An Examination of Barriers of Criminal Information Sharing Between Law Enforcement Agencies and Their Effect in Crimes Management in Nairobi County, Kenya

Lucy Wangari Kamau, Wokabi Mwangi, and Panuel Mwaeke

Abstract — The paper examined barriers of criminal information sharing between law enforcement agencies and their effect in crimes management in Nairobi County, Kenya, using data from an MA Thesis. This study was guided by four objectives; to examine the types of criminal information that is shared among law enforcement agencies; to assess the individual, organizational and technological barriers that hinders sharing of criminal information among law enforcement agencies in Nairobi County, Kenya. This study was guided by Social Exchange Theory as propounded by Homans in (1958). This study adopted a qualitative study design and non-probabilistic sample design paradigms. The main method of data collection was the interview. Interview schedule and key informants guide were used to collect data. A sample comprised of 47 law enforcement officers purposively selected from Directorate of criminal Investigation (DCI) Operation wing and the Kenya Police Service Headquarters operation wing. In addition, 10 Key informants were also purposively selected and interviewed to inform the study. Both individual barriers, organizational and technological barriers affected criminal information sharing among law enforcement agencies. Major individual barrier was competition for credit between the agencies in achieving positive outcomes which was perceived to have a backlash on security operations. Other individual barriers included the deeply entrenched culture of secrecy and the need-to-know rather than the need to share policy. Major organizational barriers include Mistrust of other organizations (89.1%), Organizational culture such as culture of secrecy (83.2%). Major technological barriers included both intra and inter-information technological gaps exacerbated by wanting levels of information technology skills. The barriers were perceived to cause ‘linkage blindness,’ where the information available in one agency is not available with other law enforcement agencies affecting remarkable achievement of outcomes. As a policy measure, the study recommended speedy removal of criminal information barriers at all levels and fast mitigation on both intra and inter-organizational information technological skill gaps. The deeply entrenched culture of secrecy and the need-to-know rather than the need to share information policy should further be revisited and dealt with. Finally, there is an urgent need for National-wide Criminal Information Management System with certain rights for all law enforcement agencies. The use of a database will reduce the technological barrier since criminal information will be made accessible to all the agencies.

Key words — Individual barriers; Organisational barriers; Technological barriers; Linkage blindness.

I. INTRODUCTION

The 21st century is fraught with innumerable challenges some that have been with humanity for eons while others are either emergent form of crime of mutating forms of criminal acts ranging from terrorism to organized crime and entrepreneurial crime in all form. Globally the safety and security of persons has been persistent issue and it has been subject of United Nation Reform process [1]. According to the report by the U.S. Department of Justice [1], establishing public safety is among government’s fundamental obligations to its citizens. According to the report, the safety of a person and security of one’s property are widely viewed as some of the basic human rights and are essential to the community’s overall quality of life. Consequently, every democratic state has a constitutional mandate to guarantee and defend personal rights and freedoms as per US, [2], Kenya Constitution [3]. Largely, this has been the preoccupation of law enforcement agencies of state organs. Undeniably, the security of a country is crucial as it determines an important framework for socio-economic and political development. Attention to preparedness of many states to deal with insecurity has been wanting because of uncoordinated efforts of law enforcement agencies due to what this study attributes to be barriers of criminal information sharing.

In comparison, suspect the news and knowledge of law enforcement agencies is literally the blood of evil conduct, principles and cultures alongside dysfunctional systems, technology, strategies, and policing procedures [4], [5] continues to hinder the exchange of information and knowledge within and within police forces and other organizations. This is demonstrated by a recent study of Best Jr's 9/11 terrorist attacks [6]. The report states that the paradox of exchanging classified information and risk management as well as different information cultures, technology and strategies is a blind "coupling the dots" for law enforcement agencies and intelligence agencies. Comparably, Campbell [7] reports on the sharp criticism of the Canadian legal compliance agencies for information and knowledge-sharing practices and procedure defects; the Bernardo Investigation Review [7], the AIF 182 Commission [8] and the Miss Air India Bombing Commission [9]. The police were charged with these three incidents for their inability to coordinate and collaborate across jurisdictions, their inadequate processes, and mechanisms for promoting knowledge and information, and for personal and
organizational principles and prejudices blocking accurate, productive information and the exchange of knowledge both inside and outside the police intelligence arena.

According to the US Office of Homeland Security [10], insecurity has become a worldwide threat. Additionally, Lake and Morgan [11] have stated that America is increasingly strategic in the African context, at a moment when a broad spectrum of security challenges dominate the security landscape, including the emergence of militia groups and armed gangs, insurgency, drug trafficking, maritime threats such as Indian Ocean pirating and oil bunkering in the Gulf of Guinea. Organised criminal activities are highly brazen and damaging, in particular abduction, human trafficking and trafficking in persons, arms smuggling, environmental and financial crimes. These are not alone, but rather a vicious circle: Irregular threat dynamics for Africa maintain black markets directly linked to corrupt states, distract attention from attempts to democratize, generating or fueling civil wars, leading to the fall of states, and creating safe havens for terrorists and more criminals, as per [12], [13].

According to Chappell [13], the majority of African countries face emerging security challenges that are likely to exceed their existing or feasible internal and military compliance capabilities. Although, in the future African governments will need to increase national protection, although threats such as Islamic extremism can require foreign military assistance, particularly in Sahel and the Horn of Africa. This may require intra and inter-sharing of centralized criminal information in or between its agencies [10].

Baylis, Wirtz and Gray [14], argued that like many other African countries, Nigeria suffers from severe safety challenges that result in thousands of deaths and incalculable social harm. Indeed, in a radical Islamic group members are gaining more ground and are becoming too disturbing the precarious state of Nigeria has seemingly become permanent as Boko Haram attacks are committed. In the East African area, numerous disturbances have occurred. There have been various threats, from one of Rwanda's most recent darkest genocides, two decades of conflict in Somalia, radical shootings of innocent civilians at the Westgate Mall, to pirate attacks off the coast of the African horn. There are a variety of safety issues in East Africa. However, to grasp these enormous obstacles in this region, at times in a state of perpetual emergency, one should look at the past of these countries and why radical jihadist groups now pose the greatest challenge in the area, with base camps in southern Somalia.

Homeland conflict[s] have generated refugee flows and trans-frontier streams of army rebels in Sudan and Somalia, regionalizing what had once been internal violence [11] and thus, the threats to security within the state have become decentral threats. The failure of certain countries to respect the sovereignty of their neighboring nation leading to political intervention in one another's internal affairs has led to instability in the region. Examples of this are Rwanda and Burundi. Rwanda is tired from Burundi’s turmoil and its effects are already strong in Rwanda. Rwanda only intervenes to ensure that its state's security is secure [15]. According to Lake and Morgan [16], in every region of the world there are its own characteristics and problems – in East Africa, what may work to end conflict or threats to Eastern Europe does not work, "every region needs its own theory". It is also very critical that we consider the root cause and risks which can be alleviated as ways of finding solutions.

Ethnic wars in the region of Eastern Sudan have been a grave cause of instability. A study published in 2014 by the British Broadcasting Company (BBC) shows that the two major ethnic groups, Dinka, and Nuer, combine oil and power. However, Al-Shabab terrorist activity appears to be the largest threat in the area. In September 2013, the terrorist group preaching a radical version of Islam took responsibility for the incidents of a number of civilian deaths, for instance the attacks at the West Gate Mall in Nairobi, Kenya. In response to Kenya's military operations in Somalia, the Somali group says "that it has carried out the strike" [17].

The NCIC database [18], and a locator file for missing and non-identified persons may be best described as a computerized index of information on recorded criminal justice for crimes or offenders of national interest. Before these criminal record systems come to light, individuals in these countries may be able to avoid their criminal history and begin a new life in another city, city, or state. In reality, the IT revolution and the criminal record and database systems have transformed society into a kind of city life in which crime can be practically tracked.

This study further acknowledges that more critical debates are apparent with the complexities and challenges around the sharing of information and knowledge. This is a theme that has been involved in many of the law enforcement and police practice and research developments over the last few years. First, studies of police organization structure have highlighted how fragmented, bureaucratic institutional forms can stifle the flow of information around police services and occupational culture research has suggested how sub-groups (e.g., frontline patrol officers) can be disinclined to share information with other sub-groups (e.g., detectives) as per [19]-[21].

Second, the introduction of new technologies over the years from two-way radio to computerised record systems, surveillance technologies and mobile computing solutions are continuing to transform law enforcement. Although assumed to improve productivity and efficiency, there are indications that technologies can reduce officers’ time spent on street-level activities due to the added requirements of completing and maintaining records [22], [23]. Related issues here include the tension between the desire to gather ever-increasing amounts of information and being faced with the massive task for sorting through and prioritising the collected data, therefore driving the development of new knowledge and information management systems [4], [24], [25].

Third, there are increasing knowledge linkages between police and non-police organizations when dealing with crime and security issues. Ericson and Haggerty [26], make the argument for an expanding 'surveillant assemblage' where law enforcement agencies are now able to access records from insurance, educational, financial and telecommunications institutions and sometimes vice versa. Furthermore, global trends are showing a change in the governance of policing with non-police organizations increasingly taking over security roles [27]. The challenge here therefore becomes how and what information is
coordinated between police and external security organizations. The need for better police collaboration with external agencies in the fields of probation, forensics, health, and law has also been highlighted by recent research [28].

Fourth, a linked issue is the conception that we are moving towards a society where there is greater assessment and management of risk and hence where there is much greater collation and dissemination of data on individuals. Jones and Newburn [29], describe this in the context of comparative national policy changes regarding sharing information on location of sex offenders with local communities. Fifth, there is an increasing movement towards transnational law enforcement where international bodies (e.g., Interpol, Europol) co-ordinate operations across sovereign borders or where law enforcement agencies in different countries directly work with each other to build an integrated understanding of security issues such as human trafficking [28], [30]. The Schengen Convention of 1990 and the 1991 Maastricht Treaty are examples of agreements which formally introduced the principles of greater co-operation between law enforcement agencies. However, Sheptycki [25] critically discusses how expanding international policing networks face problems of information silos within organizations while also pointing out the downside of the threats to civil liberties resulting from cross-border knowledge sharing of data on individual citizens. Sixth, at a higher level, Dolowitz, and Marsh [31] consider how lack of knowledge regarding policy content and the economic, political, and ideological contexts in which they originate can influence the success of policy transfer from one domain to another. For example, Jones and Newburn [29] discuss how lack of contextual knowledge affected the transfer of sex offender registration policies between the US and the UK. These types of themes therefore highlight how knowledge sharing in the future is only going to increase in scale (e.g., due to the growing impetus to collect more information as part of an enhanced risk management environment and greater citizen mobility) and to do so in increasingly complex inter-organizational and international contexts.

To improve information sharing, law enforcement agencies are centralizing their services through the implementation of shared technologies (such as mobile data terminals [MDTs], computer aided dispatch [CAD] systems and records management systems [RMS]). According to Versa term [32] private high-tech companies are taking this opportunity to design new IT and RMS to improve information sharing and collaborative policing by making summary ‘criminal and non-criminal information readily available to all agencies. Many of these advanced technologies have been readily accepted and implemented with little analysis into their ability to address the problem of inadequate information sharing and fragmented policing [33]. Yet, government and municipal investment in policing innovations that fail to address the problem of information sharing not only constitute waste and reflect inadequate governance, but more importantly affect emergency preparedness and public safety. As such, “there is a need for an informed analysis of the relationships between the situational aspects of work, the institutional context of work and the use of these technologies supporting law enforcement work’ [34].

II. PROBLEM ANALYSIS

The security of a country is crucial as it determines an important framework for socio-economic and political development. Nevertheless, in particular, Africa and Kenya face new security challenges that are likely to go beyond their existing and feasible national and domestic compliance capability. Previous studies indicate that preparedness of many states to deal with insecurity has been wanting because of uncoordinated efforts of law enforcement agencies due to what this study attributes to be barriers of criminal information sharing. This study assumes that these barriers exist at individual levels, organizational levels, and technological levels. In addition, though previous scholars have researched widely on the problem of insecurity, the barriers of criminal information sharing between the law enforcement agencies and its and their effect in crimes management in Nairobi County, Kenya have not been subject of any systematic investigation and documentation. This study sought to examine barriers of criminal information sharing between law enforcement agencies and their effect in crimes management in Nairobi County, Kenya. The study sought to investigate and fill this apparent knowledge gap.

III. METHODOLOGY

This study adopted the use of cross-sectional descriptive survey design. The design is preferred for studies where subjects respond to a series of statement or questions in a questionnaire or an interview concerning variables that are measured at a specific point in time for a defined population [35]. The definition survey is perfect for collecting information on people's views and behaviors, beliefs, habits, and a variety of social matters [36]. Purposive sampling was used to collect data from 47 respondents who participated in the study. The main method of data collection was the interview.

IV. RESULTS AND DISCUSSIONS

A total of 47 duly filled and usable interview schedules out of 60 were obtained from respondents for the study. This represented 78.3% response rate and a non-response rate of 21.7%. According to Mugenda and Mugenda [37], this was sufficient for doing the analysis. Unless otherwise mentioned, the sample size of all tables and graphs provided in this chapter is 47. In that same respect, some tables have a total response of more than 47, which is multiple answers (where respondents were required to give more than one response).

A. Demographic Information

This section presents demographic information of respondents namely: rank of police officers and gender of respondents.

B. Rank of Officers

The ranks of respondents who participated in the study were as shown in Table I below.

C. Respondents’ Years of Service

On average, the police officers that participated in this survey were fairly experienced having served in the police service for 8.5 years. Some of them had served for two years while others had served for more than two decades as shown in Table II.
TABLE I: RANK OF RESPONDENTS

<table>
<thead>
<tr>
<th>Rank</th>
<th>Frequency</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Constable</td>
<td>18</td>
<td>38.2</td>
</tr>
<tr>
<td>Corporal</td>
<td>11</td>
<td>23.6</td>
</tr>
<tr>
<td>Sergeant</td>
<td>9</td>
<td>18.2</td>
</tr>
<tr>
<td>Inspector</td>
<td>4</td>
<td>9.1</td>
</tr>
<tr>
<td>Chief inspector</td>
<td>3</td>
<td>7.3</td>
</tr>
<tr>
<td>Superintendent</td>
<td>2</td>
<td>3.6</td>
</tr>
<tr>
<td>Total</td>
<td>47</td>
<td>100</td>
</tr>
</tbody>
</table>

Source: Primary data (2021).

TABLE II: RESPONDENTS’ YEARS OF SERVICE

<table>
<thead>
<tr>
<th>Years of service in Kenya police</th>
<th>N</th>
<th>Minimum</th>
<th>Maximum</th>
<th>Mean</th>
<th>Std. Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid N (list wise)</td>
<td>47</td>
<td>2</td>
<td>25</td>
<td>8.56</td>
<td>3.591</td>
</tr>
</tbody>
</table>

D. Gender of Respondents

There was a near parity in the gender distribution of respondents who participated in the research as shown in Fig. 1.

E. Types of Criminal Information that is Commonly Shared Among Law Enforcement Agencies

First, the study sought to establish whether law enforcement agencies shared criminal information amongst each other. Besides, the study also examined the types of information shared. The nature of criminal information sharing is presented in Fig. 2.

The study confirmed criminal information sharing and reciprocity albeit based on the need to know. As shown in Fig. 2, most of the information shared among law enforcement agencies especially in Nairobi was about criminal movements (72.7%). This was followed by information on missing persons (70.9%), gang information (61.8%) and terrorist links (60%). Moreover, 58.2% of the respondents reported that gun information was shared among law enforcement agencies. This include incidences where a gun has been used to commit a crime in addition to information about the legal owner of the gun. However, this information was said to be shared only upon request. Only the DCI or national police service (NPS) are given such kind of information who based on the need to know circulates information to other agencies.

In addition, other pieces of information shared among law enforcement agencies were reports on previous convictions (54.5%), drugs and drug related information (41.8%), wanted persons (29.1%) as well as information on dangerous criminals (9.1%).

Importance of Criminal Information Sharing Among Law Enforcement Agencies to the Management of National Security

The study further sought to establish the importance of sharing criminal information among law enforcement agencies to the management of national security. The main benefits highlighted are highlighted in Fig. 2.

As exhibited in Fig. 3, sharing information serves to increase knowledge available for decision making as was reported by 90.6% of the respondents. This helps to recognize not only which criminals to target but can also solve lower risk cases in an era of resource constraints. It may also help to avoid "blindness links," where there is no information available in one of the departments of law enforcement agencies. As one of the Key informants stated,

“The consequence may be the full scope of crime that goes beyond the limits of law enforcement”. This is sometimes common in the system, and also explains why law enforcement agencies are sometimes only reactive than proactive in preventing any form of insecurity.”
Linkage blindness was a problem where a number of intelligence agencies hold information on the activities of those involved in crime or criminal activity but fail to connect the dots. Information sharing among law enforcement agencies was said to support de-confliction (as reported by 81.3% of the respondents) or duplication of roles where more than one law enforcement agency is simultaneously investigating the same individual or group. Information sharing under these circumstances can result in savings in time and resources for each agency concerned by preventing duplication of effort. In addition, law enforcement information sharing can also result in greater achievement of outcomes than would be possible for a single agency working alone. This was as reported by 73.7% of the respondents.

The study noted, absence of a single integrated information sharing mechanism is long overdue. One of the key respondents, further, stated:

“This is an information system or Centre that routinely collect relevant information and make it accessible widely to the authorized users on a timely and safe basis is a fundamental component of successful nation-wide criminal information sharing”.

All the critical sources of valuable information that is reliable, timely, and full for law enforcement officials around the country are records of criminals’ backgrounds, law enforcement statistics, records of judicial proceedings and rulings, and databases of identified and suspected terrorists. As another key informant stated:

“It is becoming more and more necessary to pull together pieces of knowledge from many different sources in a criminal enterprise marked by an increasingly sophisticated crime”.

It was further reported that, today, large numbers of police work now include data patrolling, and much of this goes beyond the local or even national level' like 'patrolling' information from, law enforcement agency, government department, financial agency and the telecommunications industry. In relation to knowledge collection and exchange, enormous operating procedures have since been carried out.

Another respondent stated:

“In order to conduct immediate investigations to minimize such risks, law enforcement officers are more easily able to transfer information to the appropriate agencies. Confidential data sharing or exchange can be boring if cooperation, confidence, and strong leadership are absent. However, collaborative efforts have been made, which have created positive outcomes in the countered-terrorism practice”.

Individual Barriers of Criminal Information Sharing Among Law Enforcement Agencies

The study also sought to assess the individual barriers hindering sharing of criminal information among law enforcement agencies. When the respondents were asked to state the individual barrier that they thought hinder information sharing, they reported barriers as presented in Fig. 4.

Based on the Fig. 4, competition was cited as one of the major factors hindering information sharing among law enforcement agencies as was reported by 20% of the respondents. This entails organizational concerns of competing for credit overachieving positive outcomes. For instance, if sharing information is expected to enhance the reputation of another agency (organizational pride) which could ultimately result in additional resources for that agency, a decision may be made to withhold that information. According to the study, this may lead to filtering of the information they provide to others, thereby providing only some of that which is available albeit at the detriment of the common good (prevention of insecurity).

According to the study, information sharing was affected by the need-to-know policy, as opposed to a need-to-share policy. This means that an agency may judge whether its information has utility for another agency, rather than the recipient agency having an opportunity to evaluate that information for itself. Similarly, some agencies such as the NIS have cultivated the culture of secrecy. This is associated with the need-to-know ethos. In this regard, there may be a general fear of sensitive information that could do harm to society getting into the wrong hands, leading to a no sharing default position.

Organizational Barriers of Criminal Information Sharing Among Law Enforcement Agencies

The study also sought to establish the organizational barriers of criminal information sharing among law enforcement agencies in Nairobi County. According to the study, 83.2% of the respondents indicated organizational culture hindered reporting of information. Notions such as ‘information is ours and not theirs” came to the fore. According to the study, 10 % of the respondents there were also pockets of mistrust. This may be explained by organizational pride that seems to affect criminal information.
sharing. According to the study, the culture of knowledge sharing is a key success factor.

Rather than partnering with other departments, there may be a temptation to concentrate internally on developing intelligence holdings. This builds a network of silted intelligence holdings and decrease the likelihood of synthesizing information from different sources.

Technological Barriers of Criminal Information Sharing Among Law Enforcement Agencies

Last but not least, the study sought to assess technological barriers they thought hinder criminal information sharing. This is because technological barriers have long plagued attempts by law enforcement agencies to share data. The highlighted technological barriers were as presented in Fig. 5.

Based on the results in Fig. 5, the main technological barrier such as lack of adequate IT experts (reported by 68.3% of the respondents), rapidly evolving IT space seemed to limit the ability of the officers to share and/or even retrieve information from other sources that can be useful to nabbing the criminals. This barrier was also mentioned during the key informant interviews where the informants revealed that the major problem affecting this information transfer is the tendency of law enforcement officers to recruit people with inadequate IT skills. As one respondent stated:

"Today, almost every crime has a digital dimension. Agencies are adapting to a technologically knowledgeable workforce and their leaders should welcome the transition and ensure that they recruit and represent a successful result."

For crimes such as identity theft, cyber stalking, misuse of chat rooms, and impersonation, Kenya has no clear provisions. It was also indicated that the 2013 Kenya Communications (Amendments) Act does not address cyber-crimes executed against a person. Incompatible IT structures (reported by 61.7% of the respondents) was said to impede knowledge flow between organizations.

V. CONCLUSION AND RECOMMENDATION

The study revealed barriers of criminal information at three levels: individual, organizational, and technological. Major individual barrier was competition for credit between the agencies in achieving positive outcomes which was perceived to have a backlash on security operations. Other individual barriers included the deeply entrenched culture of secrecy and the need-to-know rather than the need to share policy. Major organizational barriers include mistrust of other organizations (89.1%), Organizational culture such as culture of secrecy (83.2%), Conflicting organizational goals (78.5%) and Organizational pride (67.4%). Major technological barriers included both intra and inter-information technological gaps exacerbated by wanting levels of information technology skills. The barriers were perceived to cause 'linkage blindness,' where the information available in one agency is not available with other law enforcement agencies affecting remarkable achievement of outcomes. As a policy measure, the study recommended speedy removal of criminal information barriers at all levels and fast mitigation on both intra and inter-organizational information technological skill gaps. The deeply entrenched culture of secrecy and the need-to-know rather than the need to share information policy should further be re-visited and dealt with. Finally, there is an urgent need for National-wide Criminal Information Management System with certain rights for all law enforcement agencies. The use of a database will reduce the technological barrier since criminal information will be made accessible to all the agencies.

REFERENCES

[16] Lake and Morgan (1993: 8),
[20] Reiss, 1992
[28] Reid, 2013
[31] Dolowitz and Marsh, 2000

DOI: http://dx.doi.org/10.24018/ejsocial.2021.1.5.121
[32] Versaterm, 2010
[33] Manning, 2003