EasyChair Preprint

№ 7868

Assessment of Trans-Border Surveillance Strategies on National Security at Isebania, Migori County, Kenya

Kithii Njuki and Elijah O.S Odhiambo

May 1, 2022

ASSESSMENT OF TRANS-BORDER SURVEILLANCE STRATEGIES ON NATIONAL SECURITY AT ISEBANIA, MIGORI COUNTY, KENYA

ABSTRACT

A nation has security when it has the ability to preserve the nation's physical integrity and territory, to maintain its economic relations with the rest of the world on reasonable terms, to preserve its nature, institutions and governance against disruption from outside; and control its borders since national Security of any nation is the epitome of development and prosperity. This has been given little focus on Kenya in her borders thus making them porous. It's on these grounds that the study endeavored to assess trans-border surveillance strategies on national security at Isebania. Decision and complexity leadership theories were used as spring board of the study. The research employed mixed methods of research where survey research design was key. The research utilized random sampling technique on a target population that comprised of 980 persons (800 business persons, 70 village elders, 60 border Officers, 43 Police Officers, 6 Chiefs and 1 Assistant county commissioner). According to Mugenda(2008), the study considered a 30% of each category of sample population and this yielded 294 as the sample size for the study. The study also used interview, Questionnaires, and Focus group discussion tools to collect information from the respondents. Data analyzed by the use of Statistical Package for Social Sciences (SPSS). The results of the study are presented in form of frequency tables, charts and graphs. Results indicated that there was a strong need to improve technology usage at trans-border to detect explosives. From the research finding, the study recommends that modern and effective technology needs to be adopted at the border and qualified personnel also deployed to manage the same.

Key words: *Surveillance, Trans-border, National security, Image recognition technology*

1.0 INTRODUCTION

The border has been called the fundamental political institution; and the bordering process is one of the most important roles for community, delineating between inside and outside, us and them, safe and dangerous, known and unknown (Amoore and Goede, 2005). The interplay of surveillance and mobility has a long history, growing from historical fears of invasion, disease, and mass migration. However, the sinews of empire and the current network society of globalization depend on the free mobility of at least some portion of the global population. Indeed, as Foucault foresaw, one might say that "the idea of the Panopticon is completely archaic," reliant as it is on "an exhaustive surveillance" For space to open up, for circulation to take place, "we see the emergence of a completely different problem" that is not about strict demarcating but "allowing circulations to take place, controlling them, sifting the good and the bad, ensuring that things are always in movement" (Foucault, 2007).

At the same time, inter-state borders remain central to the global mobility regime, both in terms of the "international management of populations" (Hindess, 2000), but also the management of labor flows. References to border security and border insecurity not only shape discourse about the border, but also about immigration, drug policy, U.S.-Mexico relations and homeland security. Border regulation and control have effectively been upgraded to a national security mission. Customs and Border Protection (CBP), the Department of Homeland Security (DHS), agency that oversees the Border Patrol, states that its "top priority is to keep terrorists and their weapons from entering the United States."

While many illegal entry attempts take place at official ports of entry (POEs), others take place in the long and sometimes remote stretches of border in between POEs. In these areas, the Border Patrol uses patrols and sensor technology to detect illegal entry attempts (Predd *et al*., 2012). Due to limitations in resources and the difficulty in making precise estimates about the total flow of illegal activity that is undetected, it is not always possible to assess how successful the patrolling strategies are, since apprehension data alone does not provide a complete picture. In the Kenyan setting especially at Isebania, the problem of drugs, cattle rustling, and proliferation of small arms and light weapons is rampant and therefore, this led the researcher to investigate the trans-border surveillance strategies in use and their influence on national security.

In security domains like border patrolling, adversaries (e.g., transnational criminal organizations) are constantly using surveillance to gather intelligence about security operations to adapt their actions to avoid detection and interdiction. If security operations, such as patrols, are too predictable, it makes it easy for adversaries to learn patterns in the security operations that can be exploited. Using randomization can be an effective way to improve the efficiency of security policies, and game-theoretic models can be used to identify the right ways to randomize for a specific problem based on predicting the adversaries' responses to security policies (Gutiérrez *et al*., 2013). The smart border is a diffuse one physically extending both beyond and inside its geopolitical location, and involving a multiplicity of sites for the surveillance of movement. Nonetheless, in the uncertain processes leading to their implementation "strategies produce effects, some of them unintended, yet always concrete." (Cote-Boucher, 2008).

Surveillance can be viewed from different perspectives; it includes human and technological gazing where officials watch the physical movements and activities of persons. Second, surveillance involves the acquisition of personal data. This includes the collection of biographical, biometric, or transactional data on individuals harvested from personal communications, electronic transactions, identifiers, records, or other documents. In the former, observations can be used for identification or may act to advance an investigation as a component of a larger body of evidence, as in the case of CCTV data. The latter involves voice or documentary information that can be used in criminal investigations or prosecutions (Romero, 2003). Hence, the meaning given to border surveillance here is the collective action of official gathering of information on persons for the stated purpose of preventing crime and transnational terrorism or prosecuting offenders. As the police gather more personal information through surveillance, search, and seizure, a greater number of persons come within their official purview vis-à-vis suspicion profiles, threat assessments, or specific investigations. While it has been found that strong technological application in border surveillance is key, it is not clear in the context of Kenya-Tanzania setup whether a similar scenario exists.

The emergence of automated facial recognition as a security technology must be understood not only as part of post-9/11 security hysteria, but also in relation to the profound post-cold war identity crisis of the national security state. The post-9/11 technostalgic assertions made by Senator Feinstein and others not only efface the technology's muddy history and reify automated facial recognition as "hi-tech," they also frame the problem of security as one of recognition or identification, the need to accurately and reliably identify the enemy Other. While this framing enabled the biometrics industry to capitalize on the hyper-paranoia of the post-9/11 moment, the preoccupation of the national security state with identifying new enemies and problems to legitimate itself intensified a decade earlier, following the fall of the Berlin Wall and the breakup of the Soviet Union (Chellappa *et al*., 1995).

Security and surveillance technologies is something of a misnomer as the technologies elaborated in the following discussion have either been designed specifically for security reasons, or more commonly have been developed for other purposes and laterally found a security and/or surveillance application. Thus, arriving at a specific definition of border security technologies is problematic and is inextricably linked to the concept of security which is being evoked. For the purposes of this discussion security technologies are those employed in an effort to provide or enhance the security of people, property and information (Masaki, 2004).The development and proliferation of security and more specifically, surveillance technologies have been facilitated by advances in a number of scientific domains, most notably in the areas of telecommunications, information and computing as well as location tracking (Masaki, 2004).

To that effect there is great need to assess surveillance technologies that are in place at Isebania trans-border and improve on the same is deficient and or introduce new ones for the purposes of securing the nation of Kenya.

1.1 Statement of the problem

Studies that have been done on border issues centered on terrorism and surveillance strategies. For example

Ndut and Odhiambo (2020) in their article "Mechanisms of Curbing Smuggling of Food commodities from Uganda to Kenya" found that: there was heavy security deployment on both sides of the countries. This was one way of discouraging illegal interactions and had to be promoted through legal activities. In Wakhungu *et al*. (2020) article "Challenges and Opportunities Constraining and Enhancing Kenya and Tanzania Participation in the EAC Econo-Political Integration Process" quotes Article 5(1&2) of the Treaty establishing EAC (EAC Treaty, 2006) states that: the objectives of the community shall be to develop policies and programmes aimed at widening and deepening co-operation among partner states in political, economic and social and cultural fields, research and technology, defence, security and legal and judicial affairs, for their mutual benefit (5,1). Pursuance to provisions of paragraph 1 of this Article, the partner States undertake to establish among themselves and in accordance with the provisions of this Treaty, a Customs Union, a Common market, subsequently a Monetary Union and ultimately a political federation in order to strengthen and regulate the industrial, commercial, infrastructural, cultural, social, political and other relations of the partner states to the end that there shall be accelerated, harmonious and balanced development and sustained expansion of economic activities, the benefit of which shall be equitably shared (5,2). There is scanty research on identifying specific trans-border surveillance strategies and interrogating them, or especially in Kenya-Tanzanian at Isebania border.

Isebania as a frontier near Tanzania has many challenges from cattle rustling along and across the border, proliferation of small arms and light weapons (SALWs) and the menace of drugs to black economy. This study thus endeavor and examined the impacts of using Multi Agency Command Centre Strategy on National Security at Isebania trans-border, Migori County, Kenya in the effort to give suggestion on whether the strategies are relevant and their effectiveness in countering insecurity or the contrary.

1.2 Objective of the study

One of the objectives was to Assess the Impacts of using Image Recognition Technology Strategy on National Security at Isebania trans-border, Migori County, Kenya.

1.3 Research Question

What were the impacts of using Image Recognition Technology Strategy on National Security at Isebania trans-border, Migori County, Kenya?

1.4 Justification of the study

1.4.1 Academic Justification

Studies have been carried out on border surveillance strategies to mitigate national security threats in US-Mexico, Russia-Finnish, Spanish-North African lime borders and illegal migration problems, but little has been researched on border surveillance strategies in China, Africa and especially East Africa. Secondly, there have been problems of illegal drugs trafficking, illegal aliens into the country, black economy thrive in Isebania borderlands and small arms and light weapons evidenced by cattle rustling by armed criminals in Kuria West, Kuria East and Trans-Mara communities. This study was interested in examining the extent to which this problem could be solved by scaling up trans-border surveillance strategies in Isebania to keep the nation of Kenya safe. Third, this study once in the libraries will be a reference point for students at both graduate and post graduate studies and hence its necessity.

1.4.2 Policy Justification

The role of border security and territorial integrity is that of military and foreign affairs departments. In Migori County where Isebania is located, the nearest military base is found in Eldoret. Our research therefore finds a gap in that it foresees the need to recommend establishment of a military base in Migori County especially near Isebania to support police and other departments to mitigate border insecurity that could become a national security threat. The study also envisaged to examine whether the image recognition technology, customs manifest, and how multi-agency command Centre has influenced on national security and if these surveillance strategies are insufficient, to be strengthened to keep the country safe.

Security is a sensitive issue and the findings of this study help in understanding the importance of employing the right security strategies on the borders. Many boundaries of this country are porous and the findings will help know the imminent risk of not effectively guarding the borders. This study therefore will provide valuable information to the government leadership on the extent to which the issue of security could be dealt with effectively. This will help them

look for contingent measure to mitigate the lapses in national security at the border of Isebania.

2 .0 Literature Review

Literature review was founded on the premise that knowledge is cumulative. This meant that the researcher established what is already known in an area and then attempt to build on it. The assumption is that existing knowledge is accurately and properly documented and easily retrievable (Mugenda, 2008). The depth and breadth of review emphasize the credibility of the research as a scholarly piece of work but more critically, provided solid background for the investigation.

2.1 Image Recognition Technology and National Security

Our study investigated the impacts of Image Recognition Technology (IRT) as a way of curbing insecurity at Isebania trans-border. In relation to the above, the following was the reaction after 9/11, 2001 attacks in America (US) by Al-Qaeda fundamentalists. Gates (2004) notes:

> Of all the dramatic images to emerge in the hours and days following the September 11 attacks, one of the most haunting was a frame from a surveillance-camera video capturing the face of suspected hijacker Mohamed Atta as he passed through an airport metal detector in Portland, ME. Even more chilling to many security experts is the fact that, had the right technology been in place, an image like that might have helped avert the attacks. According to experts, face recognition technology that's already commercially available could have instantly checked the image against photos of suspected terrorists on file with the FBI and other authorities. If a match had been made, the system could have sounded the alarm before the suspect boarded his flight.

However dissenting voices hold that, the idea that computerized face recognition might have helped avert the al-Qaeda terrorist attacks was perhaps the most ambitious claim circulating about biometric identification technologies in the aftermath of September 11. Along with the enormous flood of imagery of the day, relayed in the news media were the out-of-focus surveillance-camera images of two of the alleged attackers. The recorded video image from the airport in Portland, Maine that appears to show Mohammad Atta and Abdulaziz Alomari passing through airport security is a familiar part of 9/11 iconography. And it is virtually impossible to reference this image without also invoking the claim that facial recognition technology could have identified the men in the image as wanted terrorist suspects. Already existing commercially available technology, according to this regretful yet strangely hopeful assertion, "Could have instantly checked the image against photos of suspected terrorists". Technologies that use digital readings of the face to identify individuals could have saved the United States from the worst terrorist attack in its history (Stikeman, 2001)

The emergence and evolution of Image Recognition Technology emerged in 2001, when Paul Viola and Michael Jones invented a simultaneous face detection algorithm allowing for human figures to be identified through their facial traits. In 2005, Dalal and Triggs published Histograms of Oriented Gradients (HOG), theorizing a feature detector for the recognition of pedestrians in security system circuits (Dalal and Trigs, 2005). In 2012, Krizhevsky, Sutskever and Hinton hit it big with a new object recognition algorithm ensuring an 85% level of accuracy. In 2015, the Convolutional Neural Network (CNN) developed Infrared tools whose level of accuracy in facial recognition exceeded 95%. Today, Google, Amazon and even some car manufacturers are channeling their efforts as well as their Research and Development (R&D) investments into the development of new technologies that integrate Image Recognition. Amazon, for instance, recently launched Amazon Recognition, a new product based on Image Recognition functions and able to scan photos, guess at emotions through face recognition and classify objects or animals.

The way technology has been utilized; used or abused in relation to National security was hyped in the Snowden Case. Transnational State surveillance hit the global headlines in June 2013 with the revelations of former National Security Agency (NSA) contractor, Edward Snowden. A series of leaked documents described the operation of the PRISM programme which allows the systematic interception, storage and analysis of at least 11 different types of electronic communications of non-US citizens from telephone and global Internet companies such as Google, Apple, Microsoft and Face book by the NSA (Greenwald, 2013). The capacity to sort between "low risk" and "high risk," between desirable and undesirable, is intensified through the biometrification of the international passport system. Passports are the primary document for identifying, regulating and tracing mobile individuals. The passport is, as Salter suggests, "a modern heuristic device which serves to link individuals to foreign policy, and according to which government agents classifies travelers as safe or dangerous, desirable or undesirable, according to national, social or political narratives" (Salter and Amoores, 2008). In most cases the rationale given for incorporating biometric data into travel documents is "national security" - meaning security from "illegal" migrants and those labeled terrorists (Thomas, 2005).

Emerging Geographical Information Systems (GIS) technologies, such as Radio Frequency Identification (RFID) and the Global Positioning System (GPS) allow us to pinpoint and track the location of people and commodities. There are a vast array of navigation and tracking systems available but principally they rely on the techniques of triangulation, proximity sensing and scene analysis (Hightower and Borriello, 2001). Global Positioning System (GPS) is a worldwide radio-navigation system formed from the constellation of 31 satellites and their ground stations. It was developed by the Department of Defense in the US during the 1970s and was fully operational by the mid-1990s. GPS technologies facilitate the collection of location information by enabling devices (mobile phones, vehicles, electronic mapping devices, etc.) to be pinpointed accurately using reference data taken from various sources, most notably GPS location referencing radio signals received from satellites orbiting the Earth. This is done through triangulation, matching three or more separate signals from a selection of the tracking satellites. The GPS receiver uses the signal from a fourth satellite to determine altitude, allowing a determination of position in three dimensions. Data is continuously transmitted by the GPS satellites to the GPS receiver which collects and stores this data. Increasingly, "active" devices are equipped with a communication module e.g. GSM which continuously communicate their present location to a third party allowing for real-time tracking of the GPS device from another location (Hightower and Borriello, 2001).

Retailers such as Tesco, the world's third largest grocery retailer uses RFID tags to help improve stock control systems and track stock through the supply chain. Since 2003, Metro Group in Germany has been running an RF ID-enabled "Future Store," where RFID technology is used for various applications throughout the supply chain (Wamba and Boeck, 2008). Animals, including pets and livestock have been implanted with RFIDs in order to track information on ownership and immunisation records and to provide the traceability of livestock needed to ensure food safety. Pets (currently restricted to cats, dogs and ferrets) travelling within Member States in EU are required to have "pet passports" and the pet is connected to the passport by an implanted RFID tag. The purpose of the passport is to protect citizens from the threat of rabies and certain other animal borne diseases (Hodges and McFarlane, 2005).

In conclusion, our literature review focused on what the surveillance strategies: image recognition technology in other jurisdictions namely; the US, EU, Australia, and Russia and Finland borderlands and how it affects the National Security of these countries and or Unions. The review has exposed the level of success in these jurisdictions and therefore our task here is to assess impacts trans-border surveillance strategies had on national security, its utilization, degree of success in identifying, deterring, and preventing and responding to insecurity at Isebania border of Migori County, Kenya.

2.3 Theoritical Framework

Wasike and Odhiambo (2016) discuss the role of theories in guiding the thrust of academic studies. They emphasize the importance of theories in offering compelling and incisive causal explanations with calculated precision. They buttress their argument by quoting Smith (1996) who asserts that theories play the role of predicting, prescribing and evaluating socio-political phenomena hence they cannot be ignored. Indeed, the high diversity and richness of theoretical frameworks give researcher a valuable opportunity to see what could seem familiar through a new and distinct perspective. Silverman argued that "Theory without some observation to work upon is like a tractor without a field" (Silverman, 2001). Therefore, a theoretical framework gives the researcher a chance to "observe" and "perceive" just certain aspects of the phenomenon under study while some are concealed. Thus, theory or theoretical framework alone cannot provide a comprehensive explanation on the issue being studied.

2.3.1 Decision theory and national security

Blaise Pascal, introduced decision theory in his famous "wager" (Hacking, 1975). His argument was designed to convince non-believers that they will be better off becoming believers, Pascal introduced several basic notions of decision theory: (i) the decision matrix, in which one's acts are independent of Nature's choices, or the "states of the world"; (ii) domination between acts, where one act is better than another no matter which state obtains; (iii) expected utility maximization, according to which the choice between un- dominated acts should be according to the mathematical expectation of the utility of the outcomes they yield; (iv) subjective probability over the states, which is an application of the mathematical probability model as a way to capture one's beliefs; and (v) non-unique probabilities, where one's beliefs are too vague to be captured by a single probability vector.

Decision theory is attractive in security technology-selection problems because it provides a methodology to deal with the uncertainty and multi-objective nature of these decisions. In decision theory, risky decisions are those whose consequences are uncertain. Risky decisions can also have multiple objectives. Each objective has an attribute that is the degree to which a given decision objective has been attained (Fischbeck and Butler, 2002). The security technologies selection problem is the task of selecting the best set of security counter-measures for an information system. Inherently, the challenge is to quantify the benefits of security countermeasures and the consequences or outcomes of successful attacks. The benefit of a security countermeasure depends on how well it stops an attack, or mitigates the consequences of a successful attack (Butler, 2001).

A security engineer must also balance multiple objectives when selecting security technologies. Consequences of successful attacks must be balanced with performance constraints, budget limitations and other design considerations. Each attack may result in a similar outcome, but with different attributes. The security technology-selection method relies on countermeasure expertise to improve the selection of countermeasures. Countermeasure expertise is used to more accurately represent the mitigation impact of a countermeasure given an attack in the security technology selection problem (Fischbeck and Butler, 2002).

Decision theory however, has been challenged and one of the earliest, and perhaps the most radical objection to the theory was raised by Herbert (1957). He coined the term "bounded rationality", and argued that people do not optimize; rather, they "satisfice": as long as their performance is above a certain "aspiration level", they stick to their previous choice. Only when their performance is below that threshold do they experiment with other choices. Simon thus challenged the very paradigm of optimization. While his theory is relatively seldom incorporated into formal decision models, it has had a remarkable impact on the thinking of many decision theorists, who developed models that are classified as "bounded rationality" even if their departure from the basic paradigm is much less dramatic than that of satisficing behavior. Expected utility maximization was also attacked based on concrete examples in which it turned out to provide a poor prediction of people's choices.

Importantly, Kahneman and Tversky (1974) also uncovered several implicit assumptions of the decision theory, which were also too idealized to describe actual choices. For example, they documented the

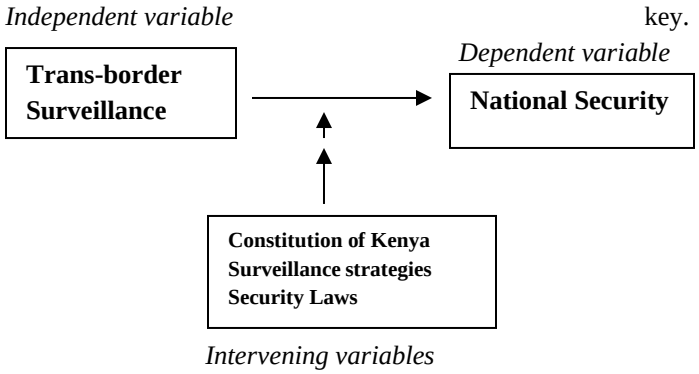
"framing effect" which shows that different representations of the same problem may result in different choices. Later, in 1979, the two scholars suggested "Prospect Theory" as an alternative to expected utility maximization. One key idea in Prospect Theory is that people respond to given probabilities in a way that is non-linear in the probability, especially near the extreme values of 0 and 1. Another idea, with potentially far-reaching implications to research in political science, is that people react differently to gains as compared to losses.

Decision theory offers guidance for national security policy and associated civil liberty issues introduced by the tragic events of September 11. Signal Detection Theory as posited and rekindled by Harvey (2014) the state-of-the art procedure for decision making considered here, provides a powerful model for detecting the presence of a "signal," whether a sensory stimulus in the laboratory, a bomb, or a terrorist. Although the underlying mathematical model is complex, predictions from the model are straight forward and were explored in a few of the many possible security-related applications.

2.3.2 Complexity Leadership Theory and national security

Complexity Leadership theory (CLT) was born Uhl-Bien and Marion (2002) where they did a research to explain the dynamics involved in leading complex organizations like the United Nations, Al-Qaeda, European Union, and governments. They held that when an organization with several ministries, departments with interacting at horizontal and vertical levels needs leader who is well-balanced, appreciates all the leaders at different level and his /her role to act as a meta-leader. Basically managing all the human resource synergies and pooling of resources without undermining any of the departments and ministries. Pollock and Coles (2015) when analysing the interoperability among the emergency government departments in Britain posited the need to have a theory that can explain succinctly the interactions optimum for effective response.

In the context of image recognition technology as a surveillance strategy, CLT forms good basis for explaining the relationship present in all the parties/organizations involved in running national security in Kenya. In the case of Isebania, Migori County, we have border officers, police, national intelligence service, national government administration officers, village elders, who must come together in order to secure the border. To succeed in the exercise, may it be an emergency, security meeting or a public barazas, a leader is of essence. In this scenario the National Government Administration Officers (NGAOs); ACC, DCC or CC) is vital so as to harmonize all the resources in order for the government to deliver as one. All the leaders have different competencies and specialized training in their fields, though in need of support in terms of human capital, and or physical resources like vehicles or money. In order to function effectively and efficiently, complexity leadership theory becomes key.



3.0 RESEARCH METHODOLOGY

This section is organized to reveal the various procedures and their appropriateness that was used in the study. It gave clear explanation on the Research Design, Location of the study, Target Population, sample Size and Sample Procedures, Data Analysis.

3.1 Research Design

In this study, survey design was applied. A survey is a method of collecting data in a consistent, or

systematic, way. This usually involves constructing a set of questions that are either asked by means of a questionnaire or through an interview (Glasnow, 2005). In addition Isaac and Michael (1997) survey research is used:

> To answer questions that have been raised, to solve problems that have been posed or observed, to assess needs and set goals, to determine whether or not specific objectives have been met, to establish baselines against which future comparisons can be made, to analyze trends across time, and generally, to describe what exists, in what amount, and in what context.

Kraemer (1991) identified three distinguishing characteristics of survey research. First, survey research is used to quantitatively describe specific aspects of a given population. These aspects often involve examining the relationships among variables. Second, the data required for survey research are collected from people and are, therefore, subjective. Finally, survey research uses a selected portion of the population from which the findings can later be generalized back to the population. In survey research, independent and dependent variables are used to define the scope of study, but cannot be explicitly controlled by the researcher. Before conducting the survey, the researcher must predicate a model that identifies the expected relationships among these variables. The survey is then constructed to test this model against observations of

the phenomena. Survey design is preferable in that it is stronger than other designs.

Surveys are capable of obtaining information from large samples of the population. They are also well suited to gathering demographic data that describe the composition of the sample (McIntyre, 1999). Surveys are inclusive in the types and number of variables that can be studied, require minimal investment to develop and administer, and are relatively easy for making generalizations (Bell, 1996). Surveys can also elicit information about attitudes that are otherwise difficult to measure using observational techniques (McIntyre, 1999). It is important to note, however, that surveys only provide estimates for the true population, not exact measurements (Salant and Dillman, 1994).

This study employed survey design research design to explore the variables and provide an opportunity for the researcher to collect systematic information on how trans-border surveillance strategies influence national security at Isebania, Migori, Kenya. The study will also employ descriptive research design which will be geared towards finding the extent to which the study variables on border surveillance influence national security of Kenya at Migori. The purpose of the design is to describe and explain events as they were or they will be. This design will be used because it is suitable for extensive research. Data will be collected by administering interview schedules, focus group discussions and Questionnaires to a sample of respondents to find out their opinions or attitudes regarding certain issues in order to answer questions concerning the current status of the subjects being studied (Orodho and Kombo 2002).

Focus group as a form of qualitative research design was utilized. In the Focused Group Discussion (FGD), attitudes, opinions or perception towards issues, product, service or program are explored through a free and open discussion between members of a group and the researcher (Kumar, 2010).It is like collectively interviewing a group of respondents.

3.2 Study Location

The study was carried out at Isebania Trans- border in Migori, Kenya. The County is one of the forty seven counties in Kenya. It is situated in the south-western part of Kenya. It borders Homa Bay County to the north, Kisii and Narok counties to the east and Republic of Tanzania to the south. It also borders Lake Victoria to the west. The county is

located between Latitude 0º24’ south and 0º40’ south and Longitude 34ºEast and 34º 50’ East and covers an area of 2,596.5 km^2 including approximately 478 km^{2}of water surface.

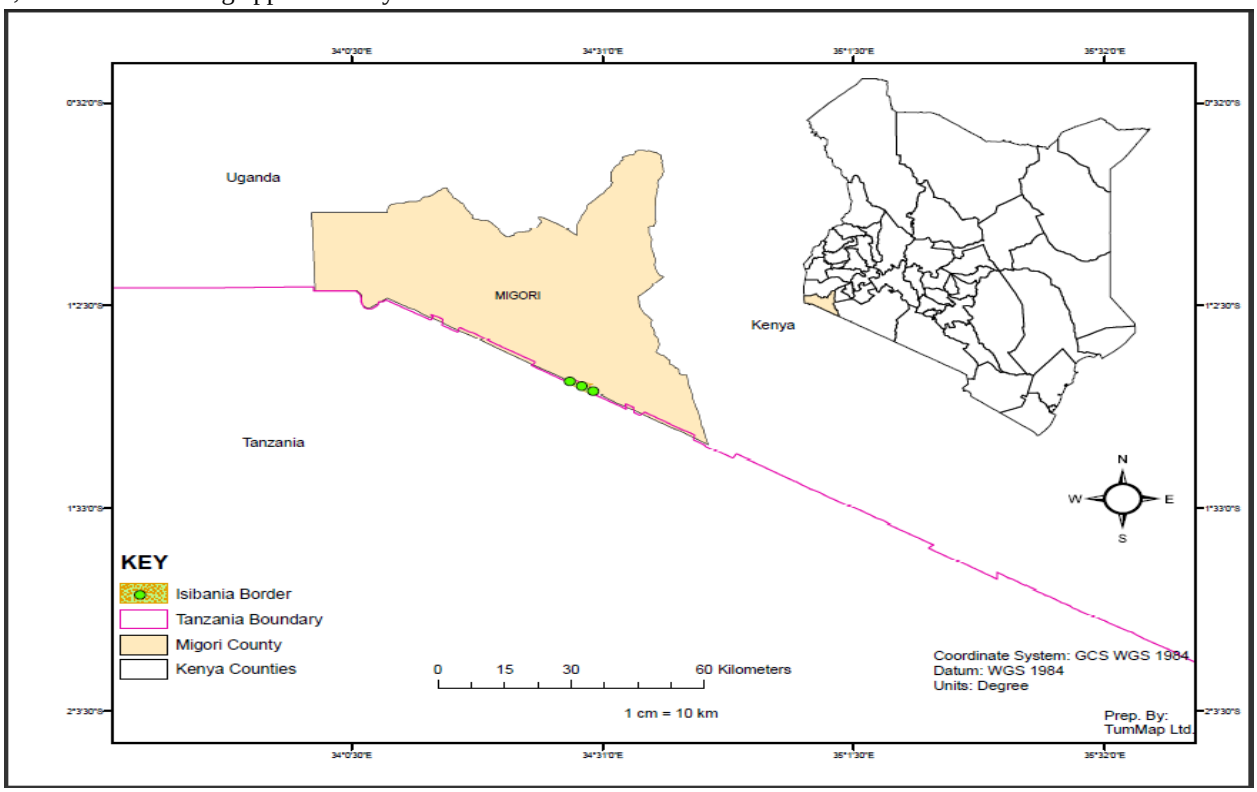


Figure 3.1 Map of Study Area
(Source: Researcher, 2019)

3.3 Target Population

According to (KNBS, Population Projection by County, Migori Office, 2011), Migori County has a population of 917,170 people. The study therefore targets the 31,931 People in Isebania division in addition, According to Migori County HR Department (2018) there are 60 Officers working at Isebania border post, 43Police Officers, 6Chiefs and 1Assistant County Commissioner (ACC) in Isebania division. The study also targets 70 village elders, and 800 business men and women. The target population therefore comprises of 800 business men and women, 70 village elders, 43Police Officers, 60 border Officers, 6 Chiefs and 1 ACCs).

3.4 Sampling Procedure and Sample Size

According to Mugenda (2008), 30% of target population is sufficient to draw viable conclusions. The sample size was derived from getting 30% of 800 business persons (BP), 70 village elders (VE), 60 border officers (BO), 43 Police Officers (PO), 6 chiefs, and 1 Assistant County Commissioner (ACC) yielding to 240 BP, 21 VE, 18 BO, 13 PO, 2 Chiefs, 1ACC.

3.5 Data Collection Instruments

The Data collection instruments which were, Interview schedules, Questionnaires and group discussions which was conducted by assembling a group of village elders together and then discuss on the topic of security and the Questionnaires to understand their views and opinions of the community members concerning the study because many of them were busy and did not find enough time to go through the Questionnaires and fill them and return them on time (Researcher, 2019)

3.6 Data Analysis

The collected data was analyzed based on the research questions. Data analyzed by use of both descriptive and inferential statistics. Descriptive statistics

included frequencies, percentages and means. Inferential statistic used involved the Chi-Square and correlation analysis to test the relationship between responses from the respondents and the variables under study. Analyzed data was presented in tables, charts and bar graphs as deemed appropriate (Mugenda, 2019).

4.0 Results and Discussion

This section presents the analysed data and the discussion of the same according to the research objective.

4.1 Image Recognition Technology

The objective of the study was to evaluate the impacts of using image recognition technology (IRT) strategy on National security at Isebania trans-border, Migori County, Kenya. The study employed eleven (11) questions leading to information specific to image recognition technology separately for clarity of the respondents. The review of few sampled questions and responses were analyzed and are as presented in Figure 4.1

4.1 Technology Needs Improvement

A bar graph showing percentage technology need for improvement

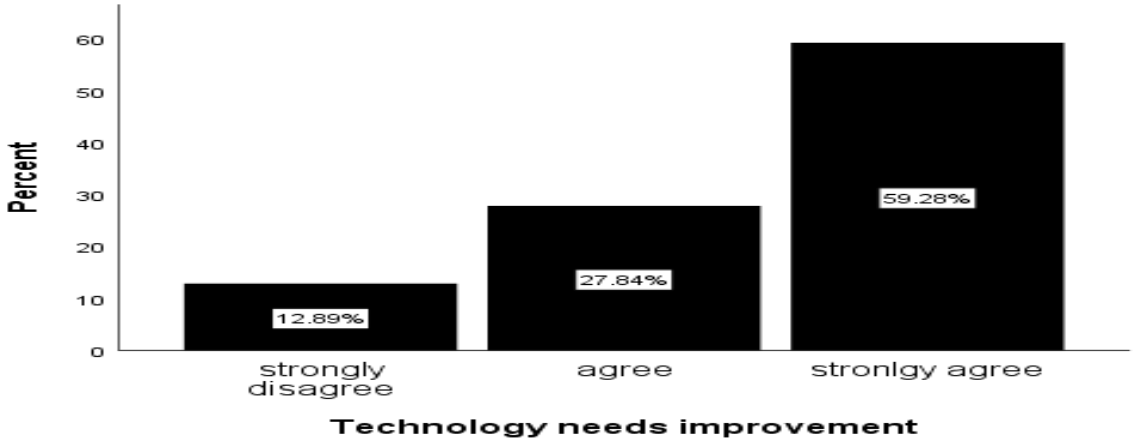


Figure 4.1: Technology Needs Improvement
Source: (Field data, 2019)

As per Technology Needs Improvement, majority of the informants strongly agree that there is need to improve technology for efficient and effective outcome as represented by 59.28%, agree at 27.84% and strongly disagree at 12.89%. In the case of Isebania border, many illegal entry into the country do not take place at the official Port of Entry (POEs) but in the long stretches of land between the POEs and therefore "the border patrol units use patrols and sensor technology to deter and detect illegal attempts" a point held by Predd *et al.* (2012) and in agreement with our findings that *"illegal goods and arms cross border unnoticed"* and "*border technology needs improvement".* The Kenyan government therefore needs to employ sensor technology to help border patrol units in long stretches of borderlands like the Northern borders between Sudan, Ethiopia and North Eastern frontiers between Kenya and Somalia.

The same position is equally held by Price Water Coppers (2015) in their *"The Future of Border Management"* that "*The physical frontiers with long land or sea borders; their surveillance be enhanced by using technological innovations such as infrared sensors, heat sensing cameras, unmanned aerial vehicles and radar and satellite surveillance*" and as

such, these technologies require better trained military personnel to operate.

Stikeman (2001) says that terrorists in on US soil triggered paranoia, which was contemplated to capitalize and take advantage of terrorists' attack for innovative techno-firms to sell their products. On the contrary, Gill *et al.* (2015) hold that the potential of using biometric means of identification was in the market and already had been marketed not in the most rigorous way, but attacks to US accelerated its adoption by states. Basing ourselves on research findings, it is prudent to point out that facial recognition technology at the border needs serious adoption and upgrade on the existing ones as well.

4.2 Radio Frequency Used to Detect Explosives

A pie chart showing if radio frequency is used to detect explosives percentage

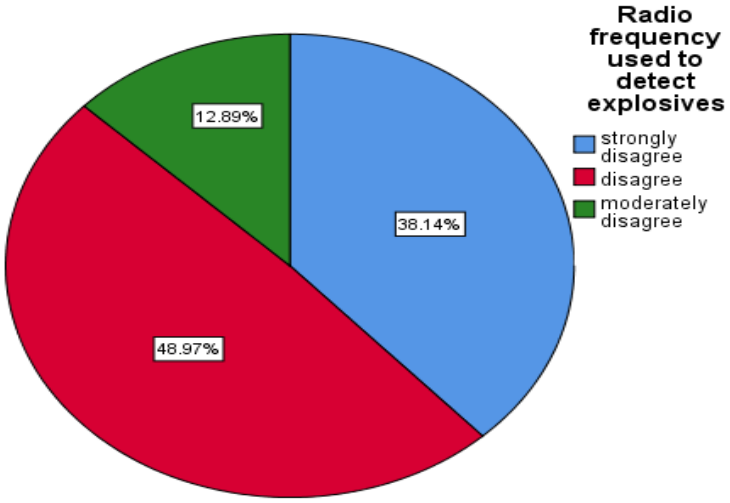


Figure 4.2: Radio Frequency Used to Detect Explosives
Source: (Field data, 2019)

Whether Radio Frequency Used to Detect Explosives is demonstrated in the Figure 4.2 which indicates that most of the respondents disagree that radio frequency is used to detect explosives as at 48.97%, strongly disagree follow at 38.14% and moderately disagree at 12.89%. The 12.89% is justifiable in that the respondents due to their limited knowledge about all the technology applicable in surveillance at the border. The 12 % may mean that it came from enlightened respondents and or border officers.

4.3: Facial Recognition Tech used

A pie chart showing percentage facial recognition

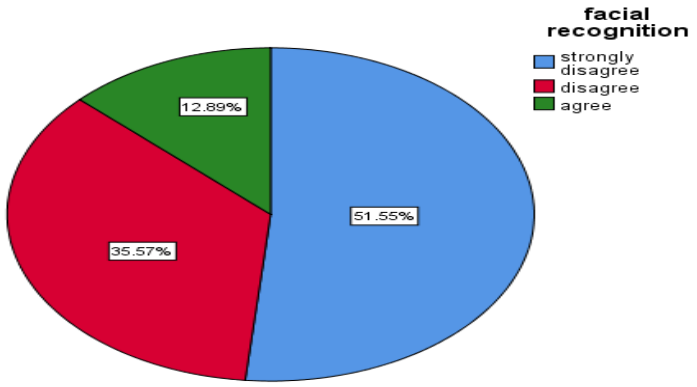


Figure 4.3: Facial Recognition Tech used

Source: (Field data, 2019)

Highest number of informants strongly disagree that there is facial recognition as represented by 51.55%, disagree at 35.57% and agree at 12.89%. Elizabeth McClellan (2020) in her work: *"Facial Recognition Technology: Balancing the benefits and concerns…"* defines Facial Recognition Technology (FRT) as:

> "An algorithm used to recognize a human face through the use of biometrics, which tracks facial features from a photo. These facial features often include the distance between your eyes, the distance from your forehead to your chin and other facial land marks thus creating your facial signature."

Governments as well as private institutions utilize facial recognition technologies in security sector, social media and medical field. Governments employ FRT to identify traffic offenders and also help the police solve serious crimes like murder, rape. Air ports and border crossing points use it to identify international criminals like drug dealers, human traffickers and terrorists (Symanovich, 2020).

Facial Recognition Technology allows users to engage in multifactor biometrics to verify a user's identity such as voice and facial recognition (Digracia, 2018). Phone companies like APPLE and Google are using multifactor biometrics and facial recognition technology to unlock phones and manage user accounts. In the medical field, use of FRT is able to diagnose genetic conditions through observation of a photo. This means that more beneficiaries with rare conditions will get diagnosis easily because specialist doctors are few and rare to get. Such ailments are for instance Down syndrome.

In the case of COVID-19, FRT was utilized to track patients with higher fever and therefore isolated with ease (Marr, 2020). Governments like "*Hong Kong had began employing Facial recognition technology at places such as border points, allowing government to track and identify individuals through facial scan*" (Adams, 2019). However facial recognition technology has challenges: FRT lacks proper legislation internationally to regulate and hold its abusers to account. A case in point, the United States (US) government does not have a federal law to govern facial recognition and other image recognition technology. Few states in US like Illinois, Texas, Washington and California have promulgated legislation to that effect (McClellan, 2020). Kenya passed its Data Protection Act, 2020 which has given comprehensive coverage on issues biometrics and other facial geometry mapping. The challenge with those legislations is that they lack clear and proper definitions of what FRT is all about. Secondly, some states in US are also limited in their applicability in geographical jurisdictions.

Companies like APPLE, Face book and Shutterfly have set privacy policy on how to voice identification and facial geometry as password to unlock these devices and log into the users' accounts. Governments like Hong Kong have been alleged to have abused FRT in identifying and surveilling the demonstrators in 2019 over national security legislation that most of Hong Kong opposed reasons being they could be extradited to main land China to face terrorism, secession or treason prosecution there (Bocchi, 2019; Lawrence & Martin, 2020).

4.4: Image Recognition Technology Useful in Curbing Crime

A bar graph showing percentage IRT usefulness in curbing crime

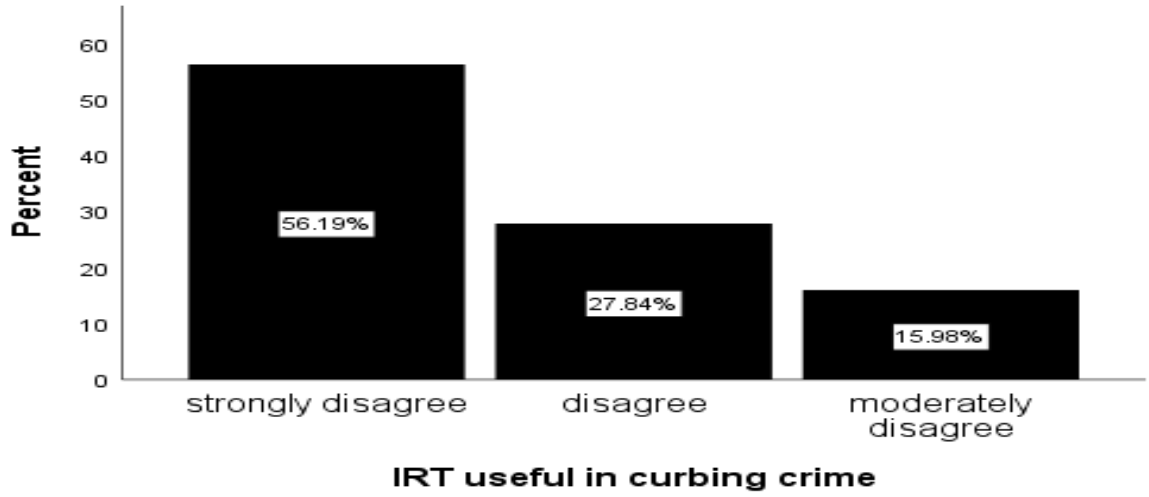


Figure 4.4: IRT Useful in Curbing Crime
Source: (Field Data, 2019)

Most of the informants strongly disagree on IRT usefulness in curbing crime as represented by 56.19%, disagree at 27.84% and moderately disagree at 15.98%. Image Recognition Technology (IRT) means Closed-Circuit Television, Infrared Cameras, X-Ray, Gamma Ray, Motion sensors and facial Recognition Technology appliances that is able to produce information in real time or in stored format such that harmful materials, people or goods and weapons are detected for the purposes of security.

Strictly speaking there is no specific image recognition technology but a multitude of application devices/ machines as mentioned earlier in this chapter. The low rating % of the usefulness IRT in fighting crime is due to this fact that the question is complex and would have required explanation to the respondents for them to be able to answer sufficiently. This is not practical in questionnaire form but in interviews and Focus Group Discussion (FGD), it is possible of which interviews and FGD were few.

Justification for this argument is that if you scrutinized the responses for facial recognition technology used scored 12.8% agree to the positive that the technology is in use and probably the responses were from border officers, police or NGAOs. Secondly, it is true that technology at Isebania border is weak as all the queries on technology weighted to the negative. Kenya Revenue Authority (2010) contradicts this finding in their white paper presented in Cairo as indicated earlier that some level of technology is in use in border points in Kenya.

In conclusion, many IRT are emerging technologies with their effectiveness not conclusively tested and also due to fear of technological sabotage and piracy, many companies conduct their test in utmost secrecy.

Many criminal organizations would like to defeat national security surveillance apparatus hence it is difficult to evaluate them exhaustively.

4.5: Scared When I see Cameras

A bar graph percentage showing if one is scared when sees the cameras

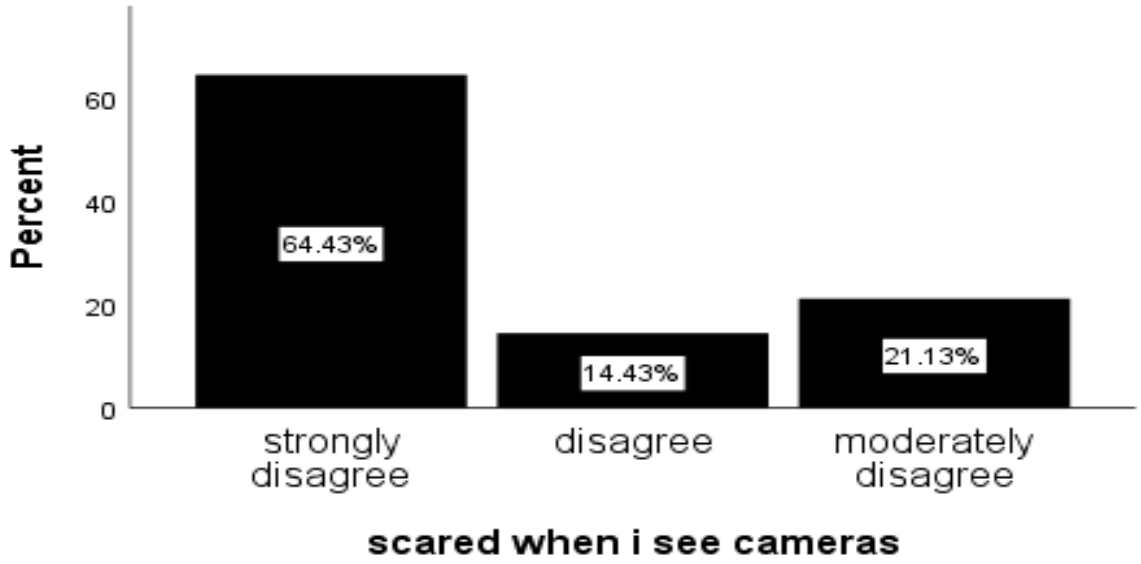


Figure 4.5: Scared When I see Cameras

Source: (Field data, 2019)

Concerning whether scared when respondent saw cameras at the border, the results in Figure 4.7 reveal that majority of the respondents strongly disagree that they are scared on seeing the cameras as represented by 64.4%, moderately disagree at 21.13% and disagree at 14.43%. If the people being gazed or served by government became aware of the surveillance media or technology, the effectiveness of the process would be self-defeating. This scenario was experienced when the public got knowledge of "PRISM", a US surveillance program and the UK's Government Communication Head Quarters (GCHQ) where after whistle blower Snowden exposed the two programs and hence they failed.

To the contrary, Juel *et al.* (2005) calls for public participation and advocacy in drafting and promulgation of legislations, border protection policies. In addition, on July 2019, the Interior Ministry and in reference to article 10 of the Constitution of Kenya, specifically public participation, integrity and principles of good governance called for public views on the same. The review pertains to Births and Death (Cap 149), Kenya Citizen and Immigration Act (No. 12 of 2011), Kenya Citizen and Foreign National Management Service Act (No.31 of 2011) and Refugees Act (No.13 of 2006). This public participation as a democratic right has given Kenyans a voice in every matter pertaining to public governance. It has seen many legislations, policies and administrative actions reviewed or nullified by courts due to inadequate involvement of the public.

5.0 Summary and Conclusion

As per Technology Needs Improvement, majority of the informants strongly agree that there is need to improve technology for efficient and effective outcome as represented by 59.28%, agree at 27.84% and strongly disagree at 12.89%. In the case of Isebania border, many illegal entry into the country do not take place at the official Port of Entry (POEs) but in the long stretches of land between the POEs and therefore "the border patrol units use patrols and sensor technology to deter and detect illegal attempts" a point held by Predd *et al.* (2012) and in agreement with our findings that *"illegal goods and arms cross border unnoticed"* and "*border technology needs*

improvement". The Kenyan government therefore needs to employ sensor technology to help border patrol units in long stretches of borderlands like the Northern borders between Sudan, Ethiopia and North Eastern frontiers between Kenya and Somalia. Concerning whether scared when respondent saw cameras at the border, the results in Figure 4.7 reveal that majority of the respondents strongly disagree that they are scared on seeing the cameras as represented by 64.4%, moderately disagree at 21.13% and disagree at 14.43%. If the people being gazed or served by government became aware of the surveillance media or technology, the effectiveness of the process would be self-defeating.

6.0 Recommendation of the Study

Modern and effective technology needs to be adopted at the border and qualified personnel also deployed to manage the same. The third specific study was to analyze the impacts of using Image Recognition technologies as surveillance strategies on national security as such recommends a study to assess security inter-agency technological intelligence sharing to avert threats to national security in Kenya.

REFERENCES

Adams, R. (2019). "Hong Kong Protesters are worried about Facial Recognition Technology; but there are many other ways they are being watched," BUUZFEED News (17 August 2019).

Amoore, L. & Goede, M. (2005). Governance, risks and dataveillance in the War on Terror, Springer.

Bocchi, A. (2019). "Protesters Use Laser against Facial Recognition Cameras. A Cyber War Against Chinese Artificial Intelligence" alessandra (@alessbocchi 31 January 2019).

Butler, S. (2001). Improving Security Technology Selections with Decision Theory, Pittsburgh PA, Carnegie Mellon University.

Cote-Boucher, K. (2008). The Diffuse Border: Intelligence Sharing, Control and Confinement along Canada's

Chellapa, R. Wilson, L. and Sirohey, S. (1995). Human and Machine Recognition of Faces: A Survey, Proceedings of the IEEE 83, No. 5 (705-740). Smart Border. Surveillance and Society.

Dalal, N. & Triggs, B. (2005).Histograms of Oriented Gradients for Human Detection. CVPR05.

Digracia, K. (2018). Cyber Insurance, Data Security, and Block-Chain in the Wake of the Equifax Breach, Journal of Business and Technology Law.

Fischbeck, P. and Butler, S. (2002). Multi-Attribute Risk Assessment, Pittsburgh PA.: Carnegie Mellon University.

Foucault, M. (2007).Security, Territory, Population: Lectures at The College De France 1977-1978, Translated by D. Macey, London: Allen Lane.

Gates, K. (2004). "The Past Perfect Promise of Facial Recognition Technology" Institute of Communications Research University of Illinois at Urban.

Glasow, A. (2005). Fundamentals of Survey Research Methodology, Washington C 3 McLean, Virginia.

Gill, P. Corner, E. Thornton A. (2015).What are the Roles of Internet in Terrorism? Measuring online Behaviours of Convicted UK Terrorists,Vox-Pol Network of Excellence.

Greenwald, G. (2013). NSA collecting phone records of millions of Verizon customers daily the Guardian (June, 2013).

Hacking, I. (1975). The Emergence of Probability, Cambridge: Cambridge University Press.

Harvey, L. O. (2014). Detection Theory: Sensory and Decision Processes. Boulder, Colorado University.

Herbert, S. (1957). Models of Man. New York: John Wiley & Sons.

Hightower, J. and Borriello, G.(2001). A Survey and Taxonomy of Location Systems For Ubiquitous Computing, University of Washington: Seattle.

Hindess, B. (2000). Divide and Govern: Governmental Aspects of the Modern States Systems, Governing Modern Societies, R. Ericson and N. Stehr, Toronto University

Hodges, S. & McFarlane, D. (2005). Radio frequency identifications technology, applications

and impact, Auton ID labs white paper series.

Juels, A. Molnar, D. & Wagner, D. (2005).Security and Privacy in E-Passports.

Kahneman, D. & Tversky, A. (1979). "Prospects Theory: An Analysis of Decision Under Risk," Econometrica.

KRA (2010). Implementation of Electronic Cargo Tracking System, Cairo: Kenya Revenue Authority

Kraemer, K. L. (1991). Introduction Paper presented at The Information Systems Research

Challenge: Survey Research Methods.

Kumar, R. (2010). Research methodology, a step by step guide for beginners, (3rded).New Delhi, Sage.

Lawrence, S. & Martin, M. (2020). China's National Security Law for Hong Kong: Issues for Congress, Congressional Research Service.Mugenda, G. (2008). Social Science research theory and principles, Nairobi: ARTS.

Masaki, H. (2004).Development of Biometric DNA Ink for Authentication Security: Journal of Experimental Medicine, Tokyo.

Marr, B. (2020). Corona Virus: How Artificial intelligence, Data Science and Technology is used to fight Pandemic, Forbes (13 March 2020).

Odhiambo, E. O. S. (2014). Religious Fundamentalism and Terrorism, Journal of Global Peace and Conflict Vol.2

Orodho, A. J. & Kombo, D. K. (2002). Research Methods, Kenyatta University, Institute of Open Learning Masola publishers, Nairobi.

Predd, J. Willis, H. Setodji, C. & Stelzner, C. (2012). Using pattern analysis and systematic Randomness to allocate US border security resources, Rand.

PWC (2015). The future of border management: Maintaining security; Facilitating Prosperity, CDC.

Salter, E. & Amoores, M. Eds. (2008).Smart Borders and Mobilities: Spaces, Zones, Enlosures, surveillance bodies network, Ontario, Canada.

Romero, A. (2003). "Living in Fear: How the U.S. Government's War on Terror Impacts American Lives" In C. Brown (Ed.) Lost Liberties: Ashcroft and The assault on Personal Freedom, New York: The New Press.

Salter, E. & Amoores, M. Eds. (2008).Smart Borders and Mobilities: Spaces, Zones, Enlosures, surveillance bodies network, Ontario, Canada.

Salant, P. & Dillman, D. (1994).How to conduct your own survey. New York: John Wiley and Sons.

Silverman, D. (2001). Interpreting Qualitative Data, Methods of Analyzing Talk, Test and Interactions, London: Sage Publications.

Stikeman, A. (2001). "The Technology Review: Top Ten Biometrics" Technology Review.

Symanovich, S. (2020). How Does Facial Recognition Work? Norton.

Thomas, R. (2005). Biometrics International Migrants and Human Rights (Global Migration Perspective, Vol.17).

Wamba, F. & Boeck, H. (2008). Enhancing Informa-mation flow in a retail supply chain using RFID and the EPC Network: A proof of concept approach.

Wasike, S. & Odhiambo, E. O. S. (2016). A Critique of the Usefulness of Theories in Explaining Socio-Political Phenomenon, Asian Journal of Basic and Applied Sciences Vol.3.