IST-Africa 2017 Conference Proceedings
Paul Cunningham and Miriam Cunningham (Eds)
IIMC International Information Management Corporation, 2017
ISBN: 978-1-905824-56-4

Applying the Gordon & Ford Categorisation and the Routine Activities Theory to Cybercrime: A Suitable Target

Sagwadi MABUNDA
University of the Western Cape, Robert Sobukwe Rd, Bellville, Cape Town, 7535, South Africa
Email: Sagwadi.mabunda@gmail.com

Abstract: This article speaks to the societal implications of technology by discussing the problems presented by cybercrime. It identifies a twofold problem. The first is that the proliferation of cybercrime is outstripping the pace at which governments can respond. The second is that there is a tendency to respond to issues relating to cybercrime on a superficial level without the appropriate technical understanding of the elements of cybercrime. This paper proposes that one of the ways of tackling cybercrime is to adopt the Routine Activities Theory, particularly the element of target suitability. This paper proposes that once a suitable target has been identified, the Gordon & Ford categorisation of cybercrimes be adopted as a policy framework for legislation and conventions. It illustrates the proposition by applying the categorisation to the South African Cybercrimes Bill.

Key words: Cybercrime, cybersecurity, routine activities theory, suitable target.

1. Introduction

As the world moves into a hyper-connected global society with near universal access to the internet, it is hard to imagine any “computer crime” that will not involve internet connectivity and interaction with cyberspace. These technological advancements require fundamental changes in the approaches to law enforcement, criminal investigation and evidence gathering, as well as issues surrounding international co-operation. [1]

In 2011, at least 2.3 billion people globally had access to the internet, a figure which is equivalent to one third of the world’s population. More than 60 per cent of all internet users lived in developed countries and about 45 percent of them were below the age of 25 years. It is estimated that by the year 2017, subscriptions to mobile broadband will encompass more than 70 per cent of the world’s population. [2] It is beyond doubt that any meaningful discussion of cybersecurity needs to take cybercrime as its primary concern.

The problems embedded in the issue of cybercrime are at least twofold. Firstly, the proliferation of cybercrime globally and, more specifically, in Africa, is outstripping the pace at which governments and lawmakers are able to respond efficiently. Secondly, where governments do manage to respond, there is a temptation to do so based on a superficial understanding of the nature of cybercrime. These problems have given cybercriminals free reign and have cost nations billions of dollars annually while posing major threats to technological development. This paper seeks to respond to the second problem by suggesting a two-part framework in which to reconceptualise cybercrime.

The first leg of the proposed framework that will be considered is Routine Activities Theory (RAT) developed by Felson & Cohen. The second leg is the two type classification of cybercrime formulated by Gordon & Ford. In combination, these legs are meant to constitute a framework upon which laws and policies may be constructed and within which cybersecurity vulnerabilities may be assessed to mitigate against breaches and major losses.

2. Cybercrime: African perspective

In a survey conducted by Stander in 2009, it was found that 45 per cent of South African respondents reported that they had experienced one or more electronic attacks within the preceding 12 months on the integrity, confidentiality and availability of systems. The respondents suspected that the most common motives for the electronic attacks on the integrity, confidentiality and availability of systems were foreign government political advantage (28 per cent), illicit financial gain (25 per cent) and indiscriminate random acts (22 per cent). [3]

It was estimated from data provided by the respondents that in the 12-month survey period, losses amounted to some R57, 8 million, with R50,1 million of this total being lost through unauthorised access to information by insiders. [4] These are rough estimates because of the low rates of reporting of computer-related crimes. Thirty per cent of South African organisations chose not to report these crimes to anyone outside the organisation or to law enforcement. This is comparable to the United States and Australia, where 30 per cent and 69 per cent of affected organisations respectively, chose not to report such crimes. When asked why this was the case, 23 per cent of respondents in South Africa noted that they reported the attacks to legal counsel for civil remedies. Thirty-three per cent of respondents in South Africa indicated that they did not report the incidents because, they believed that civil remedies would yield better results than criminal prosecution. Also, 27 per cent of the respondents were of the opinion that law enforcement would not be capable of apprehending the perpetrator and a further 27 per cent considered that the incident was not serious enough to warrant criminal reporting. [5] Only 15 per cent of South African respondents reported that the investigation resulted in charges being laid. [6]

Africa was the last continent to embrace information and communication technologies (ICT), and a decade ago, only a handful of African countries had local internet access. [7] There has been since a monumental growth in the adoption of ICT across sub-Saharan Africa. However, this has occurred in the context of inadequate telecommunication infrastructures. What is more, there has been great difficulty in securing uninterrupted access to innovative information technological advances such as e-governments, e-commerce and telemedicine. [8] Be that as it may, statistics show that the growth of online connectivity in Africa has grown by more than 1000% between 2000 and 2009. [9]

The endless possibilities created by internet access for billions across the world have created also unlimited capabilities for those tied to the criminal world. Those who wish to engage in criminal activities have taken full advantage of the internet's power to commit a host of cybercrimes. [10] The ubiquity of cybercrime has become common knowledge and its detrimental effect cannot be overstated.

The Draft African Union Convention on the Establishment of a Legal Framework Conducive to Cybersecurity in Africa pronounces that Africa needs to address cybersecurity concerns as a matter of urgency. It acknowledges that the stakes are extremely high and need to be addressed globally at the international level, with all member states of the African Union being on board with security initiatives. Some of the noteworthy initiatives that have been deployed in Africa include the ECA's comprehensive harmonisation project in co-operation with the authorities of UEMOA and ECOWAS. Also, the International Telecommunication Union has produced a guide on cybersecurity for use by developing countries.

These initiatives acknowledge the problem of cybercrime and indicate effort to address it. However, the responses remain very fragmented and disharmonious still. The cybercriminals are always a few steps ahead of law enforcement because of the extraordinary rate at which technology evolves, making it dangerous to misunderstand the creature that cybercrime is.

3. The Routine Activities Theory

3.1 Spatio-Temporal Character of RAT

Routine activities theory studies criminal violations as events, which occur at specific locations in space and in time and which involve specific persons and/or objects. [11] The aetiological formula of RAT is *crime = motivated offender + suitable target – capable guardian*. To explain this formula and/or anticipate trends in offending, the three constitutive elements need to converge in space and time. At the micro level, this means that, for a crime to be committed, both the offender and the target need to be present at a particular location at the same time, and the guardian needs to be absent. [12] At the macro level, the theory posits that there are several features in the larger society and larger community which can make the convergence of these essential elements more likely. [13] Routine activities are activities that create the variable environment where such spatial and temporal convergence can occur to provide suitable targets for offenders. According to Felson & Cohen, the organisation of time and space is central to RAT as it helps to explain how crime occurs and what needs to be done about it. [14]

For RAT to be applied to the virtual environment, cyberspace needs to exhibit spatio-temporal characteristics that are compatible with those of the "physical world". Place, time, proximity and distance need to be identifiable features of cyberspace. [15] Indeed, the language of cyberspace is replete with references to space and place, such as "portals", "chatrooms", "sites", and "backdoors", which are all linked to information "superhighways" with "ports" connecting some parts of the internet to other parts. [16] There are differing opinions as to whether these terms are merely handy metaphors adopted to help make sense of an anti-spatial and non-linear environment, or whether they denote actual spatial qualities. [17] Cyberspace is perceived to be an environment which is always only one click away, because of how thoroughly interconnected it is; conventional barriers of geography and national borders are not significantly present in cyberspace. [18] This circumstance may suggest that the design of the internet is not compatible with the central requirements of space and time. However, cyberspace does possess certain redeeming characteristics.

While chatrooms and portals exist in the virtual space, the internet itself is physically rooted in the "real world" and produced in real space. [19] For example, 50% of the world's internet domains originate from the United States, as does 83% of the total web page views. The same inclusionary and exclusionary criteria, such as wealth, education, gender and ethnicity, which exist in the real world, structure access to cyberspace and usage of the internet. In other words, the capacity distribution of the internet reflects the social and economic hierarchies that exist in the real world. Thus, even though the internet is non-linear, it is profoundly spatialised. In short, the distribution of potential offenders and potential targets is not neutral, but dependent on the distribution of cyber resources and skills. [20] Russia, for example, has highly skilled hackers (motivated offenders in RAT terminology) who are responsible for a great majority of the world's spam. [21] Further, suitable targets are more likely to be found in Europe than in Africa because of the ubiquity of the internet and internet usage in the former.

3.2 A Suitable Target

RAT specifies the social conditions that need to be present for the successful commission of a crime to occur. As already stated, the theory says that for there to be a successful offence, there needs to be a motivated offender, a suitable target and an absent capable guardian. For purposes of this discussion, the question of a suitable target is of interest because it influences predatory action.

Target suitability consists of four constituent properties, namely, value, inertia, visibility and access, rendered by the acronym VIVA. The value of targets influences their desirability to offenders. Inertia refers to the mobility of the target, as determined by how big or heavy the target is, or whether it is attached to a lock, or whether the targets for personal violations may be able to resist. A target's visibility refers to the significant risk factor for being identified by the offenders. Finally, accessibility refers to the location of the target and how suitable it is for the offender to gain legal or illegal access to it for purposes of committing a violation, as well as the opportunities available for non-detection and escape. [22]

The constituent properties of target suitability, as expressed in VIVA, are discussed *individually* and in more detail below.

3.2.1 Value

The value of a suitable target will vary depending on how it is viewed socially and economically at a juncture. Value can be monetary or symbolic, for use or resale, and would include any prejudice, challenge or sexual gratification that the offender might obtain from the target or the victim. Currently, the majority of suitable targets for cybercrime take the form of information and digital code.

Property, for example, comes in the form of intellectual property, movies, music, trade secrets, computer software and so on. Property of this nature is increasingly more valuable to motivated offenders as potential targets for theft. [23] The range of targets may be extended in cases where the motivated offenders pursue suitable targets for trespass and criminal damage. The cybercrime case in point is "hacking", which would encompass the invasion of computer systems and websites, the distribution of malware and the damage caused by viruses and worms. [24] Additionally, individuals could be targeted for stalking or bullying, or because they are members of a religious, ethnic, racial or social group. As RAT examines criminal offences from the perspective of the motivated offender, the value of targets will depend on what the offender perceives as valuable. Broadly speaking, it may be concluded that, when it comes to determining the suitability of targets to the motivated offender, the valuation process varies as much in cyberspace as it does terrestrially. [25]

3.2.2 Inertia

As intimated above, inertia refers to the physical properties of the target. There is an inverse relationship between the suitability of the target and inertia, in that the suitability of the target decreases as the inertial resistance increases, and vice versa. [26] At first glance, this relationship between inertia and suitability would appear not to apply to virtual property because the targets of cybercrime, being digitised, seem weightless. Technological advances have allowed information to be downloaded and replicated seemingly instantaneously, with the obvious example being pirated information or property in the form of movies and music. However, closer inspection of the properties of the virtual environment indicates that the goods in cyberspace do retain some inertial characteristics.

Firstly, the volume of data can provide great resistance to suitability, particularly in situations where the internet connection is not sufficiently potent to commit the offence. Secondly, it is necessary that the motivated offender have appropriate tools to carry out his criminal plans. For instance, in order for an offender to be able to steal a significant amount of data, he will need sufficient storage, in the form of hard drive space, in which to deposit that data. Therefore, although virtual information may have relatively less inertial resistance as compared to terrestrial property, its weightlessness is not absolute. [27]

3.2.3 Visibility

RAT postulates that visibility, unlike inertia, has a positive correlation with suitability in that an offender must know that a target exists to offend. [28] Persons and property that are prominently visible are more likely to be targets. This relationship is somewhat more obvious terrestrially than in cyberspace where it may seem more difficult to conceptualise the visibility of a target. However, there is no lack of target visibility in the realm of cyberspace.

In the absence of tools such as closed ICT networks (for example, intranets and virtual private networks) that are designed to reduce access or hide the virtual presence of a user, the internet is inherently public. The internet is designed not to be limited by barriers of physical distance. This means that virtually present objects are globally visible and therefore suitable targets. This global visibility may operate to advertise the existence of the targets to the largest pool of offenders. [29] The popularity and interconnectedness of social media and social networks, for example, mean that more people are exposed more and can be targeted easily for cyberstalking and cyberbullying.

3.2.4 Accessibility

Accessibility also has a positive correlation with suitability. The easier it is to access the target and get away from the scene of the crime, the greater the suitability of the target. For terrestrial crimes, a house that is situated in a cul-de-sac generally is less accessible and less desirable than a corner house because the possibilities for escape without detection from a cul-de-sac are limited. [30] Accessibility is one of the attractive traits of cybercrime because traversing cyberspace is “non-linear”. This means that it is possible to jump from one place to another in a matter of moments and disappearing from the “scene of the crime” can be as easy as severing the connection with the network. [31] It is still possible, though, that the cyber offender can be detected by security features (for example, by an Intrusion Detection System) in the target network during the commission of the crime and subsequently traced back to his “home” network. However, there are many tools readily available to circumvent attempts to trace the offenders, including anonymous remailers, encryption devices, and the use of third party servers and systems. [32]

Accenture Plc, a company that studied the aftermath of the Sony hacks in 2014, has proposed that one of the steps that can help organisations is their ability to define cybersecurity success clearly by answering several critical questions. These include whether the organisation is confident that it has identified all the priority business data assets and their location; whether it can identify a motivated adversary; whether it has the correct tools and techniques to react and respond to a targeted attack; and whether it knows what the adversary wants. [33] These suggestions contain the core pillars of RAT and knowing what the suitable target is, determines what the appropriate responses from organisations, governments and industry ought to be. Once the criteria of suitable targets have been identified, how those targets are obtained by the cybercriminal become the next important consideration. It is here that the Gordon & Ford classification of cybercrimes becomes relevant.

4. Categorising Cybercrime

Cybercrime is a complex and relatively new threat as compared to terrestrial crimes. Hence it is necessary to understand cybercrime as a form of criminality in its own right. This means that, to tackle cybercrime successfully, it is important to determine where it fits into the criminal law in a way that does not simply comprehend its various forms as analogies of conventional crimes. While there may be a number of common characteristics between ordinary crimes and cybercrimes, such as the unlawful access to data or property, certain cybercrimes, by their nature, do not have “real world” counterparts amongst the conventional crimes. Furthermore, some cybercrimes encompass multiple factors and stages which may require different levels of legal responses to them.

Gordon & Ford propose an approach which would categorise cybercrime into two basic forms, namely, Type I and Type II, with a view to foregrounding the breadth of the issue.[34] They found that it is common for researchers to define the issue too narrowly, thereby limiting law enforcement capabilities. Their dual categorisation of cybercrime is designed to provide a conceptual framework within which lawmakers may create legal definitions which will vary across jurisdictions.

4.1 Type I Crimes

Type I crimes are more technical in nature than Type II crimes. From the perspective of the victim, Type I crimes are generally singular or discrete events that often are facilitated by introducing crimeware [35] programmes into the victim’s computer system. Usually, but not necessarily, the crimeware can be introduced because of vulnerabilities in the system. Examples of Type I crimes include phishing attempts, identity or data theft, and e-commerce or banking fraud facilitated by stolen credentials. [36]

Consider this example. Cassandra uses online banking and frequently shops online because she enjoys the convenience. She receives an email from her bank which informs her that they are updating their online banking system and they need their clients to verify their credentials. The email provides a link that she is requested to follow to complete the process. Cassandra, unsuspecting of any foul play, follows the link which sends her to the homepage of her bank. However, the page she sees is actually a clone of the real website; it looks identical to the original site so when Cassandra is prompted to type in her user ID and her password, she does so without hesitation. As she types in the details, they appear in plaintext to the cybercriminal on the other side, who copies them and gains access to her bank account. Cassandra completes the transaction without suspecting anything until her bank account is emptied three days later. This is what is known as a phishing scam. When it is viewed from Cassandra’s (the victim’s) perspective, it is firstly, a singular and discrete event and, secondly, its perpetration involved the use of crimeware. She has been the victim of a Type I cybercrime.

In this context, the email client was used to deliver the spam email. However, it cannot be classified as crimeware. In this instance, the real crimeware is the software that created the clone site of the bank and the keylogger software that stole the username and password.

4.2 Type II cybercrimes

Type II crimes exist on the other end of the cybercrime spectrum from Type I cybercrimes. They include, but are not limited to, cyberstalking and harassment, extortion and blackmail, child predation, complex corporate espionage and planning or online terrorism. Type II cybercrimes usually are facilitated using programmes that would not be classified normally as crimeware, for example, Instant Messaging (IM). Furthermore, these crimes generally are repeated events from the perspective of the victim. [37]

The following interaction between Amu and Basani best illustrates Type II cybercrimes. Amu and Basani met in an online chatroom dedicated to sharing views about the current state of African politics. Amu is very fascinated with the views that Basani presents and asks her to chat through a private chat. They exchange phone numbers and begin to chat privately. The conversations continue for some weeks and Amu begins to develop some romantic feelings for Basani. He searches for her profile on a popular social media platform. He realises from her profile that she lives in the same town as he does and asks her out for a date at a local restaurant. Basani is not impressed and promptly informs Amu that she is not interested in pursuing a non-academic relationship with him. Amu is disappointed but is convinced that he can manage to persuade her otherwise if he perseveres. He continues to message her in the chat and posts "romantic" material on her social media platform. He persists with this behaviour for months and escalates it to sending her inappropriate emails on a regular basis. He is not deterred by requests from Basani to stop the behaviour and does not respond to threats of pending police involvement.

At this point, subject to the definition of what constitutes stalking, these actions by Amu can fall only under Type II cybercrime. From the perspective of the victim (Basani) these actions are not isolated events and do not involve the use of crimeware. The tools that have been used by Amu thus far are ordinary and neutral because that were not created with the aim of committing cybercrimes but rather as mediums of communication.

The interactions between Amu and Basani, however, do not end there. Amu has above-average capabilities in the field of information technology and manages to acquire malware from the Darknet. The purpose of this malware is to allow Amu to gain remote access to the Basani's webcam while she is not aware. He introduces this malware into her system by sending her a spam email that requires her to click a link; she does so and downloads the malware. Amu then uses the malware to activate her webcam to take pictures of Basani in her bedroom while she is getting dressed. He uses the pictures to blackmail her into going on a date with him.

The introduction of malware presents a second dimension of the interaction between Amu and Basani. Essentially, the crime that is being perpetrated against Basani is still within the realms of Type II cybercrimes because it is largely still cyberstalking, blackmail and online harassment. However, the introduction of the malware provides a Type I cybercrime dimension because it is, firstly, a singular and isolated event from Basani's perspective (albeit within the context of prolonged harassment) and, secondly, it involves the use of crimeware. If legislators adopt this categorisation of cybercrime, they should adopt sentencing guidelines that will anticipate this kind of category overlap. In other words, if legislative sanctions provide for a five-year prison sentence for Type I crimes and 10 years for Type II crimes, Amu would be found guilty overall of committing a range of Type II crimes with consideration being given to the one Type I crime.

5. Cybercrime Categories and the South African Cybercrimes Bill

This paper is part of a doctoral thesis that seeks to analyse critically the South African Cybercrimes and Cybersecurity Bill. The Gordon & Ford categorisation can be a useful tool to confront the question of whether legislation can provide effective mechanisms to deal with cybercrime. What follows is a consideration of the South African cybercrimes Bill in the light of the Gordon & Ford categorisation.

The conceptual framework of the categorisation allows for a simplification the classification of the offences into Type I or Type II cybercrimes by asking two questions:

a) Is the act a singular or isolated event?
b) Is the act facilitated by crimeware?

If the answer to both these questions is yes, then the offence most likely is classifiable as a Type I offence and if the answer is no to both questions, it is most likely a Type II offence.

The South African Cybercrimes Bill provides for both Type I and Type II cybercrimes. Chapter 2 of the Bill, the offences chapter, provides for some Type I offences, namely, unlawful interception of data; [38] unlawful acts in respect of software or hardware tools;[39] unlawful interference with computer device, computer network, database, critical database, electronic communications network or National Critical Information Infrastructure;[40] unlawful acts in respect of malware; [41] unlawful acquisition, possession, provision, receipt or use of passwords, access codes or similar data or devices.[42]

The Bill provides also that these acts will not be unlawful if they are performed at the request of a person who has the authority to consent to their commission. It is interesting to note that the Bill makes this exception only for Type I offences. It is not immediately clear why this exception is provided only for Type I crimes but the exception suggests an implicit classification of cybercrimes into two types.

The offences provided for in sections 11, 12, 13 and 14 of the Cybercrimes Bill may be classified also as Type I cybercrimes, but they need to be understood as special cases within Type I. These crimes, namely, computer related fraud, [43] computer related forgery and uttering, [44] computer related appropriation, [45] and computer related extortion, [46] may be classified as computer enabled crimes. The concept of a computer enabled crime is defined to mean "the use of data, a computer device, a computer network, a database or an electronic communications network to commit a prohibited act". [47] It applies also to the offences in sections 15 and 16, although they, together with the rest of the offences in Chapter 2, are Type II offences. Section 15 prohibits computer related terrorist activity and related offences while section 16 prohibits computer related espionage and unlawful access to restricted data.

The offences in sections 17, [48] 18, [49] 19, [50] and 20 [51] do not meet the criteria to be classified under Type I cybercrimes and therefore ordinarily would fall under Type II. However, upon closer inspection, it would appear that, although they are computer enabled crimes, they may not necessarily constitute cybercrimes. It is at this point where the careful definition of cybercrime acquires paramount importance. What is certain is that cybercrime is a wonderfully complex matter that needs to be examined methodically and critically to find the best solutions to the problems that it poses.

6. Conclusion

The suitability of a target under RAT shows that targets can exist on a broad spectrum, from intellectual property, through information to actual human beings. Understanding who or what may constitute suitable targets is essential to understanding the motivations that criminals have for committing crimes. Once that understanding is obtained, the manner in which the targets are identified by the criminals is of equal importance. Determining this needs to be a systematic and disciplined exercise. The complicated nature of cybercrime does not allow for a nonchalant response from those who are tasked with confronting it. Categorisations such as those proposed by Gordon & Ford, when applied together with RAT provide a framework which lawmakers and law enforcement authorities can use to inform their decisions when criminalising and prosecuting cybercrime. Combating cybercrime cannot be reduced to a perfect science because it evolves so rapidly, but academics, particularly in the legal field, need to acknowledge and accept its technical nature and embrace the challenge. It is no longer sufficient to think about cybercrime and cybersecurity in an abstract and superficial manner. Rather, it is imperative to gain an understanding that will close the gap between the proliferation of cybercrime and effective responses.

The aim of this paper was to propose ways in which cybersecurity efforts can be strengthened. The South African Cybercrimes Bill was presented as a case study. It is suggested, however, that the approach presented here can be applied to any legislation or convention on cybercrime.

[1] Grobler (2012) 1.

[2] UNODC study (2013) xvii.

[3] Stander (2009) 223.

[4] Stander (2009) 224.

[5] Stander (2009) 224.

[6] Stander (2009) 225.
[7] Longe (2009) 155.
[8] Longe (2009) 156.
[9] Longe (2009) 156.
[10] Stander (2009) 217.
[11] Felson & Cohen (1980) 390.
[12] Yar (2005) 414.
[13] Felson (2008) 70.
[14] Felson & Cohen (1980) 147.
[15] Yar (2005) 414.
[16] Adams (1998) 88-89.
[17] Yar (2005) 415.
[18] Dodge & Kitchin (2001) 62.
[19] Yar (2005) 416.
[20] Yar (2005) 416.
[21] Krebs (2014).
[22] Felson & Cohen (1980) 393.
[23] Yar (2005) 419.
[24] Clough & Mungo (1992) 85-105.
[25] Yar (2005) 419.
[26] Yar (2005) 420.
[27] Yar (2005) 420.
[28] Bennett (1991) 148.
[29] Yar (2005) 121.
[30] Beavon et al. (1994).
[31] Newman and Clark (2003) 17, 63.
[32] Grabovsky and Smith (2001) 35.
[33] Accenture (2016) 4.
[34] Ford & Gordon (2006) 14.
[35] Crimeware is defined by Ford & Gordon as malware ie malicious software that is used (directly or indirectly) in the commission of the criminal act. It does not involuntarily enable the crime, meaning that its purpose is to commit a crime unlike a neutral device such as a USB stick that is manipulated to carry malware.
[36] Ford & Gordon (2006) 14
[37] Ford & Gordon (2006) 14.
[38] Section 5 of the Cybercrimes Bill.
[39] Section 6 of the Cybercrimes Bill.
[40] Section 8 of the Cybercrimes Bill.
[41] Section 9 of the Cybercrimes Bill.
[42] Section 10 of the Cybercrimes Bill.
[43] Section 11 of the Cybercrimes Bill.
[44] Section 12 of the Cybercrimes Bill.
[45] Section 13 of the Cybercrimes Bill.
[46] Section 14 of the Cybercrimes Bill.
[47] Section 2(1) of the Cybercrime Bill.
[48] Prohibition on dissemination of data message which advocates, promotes or incites hate, discrimination or violence.
[49] Prohibition on incitement of violence and damage to property.
[50] Prohibited financial transactions.
[51] Infringement of copyright.

References

‘Building confidence: Facing the Cybersecurity Conundrum’ High Performance Security Report (2016) Accenture.

Adams P ‘Network topologies and virtual place’ *Annals of the Association of American Geographers* 88 (1998) 88-106.

Bennett R ‘Routine activities: A cross-national assessment of criminological perspective’ *Social Forces* 70 (1991) 147-163.

Castells M *The internet galaxy: Reflections on the internet, business, and society* (2002) Oxford University Press.
Clough B & Mungo P *Approaching zero: Data crime and the computer underworld* (1992) Faber and Faber, London.
Dodge M & Kitchin R *Mapping cyberspace* (2001) Routledge, London.
Felson M & Cohen L ‘Human Ecology and Crime: A Routine Activity Approach’ *Human Ecology Vol. 8. No. 4* (1980).
Krebs B Spam Nation: The Inside Story of Organized Cybercrime- From Global Epidemic to Your Front Door (2014) Source Books Inc.
Longe O *et al.* ‘Criminal uses of Information and Communication Technologies in Sub-Saharan Africa: Trends, concerns and Perspectives’ *Journal of Information Technology Impact Vol. 9 No. 3* (2009) 155-172.
South African Cybercrimes and Cybersecurity Bill.
Stander A, Dunnet A, & Rizzo J *‘A Survey of Computer Crime in South Africa’* Proceedings of ISSA 2009 conference (2009) 217-226.
Yar M ‘The novelty of ‘Cybercrime’: an assessment in light of the Routine Activity Theory’ European Journal of Criminology vol. 2(4) (2005) 417-427.