدمات في المناطق الحضرية من خلال تطبيق تقنيات المعلومات والاتصالات المختلفة. ومع ذلك ، على الرغم من الفوائد العديدة المتاحة ، فإن المدن الذكية معرضة لخطر الانتهاكات الأمنية السيبرانية الكبرى التي يمكن أن تؤدي إلى عواقب وخيمة. توفر النظريات الإجرامية أساسا لفهم النشاط الإجرامي وتفسيره. أدى التقدم في تقنيات الكمبيوتر وزيادة استخدام الأجهزة الإلكترونية والإنترنت إلى ارتكاب جرائم في الفضاء السيبراني. على هذا النحو ، اضطر علماء الجريمة إلى التفكير بشكل مختلف حول كيفية ارتكاب الجرائم في الفضاء الإلكتروني وكيف يمكن تطوير المنظورات النظرية لشرح هذه الجرائم غير التقليدية. تؤكد هذه المقالة أن النظريات الإجرامية يمكن أن تبلغ مخاطر الأمن السيبراني في المدن الذكية. تستند هذه الورقة إلى النتائج النظرية من خلال تحقيق نوعي ، وتم تحليل البيانات بشكل موضوعي. يوضح المؤلفون قيمة نظرية التعلم الاجتماعي ، ونظرية التحييد ، ورمز نظرية الشارع ، ونظرية انتقال الفضاء ، ونظرية شبكة الممثل ، ونظرية النموذج المتكامل في شرح مخاطر الأمن السيبراني في المدن الذكية.

الكلمات المفتاحية جرائم الإنترنت؛ نظريات علم الجريمة. مدينة ذكية؛ الأمن الإلكتروني؛ مخاطر الأمن السيبراني

François Paul Cornelius holds an MA in Criminal Justice and is a PhD candidate in the Department of Criminology and Security Science at the University of South Africa. His field of interest comprises criminal law and criminology, focusing on cybercrime in smart cities.

Shandré Kim Jansen van Rensburg is an Associate Professor in the Department of Criminology and Security Science, University of South Africa. Her fields of interest include cybercrime, contemporary criminology, transformative research methodology, and women in safety and security.

Sarika Kader is a Senior Lecturer in the Department of Criminology and Security Science, University of South Africa. Her fields of interest include criminology, victimology, and safety and security.

Cite this article: Cornelius, F. P., Jansen van Rensburg, S. K., and Kader, S. 2022. The Value of Criminological Theories in Explaining Cybersecurity in South African Smart Cities. *International Annals of Criminology* **60**, 220–240. https://doi.org/10.1017/cri.2022.12