



Information System Infrastructure Management Influence On Cyber-Terrorism In Directorate Of Criminal Investigation, Nairobi County, Kenya.

Wabwire Godffrey Mukekhe (BA)

&

Dr. Peter Philip Wambua (PhD)

School of Security, Diplomacy and Peace Studies in Partial fulfilment of the requirements for award of a Master's Degree at Kenyatta University.

Date of Submission: 25-08-2022

Date of Acceptance: 07-09-2022

Abstract

Cyber terrorism having combined two concepts of “cyber” and “terrorism” refers to cyber space being the medium of orchestrating terrorist acts to wit; spread of online propaganda, alteration or destruction of information, planning and carrying out of terrorist’s attacks via the use of computer networks reigns respectively. Its therefore a complex contemporary matter. Information system infrastructure management being the collation of all interrelated elements for information flow within the organization on how it is planned, organized, staffed, directed and controlled to avert leakage to unauthorised persons. In regard to Directorate of criminal investigation, the flow should be timely and secure. The directorate had gradually advanced its Information Technology traversing from the Radio calls alias “over-over”, UHF and VHF pocket phones, signal communication to the modern world of computer networks where information is dispatched via emails, WhatsApp, twitter, face book and establishment of integrated command and control centre (IC3) within Nairobi and Mombasa cities. Based on above advancements, organization information infrastructure security is critical to combat the eminent danger of cyber-terrorism. In furtherance, the study corely intended to examine how information system infrastructure of the directorate of criminal investigation is managed to avert cyber terrorism attacks adversely boasted for social, emotional, psychological and economic impact hence driving the study’s core significance. Contextually, the subject matter under study beared a dynamic scope hence readily accepted in the current sphere. On orchestration mode and being a crime of the elites, post-modern theories namely the Actor network Theory (ANT) and Technological

Determinism (TD) were incorporated for phenomenal discussion. Consequently, descriptive survey design that targeted 100 respondents and ten (10) key informants drawn from the Directorate of Criminal Investigations at DCI headquarters was done through stratified technique. While encompassing both figurative and non-figurative data collection methods through filling of questionnaires and interview guide, the study output was subjected to validity and reliability tests cognizant of research ethical values. Moreover, specific objectives were postulated to examine the study traversing from finding out the influence of planning measures on cyber-terrorism in the Directorate, establishing the extent to which staffing needs affected the organization, determining how coordination efforts related to cyber-terrorism and finally establishing effects of controlling mechanism on cyber-terrorism in the directorate. Data was analysed with the help of SPSS software. Whose findings were: - low level of preparedness with minimal impetus to launch desirable approaches, flaws in system and high hardened transformative rigidity, moderate impediments on institutional engagements and insufficient controls. Based on above findings below recommendations were deduced; Need for instant rollout of information infrastructural plans, strive for capacity building in anti-cyber terrorism trainings, uplift of institutional collaborations and finally launch of robust control mechanisms.

Key Words: hacker, phreaker, phishing, cyber-crime, cyber-security, cyber war, cyber-attack, cyber-terrorism, information system.



I. INTRODUCTION

The chapter covered background of the study entailing discussion on both Cyber-Terrorism at global, regional, local perspectives and Kenya police service Directorate of Criminal Investigation information infrastructure. On-going digitalization process in the Directorate of Criminal Investigation called for clear understanding of the information security protocols (Gerardus, 2021). Both hardware and software management were key in addressing the contemporary Cyber-Terrorism challenge (Jerry, 2021). Human and non-human actors critical in the smooth flow of information given that the Directorate posited relevant intelligence and was custodian of critical security data. Premised on the same, the infrastructure could highly be vulnerable to cyber space attacks taking the form of Malware, propel of Viruses, worms, ransomware and spyware. Moreover, through the use of the internet, entrench into violent acts either threatened the loss of life or resulted into significant bodily harm for political or ideological gains (UNODC, 2019). This chapter hence analyzed the same and other forms of Cyber-Terrorism as influenced by the way information System Infrastructure was being Managed for guaranteed secure flow and robust database. In addition, it harboured the statement of the problem, study objectives, research questions, significance of study and its justification not forgetting the scope and limitations of study.

1.1 Background of the Study

The Kenyan constitution as promulgated 2010 chapter fourteen on National Security cements the foundation where the state was mandated to ensure safety of its citizens (The constitution of Kenya, 2010). In so doing was pegged on three National security divisions which encompassed National Intelligence Services, Kenya defence forces and National Police Service to achieve its mandate. To tackle cyberterrorism, it narrowed down to the respective constituent departments within National Police Service whose vision being “a world class dignified police service” and mission “provision of professional, community driven police service achieved through societal partnerships and vindication of rule of law for secure homesteads”. The service key values were integrity, justice, participation, equity, openness, accountability, and civility. Hence mandated to combat the menace. The cybercrime unit under the Directorate of Criminal Investigation and tasked to address contemporary issues of cyberterrorism had its headquarters at DCI offices along Kiambu road near Pangani and commanded by an Assistant Inspector

General (National police service act, (2011). In executing its mandate, the unit was bound by principles and values in the constitution more so article 244; which strived for the elevated standards of discipline and professionalism among its members, promoted transparency practices, averted corruption and accountability, complied with constitutional standards of fundamental freedoms and human rights, training of staff to peak levels of competency and integrity in respect of fundamental freedoms and human rights and finally endeavored to promote and foster relations with the entire society. (Constitution of Kenya, (2010). Similarly, article 238(1) of the said constitution on National security principles defined national security as the “protection over exterior and interior warnings of the country’s territorial integrity and sovereignty of inhabitants, freedoms, rights, stability, property, peace, and progress and any other unlisted national interest”. In actualization of the aforementioned, cyberterrorism through cyberattacks geared at hacking, phishing and denial of service occasioned by viruses, worms...as a contemporary security challenge ought to have been combated for a secure police information system infrastructure.

It was clearly depicted that there was need to review existing internal police information control policies and guidelines and formulate action plans, strategic plans, operation plans to be in tandem with the legislative framework to wit National police service act 2011 (NPSA, (2011), National security amendment act 2014, service standing orders (S.S.O) and cyber terrorism act which was recently conceived. Older crime prevention paradigms which had proved inefficient propelled on password change, encryption of classified information and minimal access provisions were subject to hacking threats, world spread malware, espionage hence making cyber terror versatile (Weimann, 2013). Its magnitude had entrenched all sectors; economically, had spearheaded losses in banking sector attributed to massive fraud activities, reception of classified police operation information which led to bungled operations not forgetting the instillation of social fear on when the next attack will be. Pegged on the above, there was need to examine how Directorate of Criminal Investigation system infrastructure was managed to avert cyber-attacks. In police organization, intelligence sharing was the order of the day and therefore its security critical to avert leakage. Cybersecurity being mode of protecting against unwarranted surveillance, assemble of intelligence from any information system. However, wherever directed towards potential initiators of



cybermanaces, the ventures are useful to help guarantee cybersafety. Moreover, surveillance for disposition and monitoring of information stream would be a pivotal element of cybersafety. (Computer Hope, 2012).

On orchestration mode, cyber-attacks are executed as simple-unstructured, advanced structured or complex coordinated. A survey of emerging threats in cyber-security by journal of computer and system sciences (Surya Nepal, (2014) allude significant growth of cyberattacks to exponential growth of internet interconnections. Hence need to re-examine the robustness of police organizational information infrastructure in relation to cyber terrorism attacks and guarantee information security. Attacks on police information infrastructure had severe repercussions to wit confidential operational information upon having been hacked lands to unintended audience posing as high-risk to the organization (Spurgin, 2016). Information flow within Directorate of Criminal investigations takes four frontiers namely: downward, upward, horizontal and on rare occasions diagonal (Alex Lyon, (2012). As a recap, downward information flow emanates from the top leadership position where instructions are shared to employees at lower levels which was vice versa of upward flow. Horizontal entails exchange of information across various departments in the organization while diagonal flow was a cross-functional communication between staffs working at different organizational levels. Police architectural information flow sequence was such that upon drafting the message in form of a signal on GP 216 official form, it was passed to next immediate command by reading its content via UHF or VHF radio communication gadgets being Standard operating Procedure (SOP, (2010). At the receiving end, it was re-drafted and handed over to destined addressee. However, with modernization where stations had acquired computers, the medium had changed as upon drafting the message they are relayed through e-mails; although the method is convenient, user-friendly, timely and resourceful; eminent cyber-attacks on the system result to severe repercussions to wit confidential operational information was prone to hacking thereby leaking to undesired audience posing a high risk to the organization. Projectorilly, computers are there to stay. According to the National police service commission strategic plan (2019-2022) on ICT “The commission planned to automate all its Human capital management processes to ensure speed, integrity, accountability and fairness in recruitment, appointment, promotion and discipline

for a dignified and efficient police service that will provide enabling environment for the economy to thrive”

1.1.1 Cyber-Terrorism

A raft of years had lapsed when experts and policymakers had expressed increasing concerns over protection of Information Communication Technology (ICT) systems from cyberattacks. (Casey Crane, (2018). Deliberate attempts by unsanctioned individuals from penetrating technological systems solely for damage, disruption, theft or other illicit actions. Some experts anticipated the numerical strength and magnitude of cyberattacks to had risen progressively with time (Guitton, 2020). Historically, terrorism being a global problem orchestrated its ruthless in-humane acts whose development was to be premised on vigilante groups advocating for social justice with a political connotation and grew to world threat networks like Al-Qaeda, ISIS, Boko-haram and Al-shaabab (T. Bjorgo, (2020). There strategies were propelled towards hauling of grenades, firing and bombing. Lately, the terrorist cells have tactically retracted to recruitment, radicalization denial of service, hacking and espionage activities manifested in the use of computers and electronic gadgets hence squarely lies in cyberterrorism triggering the need to avert the same (Lay cock, (2001). This emerging trend had much far damaging effect hence need to manage the information system infrastructure of the Directorate of Criminal Investigation to avert entrench of cyber-terrorism insurgency “the imminent commination posed by cyberterrorism had precipitated considerable anxiety. Countless experts in security field, members of the political class and other societal stakeholders had published the danger of cyber terrorists hacking into computer systems for private use, institutions of government and crippling the military service and financial sectors of developed economies” so captured in United Nations institute of peace report on how factual is cyberterrorism? An activity geared at protecting ICT systems and their contents was known as cybersecurity. Thus, protection of privacy in an electronic environment was to be achieved through good cybersecurity. Computer crimes began at the birth of the internet in 1983 (Shantosh Rout, (2008). At this particular year the momentous Morris Worm which was a denial-of-service operation exhibited through manipulation of Microsoft software, spyware and cyber espionage which instilled fear transnationally. Consequently, seven years later in 1990 the cyber terror hype alias



millennium bug was discovered. Globally series of attacks were experienced just to mention but a few in 2007 Estonia experienced a Denial of Service (D.O.S) that was politically motivated, in 2011 Norton cyber-crime characterized by phishing, D.O.S, propel of viruses and worms led to massive financial losses, Ukraine on his part suffered a swamped website in 2017 while Ransom ware frayed private companies and transpired to personal information leakage. Chronologically, the events of cyber-attacks have had far reaching ramifications to the economy of many countries. As a remedial action China formed the cyber blue team comprising of 30 elite internet specialists. However, they had been accused of penetrating secure online system of foreign nations; seen as un precedented penetration of online news into societies with no sign of stopping (Ann Nguyen, (2008). An aspect replicated in South Africa where hacker clique goes online, quickly gains reputation for by passing local cell network internet curtailment where authorities are unable to pin point the master minds behind the incidents; as South Africa anti-cyber terrorism vows to stay tune hoping one day will safe community from hackers, as narrated by South African minister for economic development and finance while announcing 80 separate fraud counts related to spyware and loss of 130m Rands (Government of South Africa, (2008). Locally, Kenya has not been spared neither. Hacking of organizations platform had become a norm; among those challenged by hacking included Kenya Defence Forces twitter account, "Huduma Namba" registration software, state house official communication platform and Safaricom data bundle system. Attesting the same on 1st July 2019 on release of Communication Authority of Kenya report (2018), the economic loss subscribed to hacking of Banks, sacco's and government agencies was quantified at 29.5 billion hence a rise of 8 billion in comparison to the previous year. This prompted the government of Kenya to launch presidential digital talent programme across the county to aid in combating the contemporary menace and offer employment to the internet youth survy population. (GOK, (2019).

Based on today's attacks we are left oblivious on who did it and when they intended to strike again (E. Kaspersky, (2006). Hence it was cyberterrorism but not cyber war. He further regarded the same to wide ranging cyber weapons, such as net traveler's virus and the flame virus which his firm divulged to biological weapons, in that with interconnected world, they are inherently catastrophic. Consequently, technololytics institute attribute cyber terrorism to the premeditated

application for destructive ventures, or the warning thereof, in opposition to computer grid. purposefully aimed at causing social, ideological, political, religious harms or similar schemes destined to frighten any individual in furtherance of the said objectives. (Ios Press, (2008). On execution, included utilization of information technology to regiment and relay attacks on networks, telecommunication systems and computer infrastructure, perhaps for exchange of information or propelling electronical threats. Case in point was hacking into computer systems, introduction of viruses to vulnerable networks, denial of essential services attacks, website defacing or terroristic threat made via electronic medium of communication. Complex- coordinated Cyber-terror attacks possessed capability of coordinated attacks capable of causing mass-interruptions over integrated and heterogeneous defences as well as ability to generate complex hacking devices (cryptography), organization learning capability and highly capable target analyzed commanded control. Depicting lack of modern cryptography techniques for data security control (Christof Paar, Jan Pelzl, (2010).

1.1.2 Information Security

Embarking on the contentious aspect of (INFOSEC) Information System Security which entails methodologies and procedures involved in keeping availed information, secrecy, and satisfy its integrity; overseeing access dominance by preventing unauthorized staff from penetrating organization's systems. In so doing, organizations needed to systematize this discipline while professionals and academics ought to collaborate to offer policies, guidance and uplift of industrial standards on antivirus softwares, passwords, encryption software, firewall, legal liability, training and security awareness (Pathan, (2020). Systematization may be in the long run driven by a multitude of regulatory provisions that affect how data is accessed, stored, processed, transferred and destroyed. Its implementation on guidance and standards within an entity may however be hindered if the practice of advancement wasn't adopted. As alluded in D Trcek book titled "Managing information system security and privacy" (Trcek D, (2006). Information System Management (ISM) recount controls that any organization requires to implement for it to be sensible in protecting the confidentiality, integrity of assets from threats, availability and vulnerabilities being cognizant of the cyber-terrorism danger. Through the ISM systems assessment of risks was conducted where



protection of assets, management as well as dissemination of the risks to all appropriate members was done. An extension of ISM was ISMS which referred to Information Security Management System and represented the collection of all interacting / interrelated information security components of an organization do as to guarantee procedures, policies and objectives was to be created, communicated, implemented and evaluated for better organization's overall information security. The arrangement was typically determined by organization's objectives, needs, security requirements, processes and size (Obrien A James, (2005).

1.2 Statement of the Problem

Analogue information system infrastructure entailed dispatch of messages from one command to the other via (VHF) or (UHF) being very high frequency or ultra-high frequency respectively through radio pocket phones. Medium architecture was such that contents of message were directed to a control room (located at each sub-county) and later re-directed to the designated recipient. The system efficiency relied on signal strength subject to influence of weather condition while information accuracy depended on English command of signaller. Mouse code and Fax machines relayed confidential messages. However, in modernized era, each command had acquired a functional computer and information transmitted through e-mails, social platforms like WhatsApp and twitter with a modern control room namely integrated control and command Centre currently within Nairobi and Mombasa cities. Often information is dispatched more conveniently from end to end through e-mail accounts leaving the official directorate communication infrastructure (analogue system) with minimal operations and staffed with technologically challenged operators (Ransley, (2009). An idea echoed by the national taskforce on police reforms chaired by hon. Mr. Justice (rtd) Philip Ransley "Increase of the use of IT in the commission of crimes including complex frauds, computer hacking, credit card scams, spreading of computer viruses, facilitation of human trafficking and child pornography using internet" A problem further alarmed by recommendation that police officers lack most basic ICT knowledge on page 164 in the said report. (Ransley, (2009). Premised on the a forementioned, the second study objective geared at establishing how staffing needs affected cyberterrorism in the Directorate of Criminal Investigation is key in filling the gap. Initially, the directorate information department was

semi-autonomous, but with devolution spirit gaining momentum; supervision / monitoring of information flow, profiling, vetting of staff and re-training had become the order of the day for robust information security measures. According to Abraham Wagner and Nicholas Rostow in their book *Cyber security and cyber law* (2020), developments in communication and information technology along with introduction of new media, have had an enormous impact on almost all aspects of modern life... the rapid evolution of cyber space has left vulnerabilities to fraud, abuse and crime as well as new venue for warfare and espionage" (Wagner A (2020). Hence reinforcing the need to safeguard our information infrastructure as intended by the study. Similar sentiments echoed by April Falcon Doss in his book titled *Cyber Privacy- who has your data and why you should care*. "No matter who we are or where we go someone is collecting our data; to profile us, target us, assess us, to predict our behaviour and analyze our attitude to influence the things to do and buy" (Falcon Doss, (2020). In regard to hacking the "Art of exploitation provision on insight of network communications and current hacking techniques" highlighted seven schematic security measures being use of strong passwords, control access, firewall installation, security software, program up-date, intrusion monitoring and raising awareness (Jon Erickson, (2019). These measures were solely system oriented with little emphasis on human force precisely influence of planning measures on cyber-terrorism, extent of staffing needs, coordination efforts relations and establishment of controlling mechanism on cyber-terrorism.

Based on Tech beacons guidelines to security operations opportunities and challenges in relation to report on state of security operations (Beacons, (2019) whose recommendations summed up five remedial measures captured as "5 contemporary security technologies set to level the battle field" namely: -User behaviour analytics, hardware authentication, Data loss prevention, Cloud and Deep learning. Surprisingly, all above attributes are inadequately practiced. In addition, based on recommendations on natural academies of sciences engineering and medicine (Sem I, (2020) on protection of individual privacy in the scuffle against terrorism: a framework set for program assessment, premised 4 and 5 advocates for serious research in green field of cyber terrorism thereby triggering research course on the contemporary matter.

The study therefore intended to examine the entire directorate's information infrastructural



management and its influence on cyber-Terrorism as depicted below on study objectives.

1.3 Objectives of the Study

1.3.1 General Objective

The general objective was to examine how Directorate of Criminal Investigation information system infrastructure is managed and its influence on cyber terrorism.

1.3.2 Specific Objectives: -

- i. To explore influence of planning measures on cyber-terrorism in the Directorate of Criminal investigation.
- ii. To establish how staffing needs affected cyber-terrorism in the Directorate of Criminal investigation.
- iii. To determine how coordinating efforts, related to cyber terrorism in the Directorate of Criminal investigation.
- iv. To establish effects of controlling mechanism on cyberterrorism in the Directorate of Criminal investigation.

1.4 Research Questions

- i. What was the effect of planned measures on cyberterrorism in the Directorate of criminal investigation?
- ii. To what extent did staffing needs affect cyberterrorism in the Directorate of Criminal investigation?
- iii. How did coordination efforts relate to cyberterrorism in the Directorate of Criminal investigation?
- iv. What were the effects of controlling mechanism to cyberterrorism in the Directorate of Criminal investigation?

1.5 Significance of Study

Thinking of the repercussions of the cyber-terrorist attack (loss of livelihood, public fear, destroyed information base, shortage of resources to counter and all forms of economic loses). This becomes timely research on a contemporary field "entrench of cyber-terror insurgency on Directorate of Criminal investigation information system infrastructure" the impact traverses from social setting, emotional and psychological effects to economic impact. Adversely affected by cyber-terror attacks are organizations, financial and learning institutions hence need to conduct this research as a control mechanism within the Directorate. Government and non-governmental organizations fall prey to cyber-terror, banking sector, universities, colleges and cooperative societies aren't safe neither; in short, the society entirely is at stake. Consequently, the study was

carried out at a time the Directorate of Criminal investigation has no steady fast policy on information control vis-a-vis cyber-terror attacks. As part of pioneer studies, its findings will be a major milestone to the organization to wit filling the information gap and driving formulation of desired institution information control policy not forgetting a source of reference to future scholars and broadening the academia scope.

1.6 Scope of the Study

As depicted earlier, the study intended to cover information infrastructure of Directorate of Criminal investigation organization, how secure the system was in relation to cyber terror attacks. Geographically, Anti-Cyber-crime unit at DCI headquarters Kiambu formed a large population during data collection and findings were beneficial to the matter organization. Similar challenges experienced in other organizations, agencies and institutions traversing from the Banking sector, Saccos, learning sector, insurance companies vulnerable to hacking were to obtain valuable information in streamlining their proactive preparedness. Contextually, the matter being studied beared a dynamic scope whose findings and recommendations were to be readily applicable. On methodological scope, post-modern theories applying both figurative and non-figurative approaches were used to guarantee credible output.

1.7 Limitation and Delimitations of the Study

Given the contemporary field researched on, and organization studied. That is the "Directorate of Criminal investigation" and respondents being security experts; many respondents tented to shy off on sharing their experiences. However, the researcher endeavored to convince them that the information received was purposefully to be utilized on academic arena and confidentiality was to be observed. In this regard credible meaningful output was delivered to address the research questions. Information that beared sub-iudice restrictions and short time interval of research were anticipated challenges; the latter was overcome through deployment of two research assistants.

1.8 Organization of the Study

Research project is divided into Five chapters. The first chapter of the study consists of the study background on cyberterrorism, Information system management, Directorate of Criminal investigation information infrastructure,



problem statement, study objectives (general and specific), questions of research, significance of study, scope and study limitations and delimitations. Chapter two reviews literature and theories and similarly covered empirical reviews, research gaps and conceptual framework, while chapter three looks at research methodology/ design / site, techniques of sampling, data collection methods and instruments, data organization analysis not forgetting considerations on ethics. Chapter four analyses and interprets data by outlining the response rate and presenting reliability results. It also covers respondent's general information basically on age, gender, marital status, level of education, ranking, placement and length of service. Consequently, the chapter demonstrates respondent's perception on influence on planning measures on cyber-terrorism, how coordination efforts related to cyber-terrorism and effects of controlling mechanism on cyber-terrorism which were presented on the Likert charts. Finally, chapter five hosted the summary, conclusions, recommendations and area of further research.

II. LITERATURE REVIEW

The chapter discusses literature review by highlighting key study variables on how Information System Infrastructure especially internet network vulnerabilities escalate cyberattacks. Consequently, theoretical review of two theories the Actor Network Theory and Technological Determinism. Finally, it provides a summary of research gaps and conceptual framework.

2.1 Literature Review

2.1.1 Information System Infrastructure Management and Cyber Terrorism

Information system in short (IS) by definition, was official, socio technical, organizational system designed for collection, processing, storage and distribution of information (Rascao JP, (2017). In a sociotechnical view information system encompass five components namely software, hardware, network, database and people which amalgamate to perform input, process, output, feedback and control roles (Wiley, (2018). On the other hand, Management Information System abbreviated as (MIS) being a computer structure encompassing both hardware and software serves as the back born of the organizational chores. A MIS is geared at gathering sets of data from multiple online sources, it analyzed information thereafter relayed instrumental reports in management of decision making and strategies in

corporate information management (Warren, (2003). Information infrastructure was a shared one, open, evolved, standardized and a heterogenous installed foundation (Ole Hanseth, (2002). Echoed by Pironti "as the entire people, procedures, processes, facilities, tools and technology which support the creation, storage, use, transport and destruction of information" (Pironti, (2006). In regard to information infrastructure, it included the health systems, internet and corporate systems extending to innovations such as LinkedIn, Face book and Myspace as best examples (Bygstad, (2008). Global Information Infrastructure (GII) being the developing communication framework intended to connect all telecommunication and computer systems world-wide. Often mentioned as pond of networks, eventually was geared at ensuring all electronically transmitted or stored information accessible from every corner on the planet. Consequently, the internet upon being carefully thought was currently the de facto global information infrastructure (Michael Rustad, (2009). However, to prompt evolution of GII as envisioned, either the internet or its successor was to deal with challenging issues like privacy, safety, software and hardware compatibility, conversions, rights to identity management, information, Digital Rights Management (DRM), governance and rivalry. An idea propelled by Borgman L. Christine, having authored from Gutenberg destined to global infrastructural, information access in networked era (Borgman L Christine, (2017).

Technology usage for example internet is "a daily bread" having exponentially grown hence of paramount importance requiring strategic controls. Internet being the driver of remunerative prowess need to be safe and open to all. Browsing challenges had proportionally been availed. Communal vulnerability and addictive state key therefore overseeing network administration necessity. Players in the field should foster proper application of technology, system safety and upgrading as integral role. Such events will lead to a well-founded network. Swift development of net had seen emergency of new openings for committing universal cyber malware. Exploratively, integral susceptibilities in always changing space have seen; broadband internet signal widened, emergency of cyber related concerns and need to ensure that citizens, government and organizations are safe. Africa continent is facing a handful of net-affiliated concerns in safety grounds to control and prevent space risks; warnings of such nature can be handled by instituting a formidable cyber safety



culture, formulation of robust response capabilities and enacting appropriate and effective policies nationally. Cybercrime is not a “thing” it is a vector a channel through which others can harm governments, businesses, and our personal lives (Seymour Bosworth, (2002). Net maneuver was a beneficiary of the internet fabric, which enabled computers around the world to communicate with each other via (ISP) internet service providers. Computers interconnection systems linked to the internet through ISPs are assigned unique internet protocol (IP) addresses, which may offer static or dynamic. Computers communicate over the internet by contacting other computers using the IP addresses of those computers to identify them. Information was then exchanged among computers identified by their IP addresses, via packets of information that are sent over the internet between the two devices. The duo cyber-criminals and cyber-terrorists differed only in their motive. Both used the open structure of the internet and same methods to occasion harm. Orchestrated through hacking “a breaking and entering into a computer system to steal information”. Cyber-attack (viruses and malware) being harmful software programs and files that are implanted onto computers enabling bad actors to damage the infected computers or use of the infected computers to steal information and harm others through Distributed Denial of Service (DDOS) attacks on intended victims’ website. Holistically ideas captured in IT Systems management (Rich Schiesser, (2010) and Management IT investment (Kenneth Moskowitz, (2003).

2.1.2 Planning Measure and Cyber terrorism

Planning being a managerial process, concerned with defining set goals for the organization’s (Directorate of Criminal investigation) future policy direction and determining the mission (information system infrastructure security management against cyber-terrorism) and resources to achieve the target. Hence Institution Managers ought to have developed plans to achieve set goals and targets. It revolved on identification of resources available for the project and optimally achieving best scenario results done strategically as per dictates in United states of America National cyber strategy (UNANC, (2018). Information system component entail computer hardware, software, telecommunications, databases and internet. The internet being a volatile tool used by cyber terrorists to plan and finance terrorist activities. In addition, training of newly recruited members, communication, research,

reconnoiter disseminate propaganda; potential targets and incite others execute terrorism acts. It therefore urgently calls for Directorate of Criminal Investigation department to establish a framework that improves interoperability among constituent enforcement agencies. Emulating ideas on resources, cyber security attacks and defense strategies (Dan Lohmann, (2020). Consequently, proactively develop plans in tandem to the global multi-jurisdictional cybercrime operations to address prevalent cyber-crime threats. Such plans should similarly identify operational needs for law execution representatives. Through viable planning geared at amicably addressing the menace, there is need to develop organization strategy putting into consideration the international police (Interpol) ratifications and degrees (Michael Fooner, (2020). That ought to heed of national safety of space technological soundness and formulate strategies that will strive for information secrecy by initiating robust mechanism for protection of personal data. In order to guard over severe threats attacks of cyber-terror, acceleration of institutional infrastructural reforms and implementation of raft measures ought to be spearheaded. Formulation of operational action plans key for combating cybercrime and draft review of cyber regulations to criminalize offences related to ICTs abuse and its illicit use. An idea echoed in “evaluating risks of cyber terrorism, cyber threats and other cyber wars (James Lewis, (2002). To guarantee effective criminal justice reactions to threats presented by terrorists via the internet with a focus on unlawful criminalized acts, provision of investigative powers for law enforcement agencies against terrorist and other related investigations, regulation of internet related services like ISP and control content, development of specialized judicial / evidential procedures will be paramount. Plans to safeguard forensic data preservation and recovery for purposes of prosecution plus protection of sensitive information ought to be formulated. Application of blue ocean strategy as remedial action. (Maxi Macdongne, (2004).

2.1.3 Staffing Needs and Cyber Terrorism

In order to enable Directorate of Criminal Investigation department, protect its critical infrastructure and build capacity in rejoinder to upsurge of risks in space; there stands an urgent need to create organizational capabilities in cyber security, manufacturing sensitively well-informed manpower to lessen chances. Therefore, law enforcement officials mandated to investigate internet related crimes required acquaintance of



specialist training, skills in the technical aspects of how terrorists and other criminals can deploy net in furtherance of illicit functions. Shifting the paradigm, a robustly equipped policing enforcement unit was to effectively rely on the internet as a resource to monitor obnoxious activities of terrorist groups across the net. Principles of unit operation key (Alan, (2012). Directorate of Criminal Investigation in addressing the concern should not only increase the numerical strength of personnel but take into consideration the expertise aspect. Staffing needs should provide expertise in anti-cybercrime operation field (Marleen Weulen, (2018). Enhancement of technical capabilities to monitor and defend departmental networks. Consequently, there was need to launch an all-inclusive and detailed sensitization program including civic awareness crusades nationally and preventive estimates at any scope in alleviating space dangers. By enjoining recognizable attempts to push for setting up training and education programs in cyber security, ICT forensics, cyber-crime investigations, counter-terrorism and various specialized education being timely. Staffing and corruption have a direct correlation hence need to vet staff in this critical sector of deployment and ensure plans are in place to enhance corruption free unit (UNODC, (2013).

2.1.4 Coordination Efforts and Cyber Terrorism

Considering the replica dimensional and complexity of cybersecurity, planetary protecting of illicit schemes across internet; necessitate collaboration and harmonization pegged on a pool of players both of internal and external jurisdictional connotation. Reference to the need of ICT enterprise and its constructive effect on the socio-economic state empowerment, it prompts imperative necessity to develop universal undertaking and steadfast techniques on cyber safety at worldwide scope to guarantee information safety and peaceful society. Similar to the Evolutional cooperate matrix. Its worth noting that information security form a critical component of enterprise workflows and considerations. without information security, enterprises are at the mercy of hackers (who have little mercy to spare) (Ben Canner, (2020). Coordination was a paramount component hence strides towards improving security procedures for cybercrime probe, technologically adduced evidence management and key stake-holders collaboration. Need to promote dialogue with cyber security actors and coordinate all initiatives related to cyber-security. Facilitate the communal or personal information exchange and

adopt support of law enforcement actors and internet service provider -ISP (Orhan Ergun, (2019). Cyber-terrorism being global scourge, need to encourage interstate collaboration through coordinated and concerted efforts not limited to international cooperation, enlightening on awareness for expanding knowledge and understanding of all the challenges posed by terrorist attacks in order to better procedures for attacks of such nature against pivotal infrastructure. Furthermore, promote reliable effective exchange of information and extraction of digital analysis for divergent use. Nationally, there is need for institutional collaboration and avoid inter agency conflict especially on command and control (Murat Dogral, (2011) in his book developing universal cyber cooperation defenses.

2.1.5 Controlling Mechanism and Cyber Terrorism

Cyber space has become a vital component on contemporary world at large. However, its merit partner with rising recorded warnings on cyber occurrences, prompting urgent respective governmental indulgence in addressing the menace. Stringent measures ought to be put in place to ensure efficient investigation and combat of cybercrime at national level through enforcement of existing regulations to deter violators. More so in adapting to materiality of electronic era to amicably handle elements of cyber-crime and cyberattacks. Targeted attacks are aimed at particular individual, group or type of site or service. Unlike worms and viruses that usually attack indiscriminately, targeted attacks involve intelligence-gathering and planning to a degree that drastically changes its profile. (Aditya Sood, (2014). Within the region, necessitates formulation of blue prints and regulations that strive to instill order in prone and polarized ICT sector. As a restrictive framework, there is need to shield key organizations and endeavor to offer services with integrity. Moreover, infrastructural controls are fundamental in monitoring threats and thereby efficiently responding too. In the book of vibrations: analysis and control mechanism (Rene Sara, (2015) strived for need to assess most often, check on efficiency of legislations in the system while maintaining statistics. Similarly, need to establish policy frameworks and legislative controls by either formulating (CERT) Computer Emergency response Teams or (CSIRT) Computer Security Incident Response Team. Deficiencies in username and password can be addressed by hardware authentication. Incorporating and installation of



VPro processor (6th generation core) which combined a series of hardware enhanced elements key for validation of a user's identity and also through User behaviour analytics. Engineering to more secure systems like (SCADA) for managing technologies for emergency responders and critical physical data. In today's litigious business world, cyber-related matters could land in court (Tari Schreider, (2010). It is therefore important to be privy to the legal duty to act reasonably and responsibly to protect assets and information by identifying cyber security government regulations, upgraded policies to comply with state, federal and regulatory statutes. Equally alarming is the prospect of terrorist designing computer software for government agencies United states institute of peace special report (USA, 2004). Psychological, Political and Economic forces had combined to promote the fear of Cyber Terrorism. It was mapped as the fast-growing field of research that emerged since 9/11, identifying both analytical advancements and key challenges that remain among them funding (Erica Chenoweth, (2019). Hence the study conceptually identified government regulations, political climate and funding being intervening variables as above discussed.

2.2 Theoretical Review

2.2.1. The Actor Network Theory (ANT)

A theoretical and methodological constructivists approach to social theory; propelled by science and technology scholars Callon Michel, Latour Bruno and Low John bestowed on assumption that things socially and in natural world exists in continually shifting systems of relationships. It posits that none subsist beyond those connections. Proponents of the theory (Taylor, Van Every, (1993) alluded that innovation was key to service performance. Currently with a dynamic science field underlying operativeness of service structures, and design latest conceptual apprehension and its theoretical underpinnings were vital in systematic demonstration of the nature of behaviour of service set-ups. Development and adoption of service upheaval demand the integration of several element actors like technologies, human resource and networks across various organizations idea seconded by (Brumman. B (2007). The innovation process encompassed getting up to date ideas readily accepted for adoption and use. Organization's state of reliance on (IT) was rapidly momentous. Its strategy (IT) was initiated and implemented for particular purposes by various organizations. Hence expectations were rife to the fact that with the presence of network of actors

within the computing environment, where such network of actors were key to understanding many otherwise unprecedented situations during the development and implementation of IT strategy a perspective of (Plesner, U. (2009). The network of actors possessed marshal interests. Majority of organizations were developing and implementing their IT strategy, whilst little was known about the network of actors and their impacts, which this study revealed. The study described how ANT was employed to probe the impact of network of actors on the development and implementation of IT strategy in an organization. ANT being the best alternative in provision of relevant perspective on the importance of relationship between both non-human actors and human (La vigne, M. (2003). In adopting ANT, the theory association revolved on neutral affinity with the IS discipline as its grounded-on correlation of ontology which assumed "constrative inter-twinning and reciprocal inter-definition of material agency and human" so captured by (Pickering, (1995). It enabled modifications, analysis of the conditions and constraints of agency within networks that intertwine the language, humans, culture, technology and artifacts. On relevance, ANT was deployed as a theoretical lens to evaluate development and adoption of service innovation (Arthur Tattnell, (2002). ANT was a heterogenous amalgamation of social actors, textual and conceptual. Similarly, it provided a conceptual framework to aid in formulating and building a design methodology that reinforced the concept of development and adoption of service innovation. ANT permitted execution of open-ended array of items for alignment including work routines, system modules, incertive structures and organizational roles (Rodgers S. (2015). Hence a fundamental theory in strategy design formulation and re-adjustments of interests in regard to network of actors. Critique of ANT among them (Barbara Czarnowski, (2004) and (Bardini, (2007) cited absurdity of assigning agency to non-human actors, moral and assumption of all actors being equal as pointless. The cyber-terrorists would at a point ideologically network in the dynamic technological world to orchestrate planned illicit functions. Modern theoretical underpinnings and conceptual understanding provided for systematic explanation of its nature and behaviour in service structures. The study utilized translation notion introduced in ANT literature to study cyber terror attacks. It aimed at understanding the entire police information system infrastructure development trajectory by



seeking to disclose a variety of elements that shape the course in countering cyber terror attacks.

2.2.2 The Technological Determinism Theory

Reductionist's theory by Thorsten Veblen of Technological Determinism assumed that technology in the society determined the development of its cultural values and social structure. Generally, the idea was supported by (Peter D. Hershock, (2010) in that technology being machine driven, caused historical change by changing the human existence and material condition. The theory sought to highlight technical evolutions, media or technology as a whole, as the key mover of history and social change. As subscribed by "hyperglobalists" who claimed that as a consequence of the wide availability of technology accelerated globalizations was inevitable therefore technological development and innovation become the principal mover of social, economic and political change. TD equated technology to a timely idea, hence unstoppable. Therefore, unable to control technology (Lalia Green, (2002). This suggested that people are somehow powerless and society allows technology to drive social changes because societies failed to be aware of the alternatives to the values embedded in it a matter subjected for approval or otherwise by the study. It presumed that cultural values and social structure development was driven by society's technology. Similarly propelled by (EH Schein, (2018) inevitability thesis. The theory posits dual general ideas, firstly that the advancement in technology itself follows a predictable, traceable path largely far away from political and cultural influence and secondly that technology in turn possessed "effects" or societies that are inherent, rather than socially conditioned / manufactured because that society organizes itself to support and further develop technology once initiated. TD usually asserted on the present as projection into the future as "we were choiceless in regard to adoption of technology". consequently, a theoretical approach towards the study of technological developments and cultural effects ideas propelled by (Mupie, Andrew, Potts, John, (2003). The focus was aligned on how modern technology creates a new possibility and potential for human activities and thought. Technology was perceived in four areas; processes, structures, people and organizational culture. Furthermore, a collation of relationship was made where either technology influenced society or vice versa or technology both influenced and was influenced by society. Critiques of the theory perceived it as monistic (non-causal),

as minimizes the arguments to cause and effect. It was often very suggestive and appealing. (Lewis manifold, (2007) argued that relating technology to tools and machines was itself reductionist. on relevance, the theory stated that technology precisely media-decisively shaped how individuals feel, think and act and how societies organized themselves and operated. in so doing the theory was premised on basic ideas of assertions that: - new electronic media radically impacted on how we thought, felled and acted; therefore, the world would never be the same, electronic era superseded tribal, illiterate and print ages; inventions in modes of communications shaped human existence and finally believed that media and extensions of human faculties would amplify bodily sense.

2.3 Summary of Research Gaps

Global contemporary policing issues an outline of comprehensive overview of key challenges faced by the police dwelled. It further addressed six areas of policing; performance management, professionalism and academic partnerships, preventing and fighting crime and terrorism, immigrant and multicultural populations, policing the police and cyber security. (John Etermo, (2019). In terms of their measurement of performance; in Kenya few researches have been done on matter concerning contemporary policing challenges "cyber-terrorism". It had been noted that the challenges facing Directorate of Criminal Investigation could be looking obvious but the problems continue to permit. There have been no thorough studies and opinions on almost each of the challenges. There was need to explore the possibility of overcoming the challenges. The study therefore sought to exhaustively explore impending challenges and route way forward. This study was also able to test the applicability of the reforms on restructuring which were on-going in the entire police service suggestions put forward by other researchers and have not been considered were also put forward. This chapter dwelt at length on the background of cyber-terrorism, strategies deployed to overcome and rid out terrorism, effects of terrorism to development and how technology had affected cyber-terrorism. All in all, the approaches so discussed were pegged on the presumption that cyber-terrorism had both internal and external connotation. They strike against security agents who responded towards addressing the problem. This therefore prompted a gap in the approach especially when the cyber-terrorists orchestrate their intended mission. The aforementioned approaches would have been rendered fruitless without taking a



new dimension to counter the same. The Directorate's lack of specific network allocation from the Communication Authority of Kenya and Data base administrators increases the level of vulnerability that ought to be gapped. With the current predicament the new twist on cyber-terrorism planning which had occasioned recruitment of security agents either actively or inactive cells; calls for urgent stringent measures to

counter the same hence need to fill the prevailing gap of contemporary challenge "security information system infrastructure management against cyber-terrorism". It possessed the need to re-examine the planning, staffing needs, coordination efforts and controlling mechanism in the Directorate of Criminal Investigation in combating cyber-terrorism.

2.4 Conceptual Framework

Independent Variable

Dependent

Infrastructure Management

Planning

- Achieved set goals & targets.
- Developed specialized Mgt skills.
- Safeguarded forensic data preservation.
- Launched strategic approaches.

Cyber Terrorism
Prevent D.O.S
Prevented phishing
Minimized hacking
Fought espionage

Staffing Needs

- Enhanced best recruitment practices.
- Specialized training.
- Oversaw corruption free management.
- Undertook continuous vetting.

Coordinating efforts

- Fostered departmental cooperation (actors).
- Reduced interagency conflict.

Intervening Variable
Government

regulations

- Increased inform & intelligence sharing.
- Promoted bilateral / multilateral relations

Political climate
funding

Controlling Mechanism

- Policy harmonization
- Promoted efficient legislation.
- Developed robust access control systems

FIGURE 2.1: CONCEPTUAL FRAMEWORK; SOURCE: RESEARCHER (2021)

III. RESEARCH METHODOLOGY

3.1 Research Design

Research design being a set of methods and procedures used in collecting and analyzing measures of the variables specified in the research problem were defined by (Andrew B kirumbi, (2018). In a nutshell, the study used descriptive survey research design. This design was appropriate for the study in that it permitted the researcher to use broader options of research methods to investigate one or more variables. Through descriptive science as propelled by (Casadevall, Arturo, Fang, Ferric C, (2008) observed and measured variables. In furtherance, they asserted that the method was useful in

identifying characteristics, frequencies, trends and categories making it appropriate choice. Descriptive survey was credited for evaluating satisfaction within company products / organizational services; relevant to the research topic as gave descriptive perceptions on how information system infrastructure was managed in Kenya police service and its influence on cyber-terrorism. Daniel J. Boudah, (2010) argued that descriptive research was used to describe the features of or provide a picture of a condition or phenomenon. Researchers who conducted descriptive research did not manipulate the subject of study in order to determine cause and effect.



3.2 Research Site

The research was conducted at the Department of Directorate of Criminal Investigations headquarters within Kiambu county and targeted members of the directorate, and experts. This is a semi-autonomous unit of National Police Service to which Anti-Cybercrime unit falls. The DCI headquarters was established in 1926 and situated along Pangani-Kiambu road approximately 3km from Pangani police station. The Directorate hosts among other departments the Anti-terrorist police unit (ATPU), Special Crime prevention Unit (SCPU), Bank fraud unit (BFU), Homicide unit, Ballistics and Fingerprint bureau.

3.3 Target Population

The researcher targeted a population of 290 respondents with a sample size of 100 and ten (10) Key informants through census survey. Research respondents were varied pegged on ranks, duties and position held in the Directorate of criminal investigation department. The sample population comprised of detectives, Data base managers, human capital staff, experts, signalers, anti-cybercrime personnel, senior section detective commanders and specific members of Directorate of criminal unit. Ten (10) Key informants were drawn from the head of commands at detective's managerial level reflected as tabulated below.

Table 3.1 Questionnaires Target:

RESPONDENTS	SAMPLE SIZE	PERCENT
DETECTIVE CONSTABLES	40	40%
DETECTIVE CORPORALS	20	20%
DETECTIVE SEARGENTS	10	10%
DETECTIVE INSPECTORS	10	10%
DATA BASE MANAGER	10	10%
HUMAN CAPITAL STAFF	10	10%
TOTAL	100	100%

Source: Researcher (2021)

Table 3.2 Key Informants Target

DEPARTMENTAL HEAD	QTY	DEPARTMENTAL HEAD	QTY
Directorate of Human Capital	1	Economic Crime Unit (ECCU)	1
Data Base Bureau Manager	1	Serious Crime Unit	1
Anti-Terrorism Police Unit	1	Forensic Document Examiner	1
Forensic Ballistics	1	Homicide	1
Photographic Imaging & Acoustic	1	Cyber-Terrorism Unit	1

Source: Researcher (2021)

3.4 Sampling Technique

Since population constituted distinct categories of expertise drawn from various ranks; stratified sampling technique was appropriate therefore deployed. It ensured that each sub-group of the overall population was best represented by capturing key population characteristics of the sample.

3.5 Data Collection Instruments

The research instrument for the quantitative survey study was a questionnaire. Merited as alluded in advances in questionnaire design, development, evaluation and testing. (Amanda Wilmot, (2019). Basically, questionnaires are easy

to administer and analyze therefore time saving prompting the choice. They are known to produce valid and reliable output especially when research assistants are incorporated. The questionnaire design incorporated open-ended sections to capture respondents' genuine opinion for a more defined outcome. Semi-structured interview schedule was used for an in-depth information collection. Interviews are one on one interactive type of data collection from which the interviewer asks designed questions to the target persons to obtain appropriate answers to the study problem (Kerlinger and Lee, (2000). Interview schedules were planned for 10 key informants drawn from the population. The same was achieved upon clearance to collect data



by dean graduate school of Kenyatta university and further licensing by Director General National Commission for Science, Technology and innovation.

3.6 Validity and Reliability of Research Instrument

3.6.1. Validity of research instrument

Content validation by definition refers to a process that aimed to provide assurance that an instrument measured the content area it is expected to measure (Orodho, (2017). The content validity of the instrument was determined through involving the expertise and knowledge of the supervisor. A four-point scale of relevant, quite relevant, somewhat relevant and not relevant were administered to a population different from the one under study (Kenyatta university security class, (2015) but bearing similar characteristics to give views on the relevance; whose outcome was dominated by relevant in addition to expert opinions.

3.6.2 Reliability of research instrument

Reliability being the extent to which a measurement is free of variable error and was usually achieved when repeated measures of the same variable show limited variation (Koribo and Trump (2006). In order to test the reliability of the instrument to be used in the study, two pilot studies were carried out and a reliability coefficient computed. This was to establish the extent by which the questionnaires elicit the same responses every time it was administered (Cooper, (2011). Based on pre-testing data and Cronbach's alpha score the reliability will be examined. In adherence to Cronbach alpha range; a score between 0 to 0.6 indicate low reliability while from 0.7 to 1 show high level of internal consistency.

3.7 Data Collection Procedures

On the first material day, the researcher started by explaining the purpose of the study to all the respondents who were to be targeted. The researcher then administered the questionnaires and allowed the respondents one hour to fill them. The researcher engaged two research assistants who helped in collecting data from the members. Researcher assistance were recruited to assist since the area to be covered was composed of departments. On completion, the researcher collected the questionnaires and interview guides from the respondents.

3.8 Data Analysis and Presentation

Since the survey was geared at collecting both figurative and non-figurative information on how information system infrastructure management influenced cyber-terrorism within the Directorate. In presentation, quantitative data was analyzed using descriptive statistics including table of frequencies, percentages, cross tabulation and Pearson's chi-square with the aid of statistical programs for social sciences (SPSS). However qualitative data from key informant interviews and in-depth interviews was studied and summarized to meet the research's objectives. Unstructured components were to be analyzed manually along major concepts and themes, and the results was presented using descriptive statistics and inferential statistics. Correlation coefficient by use of regression equation was deployed where an equation like model was used to represent the pattern in the data hence explaining the variable relationship as derived below. Conclusions were drawn from the analyzed data, leading to recommendations and resolutions.

$$Y_i = \beta_0 + \beta_1 X_i + \epsilon_i$$

Diagram illustrating the regression equation $Y_i = \beta_0 + \beta_1 X_i + \epsilon_i$ with labels for each component:

- Dependent Variable: Y_i
- Population Y intercept: β_0
- Population Slope Coefficient: β_1
- Independent Variable: X_i
- Random Error term: ϵ_i

The equation is divided into two components:

- Linear component: $\beta_0 + \beta_1 X_i$
- Random Error component: ϵ_i

3.9 Ethical Considerations

Resnik (2011) described ethical considerations as a measure for conduct that

recognized and distinguished acceptable and unacceptable behaviour. Prior to conducting the study, the researcher did obtain written permission



to conduct the study from Kenyatta University and National Council of science, technology and innovation. The researcher also obtained permission from the respondents; the researcher explained to the respondents the purpose of the study. The researcher was to share the research findings after conclusion of the research to the appropriate stakeholders that had interest in the outcome of this study. The researcher was to observe three principles, viz.; confidentiality, anonymity and use of data collected for academic purposes only.

IV. DATA ANALYSIS AND INTERPRETATION

4.1 Introduction

The chapter analyses data, interpretes results, offers the response rate and reliability test results. Consequently, it displays respondent demographic, inferential and key informant's findings.

4.1.1 Response Rate Analysis

With a sample size of 100 respondents and ten key informants domiciled at Directorate of Criminal investigations headquarters within Kiambu County. Out of 100 questionnaires distributed 96 questionnaires and ten key informant responses were obtained; giving a response rate of 96% and 100% respectively. According to (Kothari, (2004) a response rate of 50% or more is adequate for analysis. Hence with indicated response rate as per table 4.1 below it was therefore sufficient to draw conclusion.

Table 4.1 Questionnaires:

CLASS OF DETECTIVES	FORMS DISTRIBUTED	FORMS COLLECTED
DETECTIVE CONSTABLES	40	36
DETECTIVE CORPORALS	20	20
DETECTIVE SEARGENTS	10	10
DETECTIVE INSPECTORS	10	10
DATA BASE MANAGERS	10	10
HUMAN CAPITAL STAFFS	10	10
TOTAL	100	96 Forms (96%)

Source: Researcher (2021)

Table 4.2 Key Informants:

SECTOR HEADS	10	10 (100%)
--------------	----	-----------

Source: Researcher (2021)

Table 4.2 above represents key informant respondents from a sample size of ten section heads. A response rate of 100% was collected for analysis.

4.1.2 Reliability Test Results

Through descriptive research design, primary data was collected by structured self-administered questionnaires and key informant. Descriptive statistics thereby used to analyze data. The overall reliability test results of 0.856 and also for all the sections were within the acceptable threshold hence paved the way for further analysis and interpretation. This is presented in Table 4.3 below.

Table 4.3 Reliability Statistics for Information Infrastructure Management

Variable	Cronbach's Alpha	No. of Items
Planning Measures	.968	5
Staffing Needs	.890	5
Coordination Efforts	.746	5



Controlling Mechanism	.818	5
Overall	.856	5

Source: Researcher (2021)

4.2 Respondents Demographic Findings

Through descriptive research design, primary data was collected by structured self-administered questionnaires and key informant. Descriptive statistics thereby used to analyze data. The analyzed data was presented in table form and figures shown in below sections of the chapter.

Being part of the respondent's general information, the study assessed Age, Gender, Marital status, Education Level, Rank in service, Duty faculty and

length of service. The information provided basic understanding on the nature of persons involved in filling the questionnaires. Their profile was essential aspect as raised opinion at times are assessed pegged on basic information.

4.2.1 Age of respondents

The study sought to establish the representation of the respondents involved in the study from selected age group and results tabulated below in figure 4.1

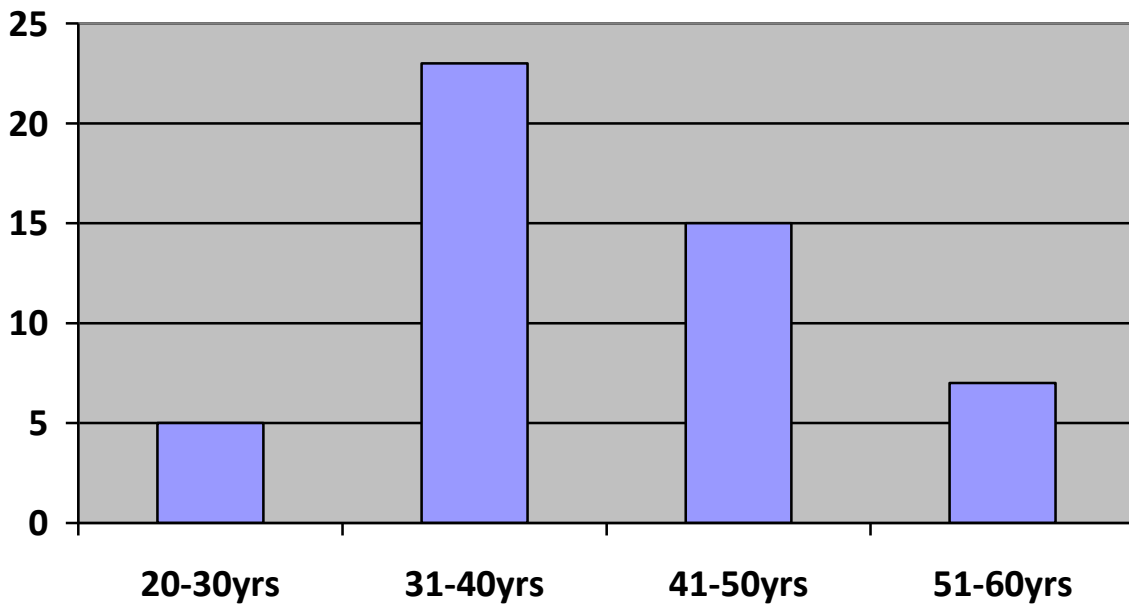


Figure 4.1 Respondents Age; Source: Researcher (2021)

4.2.5 Ranking of Respondents in Service

The researcher sought information on the respondent's hierarchical level within the service and outcome reflected as follows.

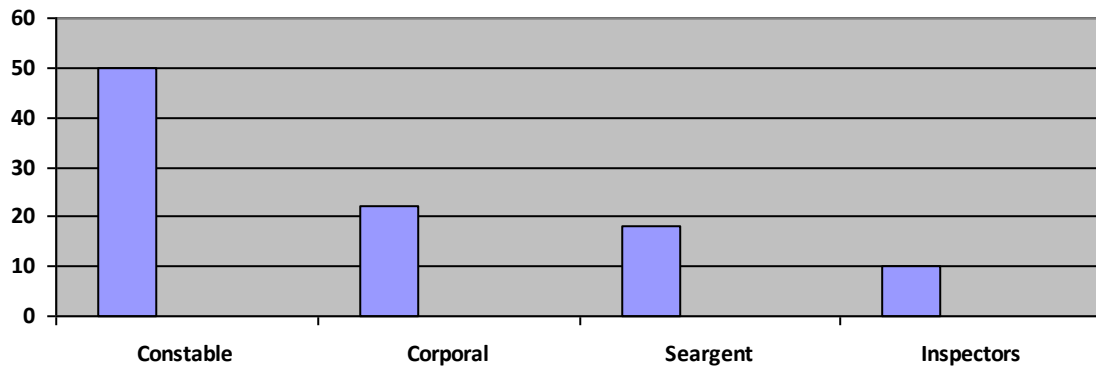


Figure 4.5 Respondents Ranking; Source: Researcher (2021)

Based on the outcome, a descending flow was witnessed where majority of the respondents were from lower cadre as compared to senior officers. Police Constable detectives led by 50%, Corporal Detectives at 22% Sergeant detective at 18% while inspectors and above constituted to 10% respectively. A true reflection of hierarchal ratio in the Directorate.

4.3 Descriptive Findings

Primary data was collected through structured self-administered questionnaires and Key informants. Being part of the respondents insight information on the subject, the study descriptively sought to establish the correlation of planning measures on cyber-terrorism in the Directorate of criminal investigation, optimal level of information infrastructural management, achievement ratio of

set goals and targets, extent of forensic data safeguard, the state of launch of strategic approaches on information infrastructural management, effect of staffing needs on cyber-Terrorism, the effect of coordination efforts on cyber-terrorism, establishment of effects of controlling mechanism on cyberterrorism, legislative enhancement approach, cyber terrorism and combat strategies.

4.5 Inferential Statistics

4.5.1 Regression Analysis

This review was directed on testing the effect of pointer factors. Coding, entering and processing was conducted through utilization of (SPSS V.20.0) evaluation. Whose model summary was demonstrated in table 4.18 below

Table 4.18 model summary

Model	R	R Square	Adjusted R Square	Std. Error of the estimate
1	.786 ^a	.541	.59	.424

Source: Researcher (2021)

Coefficient of determination was deployed in the study for evaluation of model fitness. relying on the value of adjusted R^2 , being the coefficient of multiple determinations, in that it is the percent of the variance in the dependent explained uniquely or jointly by the independent variables. The model adduced an average adjusted coefficient of determination (R^2) of which implied that 59% of the variations in information infrastructural management was explained by the independent variables under study (planning measures, staffing needs, coordination efforts and controlling mechanism).

Based on the outcome, it shows collectively that planning measures, staffing needs, coordination efforts and controlling mechanism are key influencing factors in the management of information infrastructure of the Directorate of Criminal Investigation.

However, the remaining 41% indicate that there might be other factors influencing Cyber-Terrorism in the Directorate's Information Management System other than the four.

4.5.2 Anova



Analysis of variance (Anova) technique was further utilized to test the significance of the model whose

findings were tabulated in table 4.19 Below.

Table 4.19 Anova

Model	Sum of Square	Df	Mean Square	F	Sig
1 Regression	4.92	10	0.172	8.769	0.19
Residual	1.076	48	0.32	0.32	
Total	1.178	58			

Source: Researcher (2021)

Critical Value=2.93

With an output significance level of 0.2%, an inference of perfect conclusion is hereby drawn (pvalue) was under 5% with a calculated value of 8.769 compared to critical value 2.93 therefore calculated value >critical value an indication that indeed Planning Measures, Staffing Needs, Coordination Efforts and Controlling Mechanism have a significant influence on Cyber-Terrorism in

the management of information infrastructure of the Directorate of criminal Investigations. The significance value was less than 0.05 indicating that the technique was reliable and similarly indicated that the model fitted data.

4.5.3 Regression Coefficients

Consequently, the study used the coefficient table to determine the study model whose findings were presented in table 4.20 Below.

Table 4.20 Regression Coefficients

	Unstandardized Coefficients	Standardized Coefficients		T	Sig
	B	Std error	beta		
Constant	2.75	0.843		4.150	0.003
Planning Measures	.682	.650	.444	4.439	0.001
Staffing Needs	.562	.272	.396	4.522	0.001
Coordination Efforts	.654	.345	.564	3.890	0.002
Controlling Mechanism	.735	.388	.678	2.547	0.005

Source: Researcher (2021)

Average $\beta = (.682 + .562 + .654 + .735) / 4 = 0.6583$

$Y = a + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3 + \beta_4 X_4 + E$

Becomes:

$Y = 2.75 + .682X_1 + .562X_2 + .654X_3 + .735X_4 + E$

As indicated above from regression equation, Planning Measures, Staffing Needs, Coordination Efforts and Controlling Mechanisms, whilst constant; the influence of Cyber-terrorism on information infrastructural management at Directorate of Criminal Investigation will be at 0.6583 with a significant value of 0.003. implying that the influence of Cyber-terrorism on Information Infrastructural Management of Directorate of Criminal investigation would be significantly negative where infrastructure of the DCI is poorly managed hence Cyber-Terrorism influenced by other factors. All in all, this is an indication that planning measures, staffing needs, coordination efforts and controlling mechanism have apposite influence on the management of information

infrastructure of the Directorate of Criminal investigation. Based on equation above, Planning Measures on information infrastructural management influence on cyber-Terrorism boasts of a positive regression coefficient of 0.001 the coefficient is statistically significant in comparison to the p value which is less than 0.05. This indicates that with a roll out of Planning Measures on information infrastructural management within the DCI, will influence Cyber-Terrorism by 68.2%. Consequently, Staffing Needs have a positive regression coefficient of .562 With a significant level of 0.001 which is less than 0.05; meaning that an increase in deployment of skilled information managers would robustly influence Cyber-terrorism in the Directorate by 56.2%. Consequently, both coordination efforts and Control Mechanism registered positive regression coefficients of 0.654 & 0.735 of significance levels of 0.002 & 0.005 respectively which are both below 0.05. The



outcome showed that with an up-surge in both coordination efforts and legislative framework as internal and external mechanism to manage information infrastructure; will tremendously influence cyber-terrorism within the Directorate. Moreover, deductions holistically indicate that the information infrastructure management has an outstanding influence on Cyber-terrorism in the Directorate of Criminal Investigation.

4.6 Key Informant's Findings

The researcher posted six questions during interview and whose outcome was summarized as below from ten Respondents.

4.6.1 Effects of Cyber-Terrorism

On personal level **8 respondents** indicated having been affected by **cyber-bullying** while 2 gave a clean bill of right as unaffected. Institution wise **hacking** was sighted by **5 respondents**. A clear indication of up-surge of cyber terror crimes being contemporary in nature affecting both individuals and institutions

4.6.2 Frequency of Cyber Attacks

Responses received as tabulated below: -

Table 4.19 Frequency of Cyber-Terror Attacks

OFTEN	MANY	RAMPANT	6/10	AVERAGE
3	2	2	1	2

Source: Researcher (2021)

On frequency of cyber-attacks, 7 out of ten respondents indicated the level of occurrence as many, rampant and often. Basically, with such parameters we project an increase on attacks as may recur Eugene Kaspersky (2006).

V. SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

The study targeted 100 respondents from DCI headquarters Kiambu. Collected data from respondents and key informants (10) was analyzed based on the study objectives. Hence the chapter presented the summary of the findings from the field made conclusion and recommendations.

5.2 Summary

5.2.1 Respondents Traits

The conducted study targeted members of the Directorate of Criminal Investigations being a department of National police Service hosting detectives. The study found majority of respondents were male, married, having attained a certificate of secondary education and drawn from the cadre of detective constables boasting of at least 6 year's service while ten key informants were departmental commanders with vast institutional knowledge.

5.2.2 Descriptive Findings

5.2.2.1 Planning Measures and Cyber-Terrorism

Majority of the respondents at 49.9% indicated that there exists low level of information infrastructural management planning in the Directorate. Consequently 39% of the respondents cited moderately availed planning measures while 13% indicated highly availed. On ratio of achieving set

goals and targets on planning measures; only 30% of respondents alluded for optimal achievement as 70% declined. Consequently, on impetus to launch strategic approaches 16% indicated the directorate as highly rated, moderately rated at 31% while poorly rated had 53%.

5.2.2.2 Staffing Needs and Cyber-Terrorism

On whether the directorate's staffing needs had been addressed, majority of respondents at 63% were un sure, 28% indicated yet to be addressed contrary to the 9% who affirmed. Various reasons were cited in support to wit poor communication on policy direction, inconsistency on roll out strategies in the directorate, system rigidity to changes and complement and reward of best performing through Ombudsman as a milestone achievement. On critical staffing components the findings indicated need to foster specialized training at 40%, enhancement of best recruitment practices at 38%, overseeing corruption free management at 12% while need for continuous vetting obtained 8.88%.

5.2.2.3 Coordination Efforts and Cyber-Terrorism

In regard to the third objective findings on how coordination efforts related to cyber-terrorism in the Directorate; Majority of respondents at 55% cited poor departmental cooperation, 20% showed poor intelligence sharing mechanism, interagency conflict and mistrust among stakeholders got 9% each while strain in bilateral and multilateral engagements scooped 7%.

5.2.2.4 Control Mechanism and Cyber-Terrorism

On regulation scope, 49% of respondents indicated low level, followed by 32% at very low as 12% was



high while 7% indicated very high. A further enquiry on legislative enhancement indicated majority of respondents having aligned on two strategies at 40% being striving to develop robust access control system and provision of efficient information management legislations. While need to formulate information coordination framework recorded 125 as need to roll out CERTs had 8% respectively.

5.2.2.5 Cyber-Terrorism

On whether the respondents had been victims of cyber terrorism; 62% affirmed while 30% rejected as 8% were not sure. Consequently, on the outcome of forms of cyber terrorism, 37% indicated having been victims of cyber-bullying, hacking constituted 285, introduction of viruses at 20% while other forms to wit phreaking, phishing, website defacing and terrorist threat collectively constituted 15%. Finally, on factors derailing enhancement of strategies to combat cyber-terrorism, majority cited poor skilled manpower and scarcity of resource allocation at 50% collectively. Quite a number indicated inadequate legislation at 22%, massive corruption (8%), political interference at 7%, friction in investigative agencies at 7% and tedious / unprecedented criminal justice system at 6%.

5.2.3 Inferential Findings

5.2.3.1 Regression Analysis

Coefficient of determination was deployed in the study for evaluation of model fitness. The model adduced an average adjusted coefficient of determination (R^2) of 0.59 of the variation. Therefore, implying that 59% of the variation in information infrastructural management was explained by the independent variable under study being planning measures, staffing needs, coordination efforts and controlling mechanisms. Interpretations of findings collectively indicate that planning measures, staffing needs, coordination efforts and controlling mechanism are key influencing factors in the management of information infrastructure of the Directorate of criminal investigation. However, the remaining 41% indicate that there might be other factors influencing cyber-terrorism in the Directorate's information system other than the above four.

5.2.3.2 Anova

Analysis of variance was further utilized to test the significance of the model. It gave an output significance of 0.2%. a calculated value of 8.169 compared to critical value of 2.43 was relayed. Therefore, with p-value under 5%, calculated value > critical value, a perfect inference was drawn indicating that planning measures, staffing needs,

coordination efforts and controlling mechanism had a significant influence on cyber-terrorism in the management of information infrastructure of the Directorate of Criminal investigation.

5.2.3.3 Regression Coefficients

The study findings indicated that planning measures, staffing needs, coordination efforts and controlling mechanism whilst constant, the influence on information infrastructural management at directorate of criminal investigation will be at 0.6583 with a significance value of 0.003 implying that the influence on cyber-terrorism on information infrastructural management of DCI would be significantly negative where infrastructure of the DCI is poorly managed. Hence an indication that planning measures, staffing needs, coordination efforts and controlling mechanism have a positive influence on the management of information infrastructure of the DCI.

As derived from the equation, planning measures on information infrastructural management influence on cyber terrorism boost of a positive regression of 0.001 which is statistically significant in comparison to the p value which is less than 0.05. it reflects that planning measures on information infrastructural management within the DCI was to influence cyber-terrorism by 68.2%. on the other hand, staffing needs possessed a positive regression coefficient of 0.562 with a significance level of 0.001, less than 0.05 meaning that an increase in deployment of skilled information managers would robustly influence cyber-terrorism in the Directorate by 56.2%. in furtherance, both coordination efforts and control mechanism registered positive regression coefficients of 0.654 & 0.735 of significance levels of 0.002 & 0.005 respectively which were both below 0.05. hence the outcome reflected an up-surge in both coordination efforts and legislative framework as internal and external mechanism to manage information infrastructure.

5.2.4 Key Informant's Findings

On frequency of cyber-attacks, seven out of ten respondents indicated the level of occurrence as many, rampant and often. Hence an upward cyber-terror attack projection deduced.

5.2.4.1 Planning Measures

Majority of respondents cited poor, untimely and ill-equipped plans at 50% to counter cyber terrorism. They further indicated that if planning measures were rolled out cyber terror could be immensely tackled. However, two of the respondents were indecisive while three showed availability of sufficient plans.

5.2.4.2 Staffing Needs



In adequate skills by information infrastructural personnel was supported by six respondents, 3 indicated insufficient in-service training of staff. Consequently, 9 informants were of the opinion that exists in adequate personnel who were poorly enumerated while one in support of current state.

5.2.4.3 Coordination Efforts

Two informants indicated lack of enough institutional resources to counter cyber terrorism and skewed departmental engagements due to inter-dependency aspect. However, majority at 6 informants asserted that exists cordial relationship as two reserved their comments.

5.2.4.4 Control Mechanism

On controlling mechanism, seven informants concurred with the need to formulate and tighten legislation on cyber-terrorism. As an internal control, majority alluded to the need avail a fire wall software to monitor section information interchange against leakage / unauthorized exposure. On the other hand, two indicated existence of enough rules while one wrote in not applicable.

5.3 Conclusion

Based on the findings of the study, a conclusive inference was hereby drawn reinforcing urgent need for robust protection of information system infrastructure. Cognizant of the confidentiality threshold accorded to classified information within Directorate's quotas and outcome of information leakage if any vis a vis the eminent cyber threat; this became a timely course. Entirely, the police infrastructural information system policy ought to have been re-aligned in tandem to the contemporary threat of Cyber-Terrorism. While achieving the aforementioned, infrastructural planning measures on information was to be set and strategically rolled out for objective one. Consequently, bearing in mind of the nature of contemporary crime cyber terror (crime of the elites). A momentous institutional personnel force in regard to objective two was to be availed for re-alignment to merge threats; both intellectually and strength wise.

Furthermore, for objective three Concerted departmental efforts were key in addressing the challenge and hence need to prioritize organization's coordination mechanism on relay of both information and actionable intelligence. Notwithstanding the above, robust institutional control mechanism traversing from tight legislation, internal departmental controls, supervision and purchase of secure penetration proof equipments upon uplift of resource allocation were pertinent for the last objective. Holistically, once the raft of measures was implemented than a well-managed

robust information system infrastructure was guaranteed.

5.4 Recommendations

The study identified the need to avail stringent control mechanism on information flow within the Directorate of Criminal Investigation by heightening internal supervision, severity of departmental disciplinary code and adherence to Service Standing orders. In averting information leakage, the study advocated for Creation of database for departmental timely information flow and to specific addressee framework policy as priority.

Moreover, the study recommended an overhaul of the outdated "over over" system of communication and installation of modern secure, user friendly and professional communication gadgets to achieve espionage controls. Establishment of information relay back-up system for retrieval and assessment of information. Creation of Directorate of Criminal information system management to replace signals department and mandated for strategic policy planning and direction for stringent information security management against cyber-terrorism.

Consequently, the study further identified need to increase resource allocation to the information directorate to purchase robust secure information firewall installed equipments across the department as key. Training of Information infrastructure management personnel in cyber-terrorism was seen to be timely and un-optional.

Finally, the study proposed introduction of special allowance on information infrastructural managers as a motivator, enactment of severe information control legislations to protect Directorate from eminent cyber-Terror attacks and installation of fire wall software for information access control.

5.5 Area of Further Research

The study focused on how Directorate of Criminal Investigation manages its information system infrastructure and its influence on cyber-terrorism. Further research would tentatively target the constituent forms of cyber-terror to wit Hacking, Phishing, Cyber bullying, Denial of service attacks (D.O.S), phreaking, Web site Defacing, Introduction of Viruses...effects and impact to institutions.

REFERENCES

- [1]. Abadinsky, H. (2007). Organized crime. Amazon publishers, 11th Edition.
- [2]. Alan, (2012). Terrorism.



- https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&as_vis=1&q=Alan%2C+%282012%29.+Terrorism&btnG=
- [3]. Alazab, M., & Broadhurst, R. (2014). Spam and Criminal Activity. Trends and Issues (Australian Institute of Criminology).
- [4]. Alazab, M., Layton, R., Broadhurst, R., & Bouhours, B. (2013, November).
- [5]. Malicious spam emails developments and authorship attribution. In Cybercrime and Trustworthy Computing Workshop (CTC), 2013 Fourth (pp. 58-68). IEEE.
- [6]. Andersen, R. (2007, December 31). Hacking tool guidance. Independently published.
- [7]. Ayling, J. (2009). Criminal organizations and resilience. International Journal of Law, https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&as_vis=1&q=Ayling%2C+J.+%282009%29.+Criminal+organizations+and+resilience.+International+Journal+of+Law%2C&btnG=
- [8]. Bachmann, M. (2010). The Risk Propensity and Rationality of Computer Hackers.
- [9]. Beacons, (2019). Report on state of security operations. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&as_vis=1&q=Beacons%2C+%282019%29.+Report+on+state+of+security+operations.&btnG=
- [10]. Berg, B. L., & Lune, H. (2004). Qualitative research methods for the social sciences.
- [11]. Borman, L.C. (2017). From Gutenberg destined to global infrastructural, information access in networked era.
- [12]. Brantingham, P. (2008). Crime Pattern Theory Environmental. Vol. 5 edited by Ronald Clarke CRC Press.
- [13]. Brenner, S. W. (2010). Cybercrime: criminal threats from cyberspace.
- [14]. Brenner, S. W. (2014). Cyberthreats and the Decline of the Nation-state. <https://www.taylorfrancis.com/books/mono/10.4324/9780203709207/cyberthreats-decline-nation-state-susan-brenner>.
- [15]. Brenner, S. W., & Clarke, L. L. (2004). Distributed security: Preventing cybercrime.
- [16]. Broadhurst, R. (2006). Developments in the global law enforcement of cyber-crime. https://eprints.qut.edu.au/3769/1/3769_1.pdf
- [17]. Broadhurst, R., & Chang, L. Y. (2013). Cybercrime in Asia: trends and chahttps://openresearch-repository.anu.edu.au/bitstream/1885/20466/8/CyberAsia_B&C2012pdf.pdfllenges.
- [18]. Broadhurst, R., & Choo, K. K. R. (2011). Cybercrime and online safety in cyberspace. bureaucracies, and competitive adaptation. Penn State Press.
- [19]. Bygstad, (2008). Social space. https://www.researchgate.net/publication/223873125_Bridging_social_and_technical_interfaces_in_organizations_An_interpretive_analysis_of_time-space_distanciation
- [20]. Callon, M, Latour, B, Low, J (1992). Actor network theory. https://www.researchgate.net/publication/279616291_Actor_Network_Theory
- [21]. Chantler, A. N., & Broadhurst, R. (2008). Social engineering and crime prevention
- [22]. Choo, K. K. R. (2011). Cyber threat landscape faced by financial and insurance <https://www.aic.gov.au/publications/tandi/tandi408>
- [23]. Cloward, R., & Ohlin, L. (2020). Differential Opportunity and Delinquent Subcultures. <https://www.tutor2u.net/sociology/reference/cloward-ohlin-illegitimate-opportunity-structures>
- [24]. Cohen, S. (2002). Folk devils and moral panics: The creation of the mods and rockers. https://infodocks.files.wordpress.com/2015/01/stanley_cohen_folk_devils_and_moral_panics.pdf
- [25]. Coleman, G. (2009). Code is speech: Legal tinkering, expertise, and protest among free <https://culturedigitally.org/wp-content/uploads/2016/07/Coleman-2016-Hacker-Digital-Keywords-Peters-ed.pdf>



Nairobi County Map

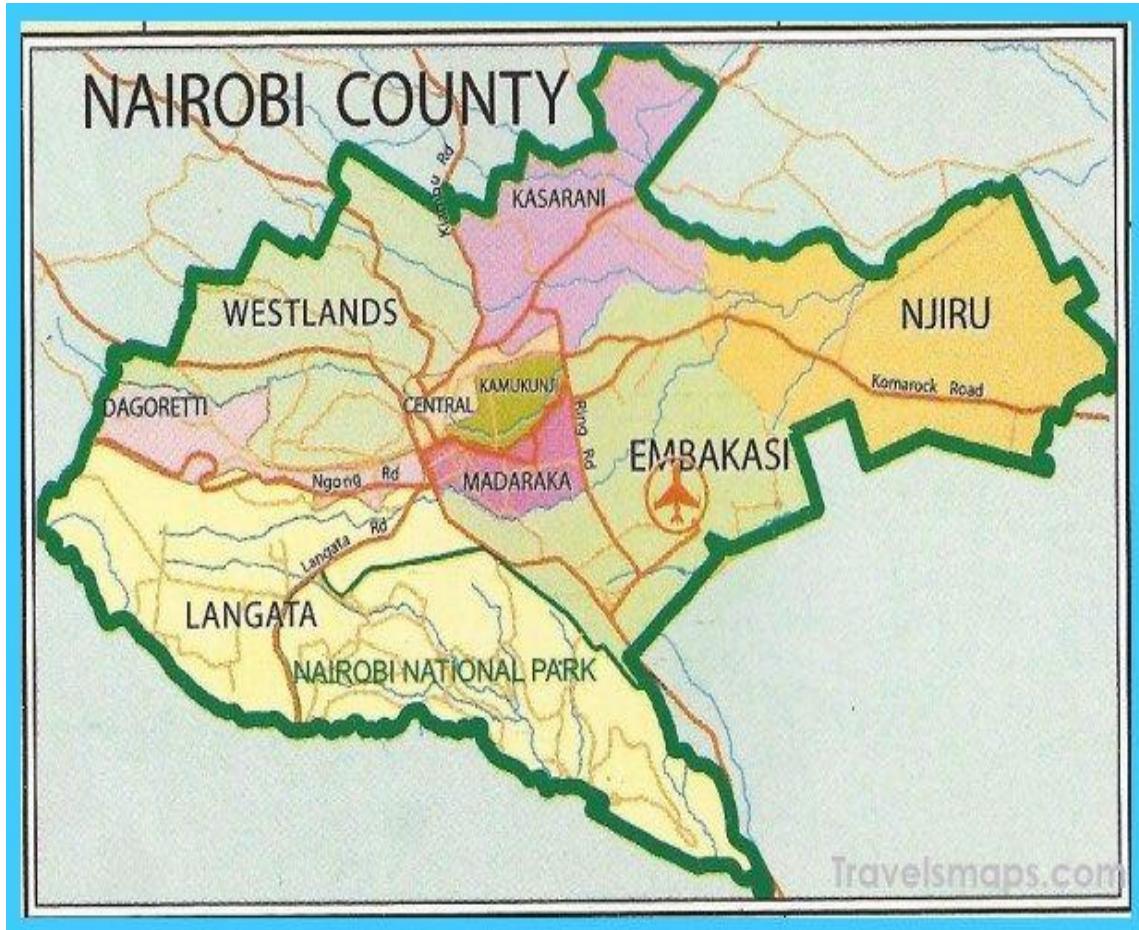


FIGURE 1.2 SOURCE : Internet



KENYATTA UNIVERSITY
GRADUATE SCHOOL

E-mail: dean-graduate@ku.ac.ke

Website: www.ku.ac.ke

P.O. Box 43844, 00100

NAIROBI, KENYA

Tel. 8710901 Ext. 57530

Our Ref: C159/MSA/PT/30702/2015

DATE: 3rd December, 2020

Director General,
National Commission for Science, Technology
and Innovation
P.O. Box 30623-00100
NAIROBI

Dear Sir/Madam,

RE: RESEARCH AUTHORIZATION FOR WABWIRE GODFFREY MUKEKHE, REG. NO. C159/MSA/PT/30702/2015.

I write to introduce Wabwire Godfrey Mukekhe who is a Postgraduate Student of this University. The student is registered for M.A degree programme in the Department of Security and Correction Science.

Wabwire intends to conduct research for a M.A Project Proposal entitled, "Information System Infrastructure Management Influence on Cyber-Terrorism in Kenya Police Service".


Any assistance given will be highly appreciated.


Yours faithfully,

PROF. ELISHIBA KIMANI
DEAN, GRADUATE SCHOOL

HI/lnn





REPUBLIC OF KENYA


NATIONAL COMMISSION FOR
SCIENCE, TECHNOLOGY & INNOVATION

Ref No: 747124 Date of Issue: 11/February/2021


RESEARCH LICENSE




This is to Certify that Mr.. GODFFREY WABWIRE MUKEKHE of Kenyatta University, has been licensed to conduct research in Kiambu on the topic: INFORMATION SYSTEM INFRASTRUCTURE MANAGEMENT INFLUENCE ON CYBER-TERRORISM IN KENYA POLICE SERVICE for the period ending : 11/February/2022.

License No: NACOSTI/P/21/8945

747124
Applicant Identification Number


Director General
NATIONAL COMMISSION FOR
SCIENCE, TECHNOLOGY &
INNOVATION

Verification QR Code



NOTE: This is a computer generated License. To verify the authenticity of this document,
Scan the QR Code using QR scanner application.