BOOK CHAPTER | Cyberspace Policing

Policing the Cyberspace – Is the Peel Theory of Community Policing Applicable?

Wada, F., Longe. O.B. & Adelodun, F.O.
[1]University of West Hartford, West Hartford, Connecticut, USA.
[2]Academic City University College, Accra, Ghana
[3]The Polytechnic, Ibadan, Ibadan, Nigeria
E-mails: wada@hartford.edu, Olumide.longe@acity.edu.gh; adelodunfelicia@gmail.com

Abstract

The current model for policing and law enforcement as proposed by Peel in 1829 is based on four characteristics that shaped how conventional offline crimes are committed. The theory is founded on the fact that criminals and victims are proximate; there are limitations in the scale and extent of crime that can be committed per time; physical constraints such as planning the crime and visiting the crime scene prior to the crime poses a challenge to criminals; and the ability of law enforcement to profile or study the crime pattern can aid detection and apprehension. Although Cyber crimes share a few of the attributes of conventional crimes, it deviates completely in terms of its operation. For instance, cyber crime is automated, thus it has in its intrinsic nature, the potential to attack multiples of victims per time at different location. Spatial confinement is therefore negated as a means for detection and apprehension. Another interesting but disturbing phenomenon on the webscape is that cyber criminals can subtly turn their victims to criminals by hijacking (using anonymous proxies) their systems. Such systems are used to propagate the crime in order to reach more victims and escape detection. Crimes of this nature are committed across international boundaries, hence sovereignty of states are violated making prosecution extremely difficult. This paper takes a critical look at the Peel theory of policing in the context of cyber crime. We identified the Achilles heel in the model and make recommendations that will assist in scaling up the theory to be able to respond appropriately to the challenges of fighting crime in the information age.

Keywords: Cyber crime, Law Enforcement, Policing, Proxies, Peel Model.

Introduction

The definition of crime from different schools of thought varies as much as there are differing perceptions of the issue in different societies. For our discussion, we view crime as act(s) committed or omitted in violation of ethics, norms and (or) laws forbidding or commanding it and for which punishment is imposed upon conviction. These acts threaten social, economic, political and other social structure in a society. Crime could be against persons, organizations, institutions, states and even global.

Citation: Wada, F., Longe. O.B. & Adelodun, F.O. (2022). Policing the Cyberspace – Is the Peel Theory of Community Policing Applicable?
SMART-IEEE-ACity-ICTU-CRACC-ICTU-Foundations Series

Examples are theft, rape, assault, murder, fraud, arson etc. Crime has plagued societies from time immemorial and new forms of crimes evolve with societal advancement. Crimes such as terrorism, espionage, spying etc can implicate a society's relations with other societies and create international disorder and tension. Law enforcement remains a potent means for maintaining order and dealing with the crime problem in conventional society set-ups.Cybercrimes are crimes committed on the cyberspace using computer and networking technology provided by Information and Communication infrastructures. In a century where "everything" runs on the internet, cybercrime is a new wave of criminal activities that, if not controlled, threatens the very usefulness and survival of the cyber space as a tool for socio-economic development of nations (Chawki, 2009, Longe et al, 2009). The remaining part of the paper is organized as follows: In the next section we discussed the conventional crime control. This is followed by a section on the challenges of fighting cybercrime with the Peel Model of community policing. In the next section we present the Real-Time Cybercrime Response Model. The paper ends with recommendations for research and practice and conclusion.

2. Crime Control

Crime control refers to a theory of criminal justice that places emphasize reducing crime in society through increased police and prosecutorial powers and. Before 1829 crime control is based on social structures that:

(a) Use general societal condemnation of violations and the violators
(b) Exact punishment on affront and appease the victim
(c) Deter future violations by sanctions and new pronouncement appropriate to the instance or new instances or genre of crime
(d) Reconcile violators and victim(s)

The disorganization of primary societies, urbanization and increase in the scale of crime rendered this method in inadequate in dealing with crime on a large scale. In 1829 Rob peel came up with the current conventional model of law enforcement and policing.

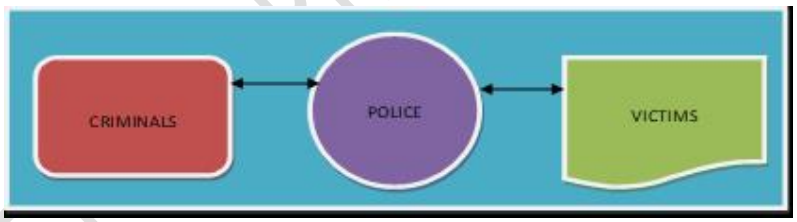


Fig. 1: The Peel Model of Community Policing

The bane of the Peel model of law enforcement is that it makes citizens assume minimal responsibility for crime and internal order. Citizens in the twenty-first century therefore see this as the sole responsibility of law enforcement agents and quasi-military police forces who maintain internal order by reacting to completed crimes (Brenner, 2006).

3. Characteristic of Real World Crime

Four characteristics of real-world crime shaped the way the way the Peel model approach the issue of crime and criminality. These are:

(a) Proximity between criminals and victims
(b) The scale of the crime
(c) Physical constraints that can discourage the criminal(s)
(d) Patterns of crime with which investigator are familiar.

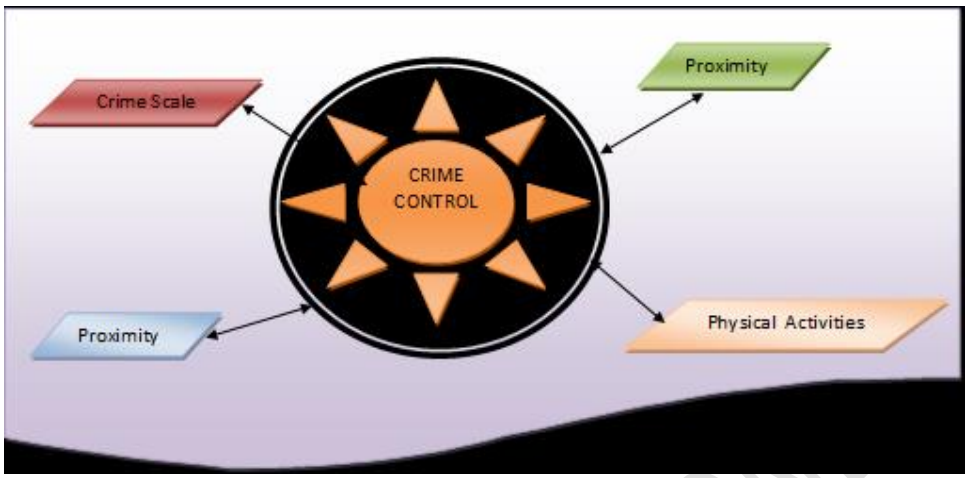


Fig 2: factors that shape the Peel Model of Law Enforcement

These facts can be explained by looking at how conventional crimes occur. Violators or criminals and their victims are usually physically proximate in most occurrences. Theft cannot occur neither is rape unless the victim and the criminals have contact. The extents of the crimes are limited by the number of criminals and victims. Also reality and distance can impose constraints on physical human activities such as breaking a safe room in a bank robbery, increasing the exertion and resources needed to commit crime thereby aiding the apprehension of criminals and contributing to evidence needed for prosecution (Brenner & Clarke, 2005). For instance, criminals can drop business cards or purchase receipts at the crime site unknowingly; they can even leave DNA evidence which can aid law enforcement in tracking them down. Demography and criminal profiling can contribute to apprehension and tracking criminals. For instance, there are certain forms of crime common to resource-poor environment or individuals while others can only be committed by economically vibrant individuals or organizations and economically advantaged individuals. . Spatial limitation is an aid to real world crime and the one-to-one relationship between victims and violators yields the assumption that crime is committed on a limited scale.

4. The Cybercrime Challenge

Cybercrime poses a lot of challenges to the Peel Model. These challenges are not more of adopting or creating new laws that criminalize certain cyber activities but more of law enforcements' ability to react to cybercrime. This is because cybercrime does not share some of the characteristics of conventional crimes that shaped the current Peel model of law enforcement. The cyberspace invalidates the very basic tenets on which the Peel Model is built. For instance in the cyberspace, the following statements are valid:

(a) No proximity is required between victims and violators. These crimes are committed, in various forms and guises, across continents. Anonimity is a factor on the cyberspace that the criminal use to their advantage.
(b) Cybercrime are faceless crimes unless the criminal chose to meet the victims as is the case with fraudulent cyber transactions, pedophiles and online pornography.
(c) One-to-one victimization therefore becomes invalid as the crime process is automated
(d) The criminal(s) can move from one location to another to beat the best internet address protocol location tools or to avoid phone call traces. They can engage a proxy server to mask or masquerade their actual locations.
(e) The criminal(s) can commit crimes against individual or individuals in multiple of places at the same time – therefore there is multiple victimization from multiple locations or from a single location.

(f) Therefore we have a one-to-many scenario in this case which clearly invalidates the conventional crime tenets.
(g) These criminal(s) can use systems and other unsuspecting people or organization systems' as zombies or detours without their knowledge thus incriminating other victims in the course of committing these crimes. This means victims can be turned to criminals even without their knowledge and further used to commit multiple crimes in multiple locations. This creates a chain effect and more victims through a singular event.

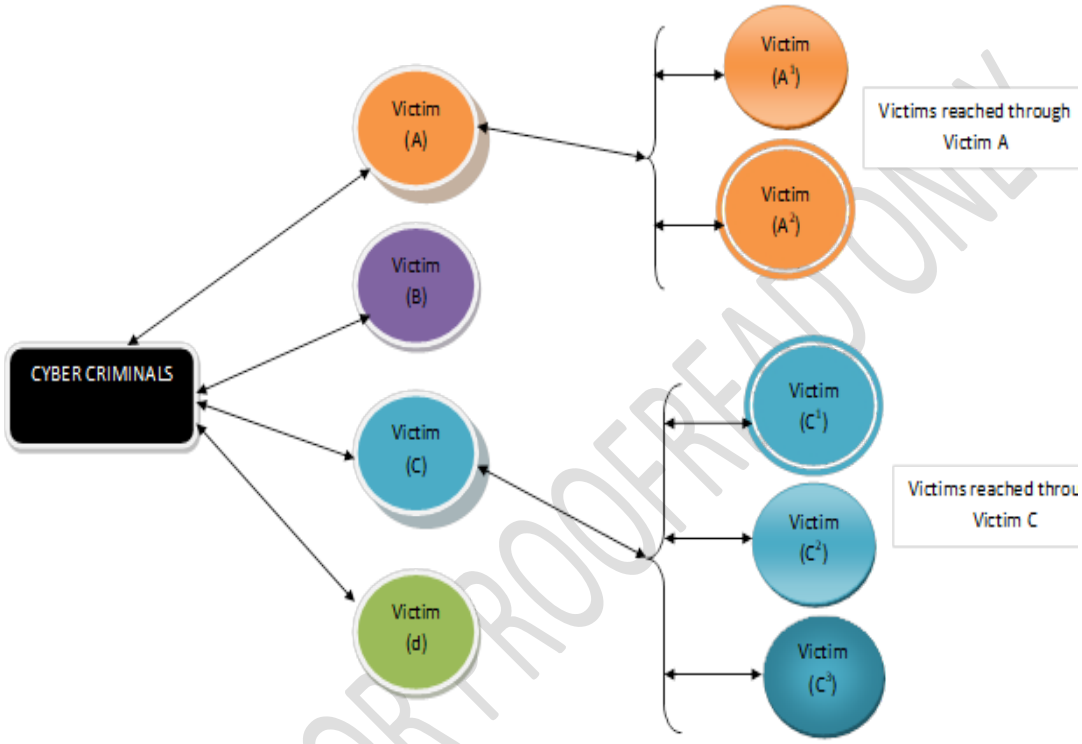


Fig 3: Multiple Effect of Reach of Cybercrime

(h) In cybercrime, **the theory of pseudo-resource ownership** is established as the cybercrime scenario since these criminals posess the potential to defraud individuals and organizations of different kinds of resources without their knowledge while such individuals or organizations still hold the physical or evidence that the resources is still in their possession. This is the case when credit card information are hacked and funds transferred in sequence out of such accounts over a period of time without the owner of such account suspecting any foul play since the so called cards and the security or pin numbers are still in "their possession".

From the forgoing, it is obvious that the current model of law enforcement cannot effectively militate against cybercrime as cybercrime deviates in nature, radically, from the characteristics of conventional crime. Anonymity, jurisdiction of law, the pseudo-resource ownership theory, global reach and multiplication of crime and its victims in multiple locations posses a great challenge to the application of current policing strategies to address cybercrime.

Fig. 4: Localized Crime Response

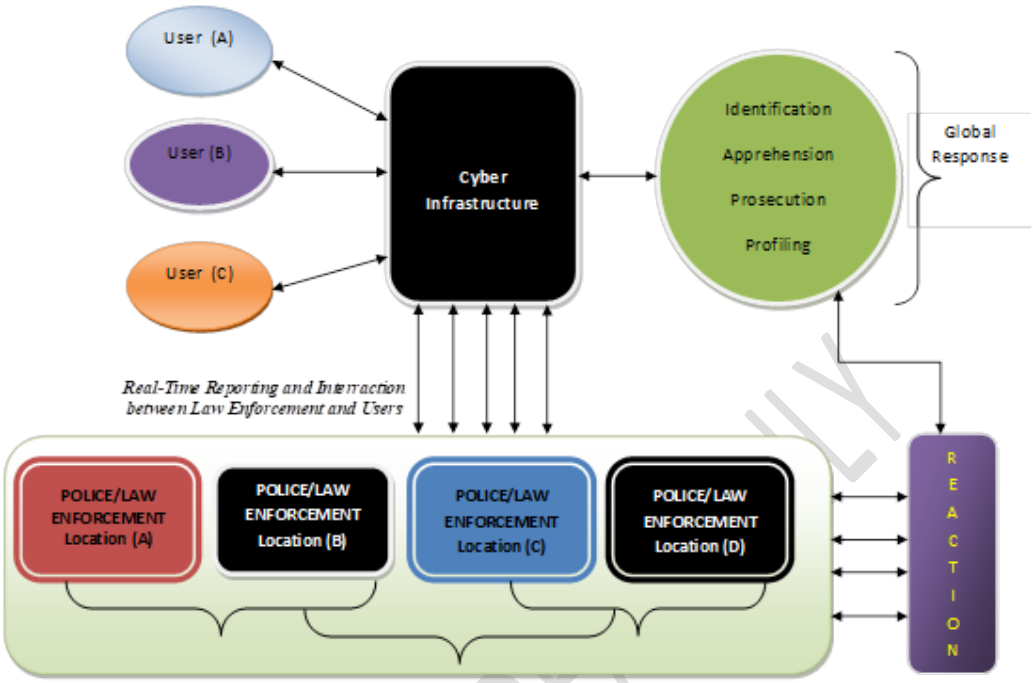
The response of law enforcement to conventional crime is subtly patterned after how the military responds to external aggression. Law enforcements effectiveness is aided by the stochastic but localized occurrence of these crimes. Unfortunately, technology, especially the internet, now necessitates the need for a paradigm shift from policing concepts and models that focused on localized crime to those that can deal with crimes that radically deviate from the localized trend. Technology has produced a new social structure that flattens conventional crime structure thereby eroding the boundaries between internal and external threats.

5. Our Model

Our opinion is that, amongst other, in the efforts to fight cybercrimes, users must be empowered as the last line of defense as compared to the Peel model where the most responsibility rests on the Police and other law enforcement agents. We propose a User-centric socio-technological model that employs technology, social theory, policy and education (awareness) as tools to mitigate the cybercrime problem. This model offers an interactive real-time challenge-demand-response platform that aids identification, reporting, apprehension and prosecution.

Our model takes into consideration the fact that cyber crime does not share the common characteristics on which the *Peel theory* rests and that the criminals plug into the webscape through remote proxies. The model provides valves that assist users identify malicious intentions through a multi-level access control mechanism. We employ the cyber infrastructure as a tool that can provide synergistic interactions between users and law enforcement. These infrastructures consist of the user interface, web browsers, the ISP etc. We propose that ISPs should send report about suspicious traffic to law enforcement and e-mail interface should have facilities that can automatically connect users to law enforcement to report suspicious cyber invasion and criminal activities.

Infact, users should be empowered through e-mail interfaces to report phishing. Scamming and other cyber violations in real-time. Law enforcement should be connected through a distributed network such that cyber criminals can be tracked anywhere in the world thus providing a global response. The reaction to information input into the system will create an effective mechanism for tracking, identification and apprehension of cyber criminals.



6. Recommendations For Policy And Practice

Cyber crime has added to the dilemma of the Peel theory for crime control. Though another form of crime, it does not have a one-to-one mapping nature to conventional crimes nor does it share the common characteristics on which the Peel theory rests. The ubiquitous nature of the web coupled with the cloud of users presents a new form of challenge to system security and demand a paradigm shift in the perception, design and implementation of security measures (Straub & Welke 1998, Schlienger & Teufel 2002).

"Most people envision cybercrime looking like the movies, where slick tech geniuses sit behind keyboards writing elaborate programs to outsmart major computer networks" (ANU, 2018). Quoting the United Nations Office on Drugs and Crime:

> *"The Internet and the criminal behaviour it transforms (cybercrime) pose considerable challenges for order maintenance and law enforcement because Internet-related offending takes place within a global context while crime tends to be nationally defined. Policing cyber-crime is made all the more complex by the very nature of policing and security being networked and nodal and also because within this framework the public police play only a small part in the policing of the Internet. In this paper it is argued that the future of the public police role in policing the Internet is more than simply acquiring new knowledge and capacity, but it is about forging new relationships with the other nodes within the networks of Internet security. These relationships require a range of transformations to take place in order to enhance the effectiveness and legitimacy of the nodal architecture. It will then be argued that some of the contradictions faced by 'the police' are being reconciled by the gradual reconstitution of a neo-Peelian paradigm across a global span, which brings with it a range of instrumental and normative challenges" (Accessed March, 2022 - https://www.unodc.org/e4j/data/_university_uni_/policing_cybercrimes_situating_the_public_police_in_networks_of_security_within_cyberspace.html?lng=en*

But oftentimes, the truth can be as simple as criminals tricking users into clicking on web links contained in clever but fake emails from familiar companies that promise free gifts, seek to help fix your "full" email inbox or track bogus packages being delivered to your home.

Unfortunately, Internet security and web design issues have continued to toe the lines of previous approaches that concentrated on technicalities and usability without scaling security issues in the light of today's challenges thereby providing a fertile ground for cyber crime to breed. To secure the internet from cyber crime and other abuses, users must not only be made aware of the existence of security flaws and vulnerabilities on the webscape, they must be empowered in a holistic manner through design, policies, practices and technology to mitigate against these risks and to understand the criminals. The performance of such protective schemes and policies must also be measurable as this will provides the basis for enhancements and improvements. Law enforcement must also be willing to revisit its mechanism for reporting, apprehension and prosecution in the light of emerging technologies, issues and concerns. Ignoring this important

7. CONCLUSION

The challenge in fighting cyber crimes stems from the fact that cyber crimes have been in existence for only as long as the cyber space exists. This explains the unpreparedness of society in general towards combating them. We have shown in this paper that the Peel model of community policing suffer some inadequacies with regards to facing the challenges posed by cybercrime. The Internet community must engage in a collective effort to curb the Internet of the demeaning crimes it is helping to fuel. We ignore these important issues at our own risk.

Acknowledgement

The author acknowledges the contributions and inputs of Longe Olumide (PhD) to the scientific contents of this work as well as permission to use some of his previous models for the study and assessment of cyber crime and criminality.

EndNote

A version of this work had appeared in the Computing & Information Systems Journal

References

1. Australian National University – ANU (2018): Policing the Cyberspace: https://regnet.anu.edu.au/news-events/news/7187/policing-cyberspace
2. Chawki, M. (2009). Nigeria Tackles Advance Free Fraud. *Journal of Information Law & Technology* (2009) No. 1. Retrieved January 12, 2010 from http://go.warwick.ac.uk/jilt/2009_1/chawki>
3. Brenner, S (2004). Distributed Security: A New Model of Law Enforcement. *John Marshal Journal of Computer and Information Law VOL. XXIII* . 2005. (4) . Retrieved December 2, 2009 from http://www.jcil.org/journal/articles/434.html
4. Longe, O., Osofisan, A., Kvasny, L., Jones, C. and Nchise, A. (2010). "Towards A Real-Time Response (RTR) Model for Policing the Cyberspace", Information Technology in Developing Countries, Vol. 20, No. 3.
5. Longe, O.B. & Osofisan, O.A. (2011). On the Origins of Advance Fee Fraud Electronic Mails: A Technical Investigation Using Internet Protocol Address Tracers," The African Journal of Information Systems: Vol. 3: Iss. 1, Article 2. http://digitalcommons.kennesaw.edu/ajis/vol3/iss1/2
6. Longe, O., Ngwa, Wada, F., Mbarika, V. & Kvasny, L. (2009). Criminal Use of Information and Communication Technologies in Sub-Saharan Africa: Trends, Concerns and Perspectives. Journal of Information Technology Impact, Vol 9, (3). www.jiti.net
7. Straub, D. W., and Welke, R. J. (1998). Coping with systems risk: security planning models for management decision making. MIS Quarterly, 22(4), 441-469.
8. Schlienger and Teufel, 2002 Schlienger T, Teufel S. Information security culture – the socio-cultural dimension in information security management. In: IFIP *TC11 International Conference On Information Security*, Cairo, Egypt; 7–9 May 2002.

9. United nations Office on Drugs and Crime: Policing the Cyberspace Situating the Public Police in Network of Security Within Cyberspace. *Accessed March, 2022 - https://www.unodc.org/e4j/data/_university_uni_/policing_cybercrimes_situating_the_public_police_in_networks_of_security_within_cyberspace.html?lng=en*
10. Nahn, J (2007): Policing Cyberspace: A Structural and Cultural Analysis https://www.ojp.gov › ncjrs › virtual-library ›