“CYBER CRIME, DIGITAL FORENSIC AND ELECTRONIC EVIDENCE IN TERRORISM TRIALS”

BEING A PAPER PRESENTED

BY

MR OLA OLUKOYEDE

THE EXECUTIVE CHAIRMAN,

ECONOMIC AND FINANCIAL CRIMES COMMISSION

AT A WORKSHOP FOR JUDICIAL OFFICERS ON TRANSNATIONAL ORGANISED CRIME AND COUNTER TERRORISM.

HELD AT THE NATIONAL JUDICIAL INSTITUTE,

JABI,

ABUJA.

23RD APRIL, 2024

CYBER- CRIME, DIGITAL FORENSIC AND ELECTRONIC EVIDENCE IN TERRORISM TRIALS

May I start by expressing my deep gratitude and appreciation to the Administrator of the National Judicial Institute and his team for extending the invitation to me to make a presentation on a paper titled- ***"Cyber-crime, Digital Forensic and Electronic Evidence in Terrorism Trials"***

The topic for discussion, I must say is both relevant and well thought out particularly against the background of the wider theme – Transnational Organized Crime and Counter Terrorism, which is an issue commanding the attention of the entire globe at this moment.

No doubt, there is hardly any part of the world presently that is immuned or shielded from transnational organized crime and terrorism. Transnational Organized Crime, being organized crime coordinated across national borders involving groups or markets of individuals working in more than one country to plan and execute criminal activities. In order to achieve their goals, these criminal groups use systematic violence and corruption as vehicles to achieve their devilish intentions. Common transnational organized crimes include drugs trafficking, arms trafficking, trafficking for sex, toxic waste disposal, and material thefts and poaching.

Terrorism on the other hand is the unlawful use of violence and intimidation, especially against civil populace in the pursuit of political, religious, racial, ideological or economic cause. Terrorists also use violence and threats of violence to influence the government or an international governmental organization or to intimidate the public.

DEFINITION OF KEY CONCEPTS:

Cyber Crime:

Cybercrime encompasses a wide range of criminal activities that are carried out using digital devices and/ or networks. These crimes involves the use of technology to commit fraud, identity theft, data breaches, computer viruses, scams and expanded upon in other malicious acts. Thus Cyber Crime is an act that violates the law, which is perpetrated using information and communication technology (ICT) to either target networks, systems, data, websites, and/or technology or facilitate a crime. Cybercrime differs from traditional crime in that it **"*knows no physical or geographic boundaries*"** and can be conducted with less effort, greater ease, and at greater speed than traditional crime.

Cyber criminals exploits vulnerabilities in computer systems and networks to gain unauthorized access, steal sensitive information, disrupt services and cause financial or reputational harm to individuals, organizations and governments.

In 2000, the 10th U.N Congress on the prevention of and the treatment of offenders placed cybercrimes into five categories namely:

- Unauthorized access
- Damage to computer data or programs
- Sabotage to hinder the functioning of a computer system or network.
- Unauthorized interception of data within a system or network and
- Computer espionage.

Internationally, both state and non-state actors engage in cybercrimes, including espionage, financial theft and other cross borders crimes.

Cyber Crimes crossing international borders and involving the actions of at least one nation state are sometimes referred to as cyber warfare.

Warren Buffett has said that cybercrime is the ***'' number one problem of mankind''*** and that it ***''poses real risks to humanity''***

The world Economic Forum – WEF 2020 Global Risk Report confirmed that organized cybercrime groups are joining forces to commit criminal activities online, while estimating the likelihood of their detection and prosecution to be less than 10% in the U.S. There are also many privacy concerns surrounding cybercrime when confidential information is intercepted or disclosed legally or otherwise.

Forensic Evidence:

Is defined as criminal evidence acquired through scientific methods, including ballistics, blood tests, and DNA tests to be used in court. It can also be holistically defined as the application of science with legal proceedings. Forensic evidence is gathered through photographs and measurements taken of the crime scene. In the case of violent crimes, these are obtained along with finger prints, footprints, time tracks, blood and other body fluids, hairs, fibers and fire debris. Each of these elements is useful in understanding what took place during the commission of the crime.

Digital Forensic Evidence

Digital Forensic evidence is a branch of forensic science that focuses on identifying, acquiring, processing, analyzing and reporting on data stored electronically.

Electronic Evidence:

Is a component of almost all criminal activities and digital forensics support is crucial for law enforcement investigations.

Digital forensics:

The digital forensics process involves the - search, acquisition, preservation, and maintenance of digital evidence; description, explanation, and establishment of the origin of digital evidence and its significance; the analysis of evidence and its validity, reliability, and relevance to the case; and the reporting of evidence pertinent to the case.

Digital Evidence:

In the field of digital forensics, digital traces are left behind as the result of individuals' use of information and communication technology (ICT). Particularly, a person utilizing ICT can leave a digital footprint, which refers to the data left behind by ICT users that can reveal information about them, including age, gender, race, ethnicity, nationality, sexual orientation, thoughts, preferences, habits, hobbies, medical history and concerns, psychological disorders, employment status, affiliations, relationships, geolocation, routines, and other activities. This digital footprint can be active or passive.

An active digital footprint is created by data provided by the user, such as personal information, videos, images, and comments posted on apps, websites, bulletin boards, social media, and other online forums. A passive digital footprint is data that is obtained and unintentionally left behind by the users of the Internet and digital technology (e.g., Internet browsing history). Data that are part of active and passive digital footprints can be used as evidence of a crime, including cybercrime (i.e., digital evidence). This data can also be used to prove or disprove a matter being asserted; refute or support the testimony of a victim, witness, or suspect; and/or implicate or exculpate a suspect of a crime.

OVERVIEW OF CYBERCRIME

Cybercrime, also known as computer crime, is a broad category of crimes that includes a wide and growing variety of crimes involving computers, Cybercrime is generally seen as consisting of five general categories which are:

- Theft of services: that is, unauthorized use of computer facilities specifically offline, to process information.
- Illegal use of computer/ internet data for personal gain.
- Improper use of computers for numerous types of financial and other benefits, e.g. forgery and document counterfeiting.
- Using a computer to damage another person's assets, for example, planting a damaging virus to destroy data (Malware).
- Theft of software through lawful copying.

From this categorization, it could be understood that computer facilities are used to commit crimes in four different instances:

- Computer as the target: In this type of cybercrime, somebody's computer is the target because it carries certain vital information that can be used to sabotage or destroy one personality or organization—for example, customers' list, medical records, and personal history.
- Computer as the means of committing a crime: In this category, the processes of the computer system, not the content of the computer files, facilitate the crime. In this, the criminal manipulates the normal processes of the computers, to have illegitimate access to other facilities. Crimes under this category include fraudulent use of ATM Cards, illegal transfer of funds or stocks, phishing, hacking and child pornography.
- Computer as incidental to other crimes: In this category of cybercrime, the computer is not essential but its presence or facilities help the crime to occur faster and easier. Crimes in this category include money laundering, unlawful banking transactions, and many other crimes like murder and terrorism.
- Hardware and software as target: The prevalence of computers and particular microcomputers generate new versions of cyber-crime. In this type of cyber-crime, offenses like software piracy, copyright violation of computer programmes and counterfeit hardware are included.

In Nigeria, the Cybercrime (Prohibition & Prevention Etc.) Act, 2015 has identified cybercrimes to include cyber terrorism, child pornography and related offences; cyber stalking, cybersquatting, racism and xenophobic crimes. It also includes manipulation of ATM/POS terminals, phishing, spamming, spreading of a computer virus, use of a fraudulent device or attached e-mails and websites; card fraud, breach of confidence by service providers, importation and fabrication of e-tools and fraudulent issuance of e-instructions. See Sections 5-36 of the Act for the comprehensive listing.

Europol segments cybercrime into cyber-dependent crimes (i.e., "any crime that can only be committed using computers, computer networks or other forms of information communication technology;" and cyber-enabled crimes (i.e., traditional crimes facilitated by the Internet and digital technologies).

The key distinction between these categories of cybercrime is the role of ICT in the crime - whether it is the target of the offense or part of the modus operandi (or M.O.; i.e., Method of Operation) of the offender. When ICT is the target, of the offense, this cybercrime negatively affects the confidentiality, integrity, and/or availability of computer data or systems. Confidentiality, integrity, and availability make up what is known as the "CIA Triad": put simply, private information should stay private, it should not be changed without permission from the owner, and data, services, and systems should be accessible to the owner at all times. When the ICT is part of the M.O., the cybercrime involves a traditional crime (e.g., fraud and theft) facilitated in some way by the Internet and digital technologies.

TERRORISM AND CYBERTERRORISM:

Information and communication technology (ICT) can be used to facilitate the commission of terrorist-related offences (a form of cyber-enabled terrorism) or can be the target of terrorists (a form of cyber-dependent terrorism). Specifically, ICT can be used to promote, support, facilitate, and/or engage in acts of terrorism. Particularly, the Internet can be used for terrorist purposes such as the spreading of "propaganda (including recruitment, radicalization and incitement to terrorism); [terrorist] financing; [terrorist] training; planning [of terrorist attacks] (including through secret communication and open-source information); execution [of terrorist attacks]; and cyberattacks". The term cyberterrorism has been applied by some to describe the use of the Internet for terrorist purposes.

Just as there is no consensus on a definition of cybercrime, there is also no universally accepted definition of terrorism nor of cyberterrorism. The North Atlantic Treaty Organization (NATO) defines Cyber Terrorism as a cyberattack that uses or exploits computer or communication networks to cause ***"sufficient destruction or disruption to generate fear or to intimate a society into an ideological goal".*** But all definitions share a common denominator.

Cyber Terrorism also known as digital terrorism is defined as disruptive attacks by recognized terrorist organizations against computers systems with the intent of generating alarms, panic or the physical disruption of the information system.

Conceptions of cyberterrorism have ranged from "more expansive conceptions [including] any form of online terrorist activity and narrower understandings of this concept". The narrow understanding of cyberterrorism has been described as "pure cyberterrorism" by some. This narrow definition considers cyberterrorism as a cyber-dependent crime perpetrated for political objectives to provoke fear, intimidate and/or coerce a target government or population, and cause or threaten to cause harm (e.g., sabotage). Examples of this narrow conception of cyberterrorism include "attacks that lead to death or bodily injury, explosions, plane crashes, water contamination, or severe economic loss. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not". It is important to note that this limitation of cyberterrorism to cybercrimes committed against critical infrastructure or pure cyberterrorism is not widely held.

OVERVIEW OF FORENSIC EVIDENCE

Forensic evidence is any kind of evidence that is obtained via scientific methods, like blood tests, DNA tests, ballistics analysis, and so on. It’s the kind of evidence often shown in popular crime shows on TV, and it can be crucial in coming to a fair and justified decision in a legal case. Although television crime dramas, present the discovery of forensic evidence as a fait accompli to a conviction, in real life, such is not always the case. Forensic evidence can be challenged, and challenged successfully.

Digital Forensics

Is a branch of forensic science that focuses on identifying, acquiring, processing, analyzing, and reporting data stored electronically. Electronic evidence is a component of almost all criminal activities and digital forensics support is crucial for law enforcement investigations.

Standard Principles of Digital Forensic Evidence and its Application Investigation:

Special consideration is necessary to establish authenticity, protect integrity and maintain the confidentiality of digital evidence. These considerations include:

- Ensuring that the collection of digital evidence is properly authorized and conducted in compliance with standard practice.
- Documenting the collection and preserving the documentation for later review.
- Not altering the digital evidence, unless it is necessary, and only by a trained person.
- Documenting all interactions with the evidence.
- Establishing a Chain of Custody as soon as possible.
- Backing up the digital evidence and only working with copies.
- Ensuring that evidence and all copies are securely stored, transported, and disposed of.

Digital evidence can be used as evidence in investigation and legal proceedings for:

- Data theft and network breaches—digital forensics is used to understand how a breach happened and who were the attackers.
- Online fraud and identity theft—digital forensics is used to understand the impact of a breach on organizations and their customers.
- Violent crimes like burglary, assault, and murder—digital forensics is used to capture digital evidence from mobile phones, cars, or other devices in the vicinity of the crime.

- White collar crimes—digital forensics is used to collect evidence that can help identify and prosecute crimes like corporate fraud, embezzlement, and extortion.
- Terrorism

Digital Forensic Techniques

Digital forensics involves creating copies of a compromised device and then using various techniques and tools to examine the information. Digital forensics techniques help inspect unallocated disk space and hidden folders for copies of encrypted, damaged, or deleted files. Here are common techniques:

- Reverse Steganography: Terrorists and cybercriminals use steganography to hide data inside digital files, messages, or data streams. Reverse steganography involves analyzing the data hashing found in a specific file. When inspected in a digital file or image, hidden information may not look suspicious. However, hidden information does change the underlying has or string of data representing the image.
- Stochastic Forensics: Stochastic forensics helps analyze and reconstruct digital activity that does not generate digital artifacts. A digital artifact is an unintended alteration of data that occurs due to digital processes. Text files, for example, are digital artifacts that can contain clues related to a digital crime like a data theft that changes file attributes. Stochastic forensics helps investigate data breaches resulting from insider threats, which may not leave behind digital artifacts.

- Cross-drive Analysis: Cross-drive analysis, also known as anomaly detection, helps find similarities to provide context for the investigation. These similarities serve as baselines to detect suspicious events. It typically involves correlating and cross-referencing information across multiple computer drives to find, analyze, and preserve any information relevant to the investigation.
- Live Analysis: Live analysis occurs in the operating system while the device or computer is running. It involves using system tools that find, analyze, and extract volatile data, typically stored in RAM or cache. Live analysis typically requires keeping the inspected computer in a forensic lab to maintain the chain of evidence properly.
- Deleted File Recovery: Deleted file recovery, also known as data carving or file carving, is a technique that helps recover deleted files. It involves searching a computer system and memory for fragments of files that were partially deleted in one location while leaving traces elsewhere on the inspected machine.

Digital Forensic Tools

Before the availability of digital forensic tools, forensic investigators had to use existing system administrative tools to extract evidence and perform live analysis. The drawback of this technique is that it risks modifying disk data, amounting to potential evidence tampering.

In 1989, the Federal Law Enforcement Training Center (a Bureau of the Department of Homeland Security, USA) recognized the need and created SafeBack and IMDUMP. In 1991, a combined hardware/software solution called DIBS became commercially available. These tools work by creating exact copies of digital media for testing and investigation while retaining intact original disks for verification purposes.

By the late 1990s, growing demand for reliable digital evidence spurred the release of more sophisticated tools like **FTK** and **EnCase**, which allow analysts to investigate media copies without live analysis.

Today, the trend is for live memory forensics tools like **WindowsSCOPE** or specific tools supporting mobile operating systems. Commercial forensics platforms like **CAINE** and Encase offer multiple capabilities, and there is a dedicated Linux distribution for forensic analysis. Open-source tools are also available, including **Wireshark** for packet sniffing and **HashKeeper** for accelerating database file investigation.

The main types of digital forensics tools include disk/data capture tools, file viewing tools, network and database forensics tools, and specialized analysis tools for file, registry, web, Email, and mobile device analysis.

When evaluating various digital forensics solutions, the following are the major consideration:

- Integration with and augmentation of existing forensics capabilities.
- Support for various device types and file formats.
- Availability of training to help staff use the product.
- CLI, graphic UI, and ease of use.
- Compatibility with additional integrations or plugins.

- Types of configurations available.
- Advanced features for more effective analysis.

THE ROLE AND IMPACT OF DIGITAL FORENSIC IN TERRORISM TRIALS

Forensic evidence – evidence collected through the use of scientifically accepted modern forensic sciences, consistent with applicable domestic and international law, including international human rights law – can be a valuable tool in the investigation and prosecution of terrorism-related crimes

Forensic science can help to prove that a crime has been committed (offence level), to identify victims and perpetrators (source level), or to describe how the crime has been committed (activity level). Forensic science can be used in the investigation and prosecution of terrorism-related crimes and can in some cases also be used in the prevention of terrorist incidents.

Forensic data can be retrieved from the crime scene, during the aftermath of a terrorist attack and/or on the battlefield, or from other relevant areas. The type of evidence recovered could range from fingerprints from unexploded improvised explosive devices (IEDs) to chemical characteristics of a bomb or data retrieved from electronic devices such as computers, mobile phones, flash drives or digital cameras. The forensic data can further be analyzed and documented at the crime scene itself – with the help of mobile equipment – or in laboratories.

Forensic science consists of many different methodologies such as ballistic and firearms examinations, fiber analysis, forensic chemistry or the use of biometric technology. In particular, biometrics – through a semi-automated recognition of individuals based on specific traits such as face, fingerprints, iris, voice, DNA or teeth – are frequently used. Forensic technology, especially concerning biometrics and DNA analysis, is advancing very fast. Those that have the technical and financial means could invest in forensic research, develop more sophisticated and reliable techniques that can be used in terrorism-related crimes, and assist in building forensic capabilities.

The collection, analyzing, storing, using, and sharing of forensic data can have implications for privacy rights, but can also affect the right to a fair trial. Privacy – although not absolute – is a human right recognized in article 17 of the International Covenant on Civil and Political Rights (ICCPR).

According to UNSCR 2396 (2017), all States shall develop and implement systems that collect biometric data to responsibly identify terrorists including FTFs in a manner that complies with States' domestic law and international human rights law. To further develop the use of forensic science in terrorism-related crimes these legal requirements including privacy rights should be addressed.

In conclusion, Nigeria needs to invest in developing its forensic capabilities, which includes investing in scientific research, technology, facilities, expertise, and training staff but also ensuring that the current system is capable of adapting to new scientific developments such as forensic intelligence. Through developing new applications, using internationally accepted or scientifically proven standards for storing, analyzing, and sharing forensic data, and furthering forensic cooperation between different stakeholders, forensic science can play a vital role in preventing and countering terrorism.

Thanks for listening.