The Use of Internet, Other Cyber and Digital Platforms as well as Digital Devices to Support and Commit Acts of Terrorism in Eastern Africa

Abstract

The issue paper presented is based on an extensive literature review and evidence-based research, accounted by digital forensic investigators, police investigators, counter-terrorism officers, national intelligence officers and INTERPOL officers. This paper will focus on the use of internet, other cyber and digital platforms, as well as digital devices, used to support and commit acts of terrorism in Eastern Africa region. The primary objective of this paper is to understand the prevalence of terrorist organizations using the internet, other digital platforms and digital devices throughout the attack cycle and determining the nature of social media or encrypted internet-based messaging used for terrorist activities. The recommendation presented will be essential in building capacity, awareness raising, strengthening cooperation, good information sharing practices, and detailed mutual legal assistance in countering cybercrime.

UNODC
United Nations Office on Drugs and Crime

Author: Claudia Jematia, UNODC Cybercrime Expert (Consultant)

1. Introduction

The internet and social media continue to be used to facilitate various terrorist activities, including communication, enabling financing, incitement, radicalization, recruitment, and to execute acts of terrorism. Terrorist organizations may use the internet to raise and collect funds through direct solicitation, online payment exploitation tools, charitable organization and E-commerce.

The United Nations Security Council (UNSC), through **Resolution 1373 (2001)**[1], reaffirmed the need to prevent all such acts of international terrorism, by upholding international peace and security. The UNSC highlights the importance of intensifying and accelerating the exchange of operational information on the use of internet and its technologies in addressing the global threat of terrorism, and in encouraging Member States to share and exchange information on the use of digital technologies by terrorist groups, in order to subdue terrorist radicalization and recruitment.

Subsequently, the UNSC **Resolution 2129(2013)**[2] acknowledges the evolving technologies used by terrorists and their supporters, in particular the internet, for the purposes of recruitment, radicalization, and incitement to commit acts of terrorism, as well as for the financing, planning and preparation of their activities. It further underlines the need for Member States to respond cooperatively to the exploitation of technology, communications and resources to influence support for terrorist acts, while respecting humans' rights, fundamental freedoms, and in conformity with other commitments under international law[3].

Moreover, UNSC **Resolution 2462 (2019)**[3] emphasizes the primary responsibility of Member States in countering terrorist acts and their obligation to prevent and suppress the financing of terrorist acts, as well as calling on all Member States in countering terrorist acts and their obligation to prevent and suppress the financing of terrorist acts. Furthermore Resolution 2462, calls on all States to be part of international counter-terrorism conventions and protocols.

A further focus will be on the use of information and communication technologies, in particular, the internet, to facilitate terrorist acts, as well as their use to incite, recruit, fund, or plan terrorist acts[4].

This research paper will primarily focus on the use of internet, cyber and digital platforms as well as digital devices in support, preparation and conduct of acts of terrorism in Eastern Africa. However, due to the nature of cybercrime and cyber-enabled crime, the research will include examples of other cyber related activities within the region and beyond.

The research findings will be critical in: raising awareness regarding the use of digital and internet-based technologies to commit acts of terrorism within the region; providing law enforcement agencies with evidence-based research; and lastly, building additional programming and trainings on the provided needs assessments.

1.1. Specific Aims and Objectives

Develop an understanding of the prevalence of terrorist organizations using the internet, other digital platforms and digital devices throughout the attack cycle;

i. Understand the use of social media or encrypted messaging applications, such as Facebook, Instagram, Twitter, TikTok, Telegram, Signal, WhatsApp and internet forums in relation to terrorism activities;

ii. Determine the mobile money applications, Hawala systems, mobile applications, and financial institutions used by terrorist to finance their activities;

[1] The UN Security Council Resolution 1373 (2001) (https://undocs.org/S/RES/1373(2001)) , dated, 28/09/2001

[2] The UN Security Council Resolution 2129 (2013) (https://undocs.org/S/RES/2129(2013)) , dated 17/12/2003

[3] UNSC Resolution 2462 (2019) (https://www.un.org/securitycouncil/content/sres24622019), dated 28/03/2019

iii. Understand how law enforcement officers within the region collect digital evidence, and request legal assistance, evidence or information, either through Mutual Legal Assistance (MLA) in relation to internet or social media applications, or through preservation or other requests to service providers.

To achieve the above objectives, this paper includes an extensive literature review on use of internet and social media for acts of terrorism in Eastern Africa and beyond; with emphasis on cybercrime, cyber-enabled crime, counterterrorism, use of internet-technologies to commit acts of terrorism, financing of terrorism, use of social media to radicalize supporters, countering financing of terrorism, and international cooperation through structured Mutual Legal Assistance (MLA). For the purpose of this research paper, the use of internet to commit acts of terrorism will be categorized into six elements: **planning, online propaganda, training, financing, execution, and cyberterrorism.** Additionally, the paper will focus on case studies in the region, where terrorist groups might have used the internet to commit acts of terrorism. For example, the Dusit D2 attack and Westgate Mall attack – the Nairobi Westgate Mall attack in 2013 will serve as the case study upon which the theoretical framework will be analysed. This attack was the first time a terrorist group used Twitter to claim responsibility for and cover an on-going attack in real-time with periodical updates during the terror operation.

From analysis, these two attacks involved the use of internet and digital devices, particularly, during the Westgate Mall attack where the terror group twitter account was used to broadcast updates to the public in an active terror operation. On the other hand, the CCTV footage released after the Dusit D2 terror attack showed how the terror group communicated with their phones before launching an attack; These examples illustrate how digital devices and the use of internet as an enabler have been used to facilitate acts of terrorism within the region. If intercepted, these devices, which contain crucial information on location, calls, videos, text messages, documents, history searches, images and internet-based messaging applications, might be useful to investigating officers.

The final section will focus on respondents, in regards to investigating terrorism cases, especially on the use of internet, cyber and digital platforms as well as digital devices by terrorist groups, to commit acts of terrorism, and methods used by law enforcement agencies within the region to collect, request and preserve digital evidence, before recommendations are presented.

2. Background and Relevance

2.1. Introduction

The development of increasingly sophisticated technologies has created a global reach of networks, making it easier for individuals to communicate with relative anonymity[6], quicker and more effectively across borders, to an almost infinite audience. The benefits of Internet technologies are numerous, with its unique suitability for sharing information and ideas, which is regarded as a basic human right[4]. It must also be recognized, however, that the same technology that facilitates such communication[6] can also be exploited for terrorism acts.

The internet and social media continue to be used to facilitate various terrorist activities. For the purpose of this issue paper, ***the Use of Internet, Social media, and other Digital platforms for acts of Terrorism***; these activities will be categorized into six elements:

- **Planning:** Including through encrypted communication and Open Source Intelligence (OSINT);
- **Online Propaganda:** Including social media recruitment, radicalization and online incitement to terrorism;
- **Training:** Either through dissemination of training guides through internet-based messaging application, such as Telegram, Signal, WhatsApp and Messenger, among others;
- **Financing:** Including the use of the internet to raise and collect funds through direct solicitation, online payment exploitation tools, Hawala systems, cryptocurrencies fraud, charitable organization, front companies, and E-commerce[5].
- **Execution:** Including, for example, the use of mobile phone devices to detonate Improvised Explosive Devices (IEDs).
- **Cyberterrorism:** Information and Communication Technology (ICT), can be used to facilitate acts of terrorism-related offences (a form of cyber-enabled terrorism)[6], such as cyberattacks - Distributed Denial-of Service (DDoS) attacks, Man-in-the Middle (MITM) attacks and Phishing)[6].

2.1.1. PLANNING

The Internet is a crucial tool for global terrorism[7] - Terrorists have exploited commercial communication networks, encrypted internet-based messaging applications and used open source intelligence to gather target building architectures, surveillance and monitor persons' movements into the target location.

These networks have enabled terror insurgent groups to coordinate and mount operations that would be impossible and beyond their capabilities before the 1990s[7]. According to the Straits Times[8], all four gunmen, who were involved in Kenya's Westgate mall attack, trained in Somalia for four months, before crossing into Kenya. From an analytical point of view, the choice and the timing of the attack on the Westgate mall[9] showed that the Al-Shabaab had spent several months planning the attack to guarantee the enormous atrocities committed during the siege.

The choice of the Westgate terror attack could have been determined by three critical interrelated considerations:

- Firstly, by choosing a soft target that is popular with foreigners and affluent Kenyans[9], to

[4] See, for example, International Covenant on Civil and Political Rights (General Assembly resolution 2200 A (XXI), annex), art. 19, para. 2.

[5] UNODC Policy Paper on The Use of the Internet for Terrorist Purposes (https://www.unodc.org/documents/terrorism/Publications/Use_of_Internet_for_Terrorist_Purposes/ebook_use_of_the_internet_for_terrorist_purposes.pdf), September, 2012

[6] UNODC E4J University Module Series: Cybercrime (https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberterrorism.html)

[7] Journal Article by James A. Lewis during the **Proceedings of the Annual Meeting (American Society of International Law** on The Internet and Terrorism, Vol 99(March 30 – April 2, 2005), pp.112-115

[8] The Straits Times News Article titled: **"Westgate Mall attackers spent four months planning in Nairobi"** (https://www.straitstimes.com/world/westgate-mall-attackers-spent-four-months-planning-in-nairobi), published 19/11/2013

[9] Aljazeera Centre of Studies Report on Westgate Attack Al-Shabaab's Renewed Transnational Jihadism by Dr. Freedom C. Onuoha, (https://studies.aljazeera.net/en/reports/2013/11/201311111128185804 17.html), dated 11/11/2013, retrieved on: 21/05/2021

promote their ideology of successfully planning and executing attack on several foreigners, especially westerners;

- Secondly, and as the outcome to the above, the inclination to launch attack on the upper class within the Kenyan communities - given that the Westgate mall was well frequented by affluent Kenyans and foreigners[9], the Al-Shabaab strategists considered the high-profile target for its attack, to put pressure on the Kenyan government to withdraw its troops from Somalia[9]. For its part, Al-Shabaab retaliated on the sustained involvement of the Kenya Defence Forces (KDF) in Somalia, which was too porous for the Kenyan people; as reported by the Star Newspaper[10]: the plan for KDF to exit Somalia is underway, and this will likely end KDF's presence in Somalia under Amisom's Concept of Operations (Conops) and the Somalia National Defence Forces will soon take over the security of their country. This development will probably have an impact on Kenya especially in ensuring that border control within the Somali borders are well manned to prevent unauthorized illegal exit and entry into Kenya;

- Thirdly, with the high-profile nature of Westgate's mall and the Al-Shabaab's external operations[9] influence, the insurgent group must have considered a strategic target location that would attract local and international media in order to amplify its global jihadism rank[10]. In this degree, the attack was planned to be in the form of selective killing and hostage-taking rather than suicide bombing, to maximize the media cover, compared to suicide bombing where the media coverage would be more minimal and for a shorter period. It should be noted that the siege took place in Nairobi's busiest mall where the local and international media networks could easily live stream the events. This was coupled with delayed hostage situation allowing the terror group to serve its propaganda on Al-Shabaab's capacity[9].

Communication is critical for Al-Shabaab operations, through live tweeting, posting images and videos online, for example during the Westgate attack, the terrorist group used social media during the attack to give updates[11] of their actions to the public. While social media has been used in the past to support terrorist operations in Mumbai[12] attacks, the Al-Shabaab Westgate incident is an example of the real time, directed to target audience propaganda that social media facilitates[11].

Furthermore, Al-Shabaab made the strategic move to target the mall during the weekend, with huge traffic of shoppers and visitors, therefore inflicting maximum damage and destruction[9] and also gaining more international attention by killing several people of different nationalities.

On a tactical level, Al-Shabaab uses Twitter to coordinate members' knowledge and maintain movement coherency[13]. Twitter's short and easy transmission can captivate an audience allowing easy reach to global audience and acting as an ideological communication channel, facilitating framing and belief dissemination[13].

The group now uses Internet platforms like Facebook, Twitter and YouTube to reach a greater audience[13], to challenge opponents and to spread its ideologies. Given these benefits, it is unsurprising that many Islamic movements now consider Twitter to be valuable asset[11], a community torn between rejecting innovation and embracing modernity[13]. These events highlight how important connective devices have become for the strategic number of Islamic social movements.

In addition, internet technology may be used to facilitate the preparation of acts of terrorism. For example, the Ferizi case[14], where a suspect hacker in

[10] The Star News Report on KDF Exit Plan from Somalia (https://www.the-star.co.ke/news/big-read/2020-10-18-reality-dawns-as-kdf-gears-up-for-smooth-exit-from-somalia/), dated 18/10/2020, retrieved on: 21/05/2021

[11] Report by Stewart Bertram and Keith Ellison on Sub Saharan African Terrorist Groups' use of the Internet (https://www.researchgate.net/publication/282829958_Sub_Saharan_African_Terrorist_Groups'_use_of_the_Internet), dated February, 2014, DOI: 10.15664/jtr.825

[12] CNN News Report by Stephanie Busari on Tweeting the Terror: **How Social Media reacted to Mumbai** (https://edition.cnn.com/2008/WORLD/asiapcf/11/27/mumbai.twitter/), dated 27/11/2008, retrieved on: 21/05/2021

[13] Lindsay Pearlman, "Tweeting to Win: Al-Shabaab's Strategic Use of Microblogging," Yale Review of International Studies Nov. 2012. Available at http://yris.yira.org/essays/837 (accessed 21/05/2021);

[14] The Ferizi Case: The First man charged with Cyber Terrorism (https://resources.infosecinstitute.com/topic/the-ferizi-case-the-first-man-charged-with-cyber-terrorism/), dated 09/03/2016, retrieved on: 23/05/2021

Malaysia, was charged with stealing data belonging to the US service members and distributing it to ISIS members, with the intent to support the group in planning attacks against western targets. Data stolen by Ferizi included names, email addresses, locations and phone numbers of 1315 U.S military and other government personnel. The data was posted online on Twitter with a download link to the 30-page file[14].

2.1.2. ONLINE PROPAGANDA

The internet provides a relatively unregulated and unrestricted place where terrorists can craft and disseminate propaganda through seemingly limitless number of websites and social media platforms[15], tailoring their message to target thousands of potential new recruits to join the insurgent groups and further their cause and reach.

ISIS, in particular, produces the most technologically advanced propaganda[15], through sophisticated digital means, promoting the idea online that ISIS has successfully established a caliphate and recruited thousands of new members to join the terror group.

One of the primary uses of the internet by terrorists is for propaganda dissemination[5], generally in the form of multimedia communication, detailing ideological or practical instructions, explanations and justification of terrorists activities.

These may include audio, video files, online messages, magazines and presentations. These violent and gruesome effects portray ISIS terrorists as heroes, with pictures and posts describing exciting encounters by ISIS youth[15]. The combination of horrific and tantalized videos is deliberate in targeting young adults through social media by showing glamourous ISIS territories. However, such propaganda fails to show the harsh realities of life in ISIS territories.

Modern terrorist organizations produce a wide range of propaganda in the form of images, videos, and audio files[16]. These can be categorized into: Content Hosting, Audience Development, Secure Communication, Community Maintenance, Information Collection and Curation.

i. Content Hosting

Prior to broadband internet, propaganda materials were distributed manually, either in the form of printed material or video tapes, cassettes or DVDs. Since the advent of 3G/4G broadband, especially within the Eastern Africa region, terrorist organization have migrated those repositories online, first through file-sharing sites where users can download media and enable even large-scale file sharing and video-streaming[16]. Groups like Al-Shabaab consistently use video-streaming services to distribute propaganda material, with some offering unique capabilities including the ability to livestream video from a phone or camera; while social media platforms also facilitate easy video and image hosting.

ii. Audience Development

Terrorist groups require an audience for all sorts of reasons: to directly engage the population, to attract media attention (in order to indirectly engage the population), and to identify potential recruits. However, there are limited studies in comparing how terrorists use social media and traditional mass media[16], as traditional media is likely still a critical method for conducting audience development.

iii. Brand Control

The desire of terrorist groups to control their political messages creates a need for well-branded information that can be used to validate the initial distribution of propaganda, therefore, the use of spokespeople, a dedicated media production house and reliable information-distribution channels online are critical.

Modern terrorists groups have used dedicated web forums[16], Twitter handles and Telegram channels to help cue their target audience, showing that the distribution is authentic; while maintaining brand control requires consistency

[15] A Report by Ariel V. Lieberman on Terrorism, The Internet and Propaganda (https://jnslp.com/wp-content/uploads/2017/04/Terrorism_the_Internet_and_Propaganda_FINAL.pdf), Journal of National Security Law & Policy, Vol. 9:95, Year: 2016

[16] A Report by Brian Fishman on Crossroads: Counter-terrorism and the Internet (https://tnsr.org/2019/02/crossroads-counter-terrorism-and-the-internet/), Texas National Security Review: Volume 2, Issue 2 (February 2019), Retrieved on : 23/05/2021

and allowing technology platforms to distribute their propaganda with a high-level of control.

iv. Secure Communication

Despite occasional lone-actor attacks, terrorist violence is usually planned and executed as part of a group. As such, secure communications between conspirators are important, with the ubiquity of encrypted messaging tools prompting the increased scrutiny of platforms that provide encrypted services.

However, terrorist groups have used different variety of techniques to ensure secure messaging on the internet, for example, Al-Qaeda famously employed 'email dead drops'[16] where users share login credentials with each other and leave messages in drafts, thereby avoiding message scan while on transit. Obscurity is often a tool for security - facilitating data exchange through fake accounts, multiple accounts, and secret web forums only accessible to invited members.

Alternatively, such techniques can be countered by use of steganography where terrorists use a pre-determined but complicated code word to send a message or reference a shared experience to authenticate their identity online.

v. Community Maintenance

Terrorist groups often rely on in-group or private social networks as compared to public groups. As such, allowing restricted access where propaganda can be shared, watched, and discussed, are critical for the group. However, once presence has been established, group members will share and radicalize more supporters.

vi. Information Collection and Curation

Terrorist groups also use the internet to collect information[16]. For example, online mapping tools are used to plan attacks, monitor news and identify potential recruits. Various platforms can be used for these purposes, including social media, search engines, traditional media, and specialized tools for identifying critical infrastructure and other sensitive targets.

It is important to note that some online platforms are better suited for some functions listed above than others, which means that terrorists often use multiple platforms for their online activities. For example, a terrorist might use Facebook for audience development, but convince a target for recruitment to shift to Telegram or Signal to communicate securely, where the recruit can be radicalized. In addition, Al-Shabaab within the region, have continuously used Twitter to give updates during a terror attack or to claim responsibility for an attack.

Audience development, however, requires the utilization of a platform with an audience or active users like Facebook, Twitter or Instagram. On the other hand, platforms, such as Telegram, have also become a key tools for many terrorist organizations. Telegram is effectively only useful for brand control, community maintenance and secure communication, rather than for audience development and content hosting.

2.1.3. TRAINING

With the advancement of internet technologies, terrorist organizations have increasingly moved to the internet as an alternative training ground for terrorists[5]; with growing range of media that provides detailed platforms for dissemination of practical training guides, in the form of online manuals, audio, video clips, information and advice[5].

The Internet has two functions with regards to training and the transfer of knowledge[17]. It is a library where training manuals and handbooks can be easily accessed from anywhere in the world. The other function is to provide an interactive environment where terror groups can discuss training-related issues, exchange personal experiences, and communicate with online trainers on problematic subjects.

These internet platforms act as virtual training camps, providing detailed instructions, often in easy multimedia format and multiple languages, which offer terrorists and extremists the same opportunity and capability that it does for the rest

17 A Report by Anne Stenersen on The Internet: A Virtual Training Camp? Journal Article in Terrorism and Political Violence (https://www.researchgate.net/publication/240521278_The_Internet_A_Virtual_Training_Camp/link/56080a8908ae8e08c0945eba/download), dated: April 2008

of internet users[18]: to communicate, collaborate, radicalize and convince. There are already significant quantities of radical materials available online, which increase daily.

The available handbooks can be on any topics such as conventional weapons, improvised weapons and explosives, field tactics, guerrilla warfare, organizational and field security, and physical training[17]. While some training manuals are in plain text, others, especially practical manuals, can be illustrated with explanatory sketches or photos and some appear in video formats. These can mostly be derived from open sources[17].

The following Table 1 below illustrates today's wide-spread availability of material pertinent to violent extremism and terrorism on-line:

Table 1: Google search for: examples of critical keywords, as of May 24, 2021

Search Term	Number of Results
"How to make a bomb"	499,000,000
"Salafi publications"	329,000
"Beheading video"	30,900,000
"Al-Shabaab Training Videos"	345,000

According to Reuters News[19], Kenya police arrested two suspects linked to the Islamic State who were planning to launch an attack, seizing bomb-making materials. These materials included nails, ball bearings, batteries, electric wire, fertilizer, cell phones and other explosive substances which were later taken for forensic analysis. Moreover, initial investigations shows that the two men drafted a document that was circulating online, supporting Islamic States leader at that time, the late Abu Bakr al-Baghdadi[19].

On the other hand, the Somali-based Al-Shabaab has influenced Islamic extremists networks in Tanzania[20], with a presence in the country since at least 2008, according to Tanzanian officials[20]. Since 2008, Tanzanian authorities have linked numerous incidents to Al-Shabaab. In October 2013, in the first large-scale arrest of Al-Shabaab operatives, police in the southeast region of Mtwara confiscated firearms, machetes and 25 DVDs containing All-Shabaab training materials[20].

According to authorities, the suspects – all Tanzanian nationals – had engaged in military training exercises. In Tanga Region authorities dismantled Al-Shabaab training camps, arresting 69 suspects and seizing 12 Al-Shabaab videos containing lectures instructing followers to liberate Muslims in East Africa and throughout the world[20]. Nevertheless, the seizure of Al-Shabaab materials and videos inside Tanzania suggest some level of the group presence and influence.

According to the U.S States Department of Justice Press Release[21], two suspects were arrested and charged in relation to their alleged attempt to provide material support to a designated foreign terrorist organization, the Islamic State of Iraq and Al-Sham (ISIS). To gain supporters, ISIS, like many other terrorist organizations, spreads its message using social media, internet platforms, and email. Using these platforms, ISIS has disseminated a wide variety of recruiting materials and propaganda through social media[21], which includes photographs and videos depicting ISIS activities, including beheading and other atrocities, as well as audio and video lectures by members of ISIS and members of other Islamic extremists organizations[21].

Among other internet and social media platforms, ISIS has popularized the use of end-to-end encrypted communication services and applications as a means of recruiting, communicating with, and disseminating terrorist training materials and propaganda to its members and supporters[21].

The instructional materials available online can include tools that facilitate counter-intelligence and hacking activities[5], and improve the security of illegal communication and online activities

[18] A Report on Radicalization in the digital era: The use of the internet in 15 cases of terrorism and extremism by Ines Von Behr, Anais Reding, Charlie Edwards and Luke Gribbon (https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf), 2013

[19] Reuters News Report on Kenya Police arrest two for planning Islamic State-linked attack (https://www.reuters.com/article/kenya-security/kenya-police-arrest-two-for-planning-islamic-state-linked-attack-idINKCN0YG28E), dated 25/05/2019

[20] Counter extremism Project Report (https://www.counterextremism.com/countries/tanzania) : 2021

[21] The United States Department of Justice Press Release on suspects charged with attempting and conspiring to provide material support to ISIS (https://www.justice.gov/opa/pr/man-and-woman-charged-attempting-and-conspiring-provide-material-support-isis),(https://www.justice.gov/opa/press-release/file/1382551/download) dated 01/01/2021

through the use of publicly available encryption tools and anonymized techniques. Using interactive internet platforms helps to build a sense of community among individuals from different geographical locations and backgrounds, motivating the creation of exchange network for instructional and tactical materials[5]. However, the use of internet applications, such as YouTube, for online video streaming, cannot be limited for all users because bad actors used or abused some of its content. Google Earth as a tool assists a vast number of people on everyday basis and although it is possibly used by terrorists to examine target locations, this should not stop Google Earth from operating for common good[22] and for profit.

2.1.4. TERRORIST FINANCING

Terrorist organizations and pro-supporters might use the internet to finance acts of terrorism[5] – Terrorist organizations require financing to recruit and support members[23], maintain logistics hubs, and conduct operations. Terrorist organizations use the internet to raise and collect funds and resources. These can be categorized into: E-commerce, direct solicitation, charitable organization, exploitation of online payment tools, Kidnapping for Ransom (KFR), front companies, cryptocurrencies and bitcoin.

The Statement[24] by Mr. Vladimir Voronkov, the United Nations Under-Secretary-General, Office of Counter-Terrorism during the 28 March 2019 Meeting of the Security Council on Adoption of Resolution 2462 (2019) on Countering the Financing of Terrorism, highlights the need for member states to identify ways to suppress terrorist financing and developing capacities to implement key priorities[24].

UNSC Resolution 2462 (2019)[25] reaffirms that terrorism in all forms and manifestations constitutes to most serious threats to international peace and security – with the primary responsibility of Member States to counter terrorist acts and to prevent and suppress the financing of terrorist acts. Resolution 2462 calls on member states to be part of International Counter-terrorism conventions and protocols, including the International Convention for the Suppression of the Financing of Terrorism.

Additionally, UNSC Resolution 2462(2019)[25] addresses the use of information and communication technologies, in particular, the internet, to facilitate terrorist acts, as well as their use to incite, recruit, fund, or plan terrorist acts.

According to RAND Testimony by Colin P. Clarke[26], the Islamic State in Iraq and Syria (ISIS) generated over $6 billion at the height of its territorial control in 2015. While ISIS's territorial control has declined, it still retains financial power and allegedly has smuggled as much as $400 million out of Iraq and Syria, and used it to invest in legitimate businesses, such as hotels, farms, hospitals, front-mall shops and car dealerships throughout the region[26].

The fact that ISIS and other terror insurgent groups are able to acquire such vast financial reserve demonstrates that the international community is still learning how to combat terrorist financing, especially through the use of internet. To critically understand the terrorist financing activities in the Eastern Africa region, the following will be reviewed and analyzed:

i. Explore how terrorist groups generate income;

ii. Analyze how terror groups might use its funds to regenerate;

iii. Understand current and emerging trends in this area.

Within the scope of this issue paper, the focus will be

[22] A Report on Prevention of (Ab-)Use of the Internet for Terrorist Plotting and Related Purposes by Branislav Todorovic and Darko Trifunovic (https://icct.nl/app/uploads/2021/02/Handbook-Ch-19-Todorovic-and-Trifunovic-Prevention-of-Ab-Use-of-the-Internet-for-Terrorist-Plotting.pdf), Year: 2021, Retrieved on: 24/05/2021, DOI: 10.19165/2020.6.0119

[23] UNODC webpage on Countering Terrorist Financing (https://www.unodc.org/unodc/en/terrorism/news-and-events/terrorist-financing.html)

[24] Statement of Mr. Vladimir Voronkov, United Nations Under-Secretary- General Office of Counter-Terrorism, on Meeting of the Security Council on Adoption of Resolution 2462(2019) on Countering the Financing of Terrorism (https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/20190328_USG%20Statement_SecurityCouncil_CFT28March.pdf), dated 28/03/2019, retrieved on: 25/05/2021

[25] UNSC Resolution 2462 (2019) adopted by the Security Council at its 8496th meeting on 28 March 2019 (https://undocs.org/en/S/RES/2462(2019))

[26] RAND Testimony by Colin P. Clarke on lessons from the Islamic State in Iraq and Syria and Other Emerging Threats (https://www.rand.org/pubs/testimonies/CT498.html), Testimony presented before the House Financial Services Committee, Subcommittee on Terrorism and Illicit Finance on September 7, 2018.

on how terrorists and insurgent groups are always seeking emerging innovative means, like the use of internet technologies, to evade and to disrupt law enforcement networks. In the contemporary global security environment, these challenges are further complicated by the cross-border movements and anonymity facilitated by the internet. Considering the already complex landscape of weak states and poorly governed territories, the process of following money trail is an immensely difficult task.

After the September 11 attacks, the highest-level US government officials publicly declared that the fight against al Qaeda financing was as critical as the fight against the terror group itself[27]. Terrorist groups have made increasing use of the internet to further the organizations' goals and activities[28] - with the global reach provided by internet technologies, terrorists are able to reach millions of people across the world. One of the primary ways that terrorist groups are using the internet is to raise funds through illegal activities[28]. For instance, regulators have documented the ongoing misuse of the internet and social media platforms by terrorist organizations to finance their activities[29]. For example, terror groups have used social media to communicate, propagate, radicalize, recruit supporters, and transfer knowledge and skills[29]. The Monitoring Team Reports by the UN Security Council have highlighted the use of internet and social media by ISIL, al-Qaeda and the Taliban since 2014[30]. The UN report from January 2020 highlighted that al-Qaeda's affiliate in Syria Hurras al-Din (HAD) uses two encoded messaging applications, Telegram and WhatsApp, to raise funds locally[30].

However, there has been some incremental progress in combatting these types of misuse; in November 2019, Internet and social media providers cooperated with Europol[31] and coordinated effort by the EU's Internal Referral Unit during the 16th Referral Action Day, resulting in the removal of significant amount of ISIL-related accounts. Among the items removed were propaganda videos, publication and social media accounts supporting terrorism and violent extremist[31]. With these developments, it is evident that online terrorism activities are cross-border, with no geographical specific location; prompting several parties within the internet providers' spectrum to partner in removing harmful and abusive content.

Additionally, there has been limited public attention on the misuse of internet-based communication services for terrorist financing, despite ISIL and other terrorist organizations regularly using these technical capabilities to disseminate financial information, raise funds and organize donation drives[32]. Furthermore, a deeper understanding is needed of the risk presented by terrorist organizations with misuse of cryptocurrencies and the related technical instruments to raise, transfer or store funds. These technological development present new challenges in the fight against terrorist financing for both regulators and anti-money laundering efforts.

In recent years, regulators have documented the ongoing misuse of the internet and social media platforms by terrorist organizations to finance their activities[29]. In 2018, the US government updated its National Terrorist Financing Risk Assessment, explaining the risks concerning major international terrorist groups, in particular ISIL, al-Qaeda in the Arabian Peninsula (AQAP) and al-Shabaab33. Most recently, a report by the Asia/Pacific Group on Money Laundering (APG), in cooperation with the Middle East and North Africa Financial Action

[27] Report on National Commission on Terrorist Attacks Upon the United States: Monograph on Terrorist Financing by John Roth, Douglas Greenburg and Serena Wille (https://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Monograph.pdf)

[28] Terrorist Financing and the Internet by Michael Jacobson (https://www.tandfonline.com/doi/pdf/10.1080/10576101003587184?needAccess=true), dated 09/03/2010, DOI: 10.1080/10576101003587184, Retrieved on: 27/05/2021

[29] ACAMS Today Report on New Technologies: The Emerging Terrorist Financing Risk (https://www.acamstoday.org/new-technologies-the-emerging-terrorist-financing-risk/), dated 03/06/2020, Retrieved on: 27/05/2021

[30] Letter dated 20 January 2020 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da'esh), Al-Qaida and associated individuals, groups, undertakings and entities addressed to the President of the Security Council," **United Nations Security Council**, 20 January 2020, (https://undocs.org/S/2020/53)

[31] "Referral Action Day Against Islamic State Online Terrorist Propaganda," Europol, 22 November, 2019, (https://www.europol.europa.eu/newsroom/news/referral-action-day-against-islamic-state-online-terrorist-propaganda), Retrieved on: 27/05/2021

[32] "Emerging Terrorist Financing Risks," Financial Acton Task Force October 2015, (https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf)

[33] National Terrorist Financing Risk Assessment, U.S Department of the Treasury, 2018 (https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf)

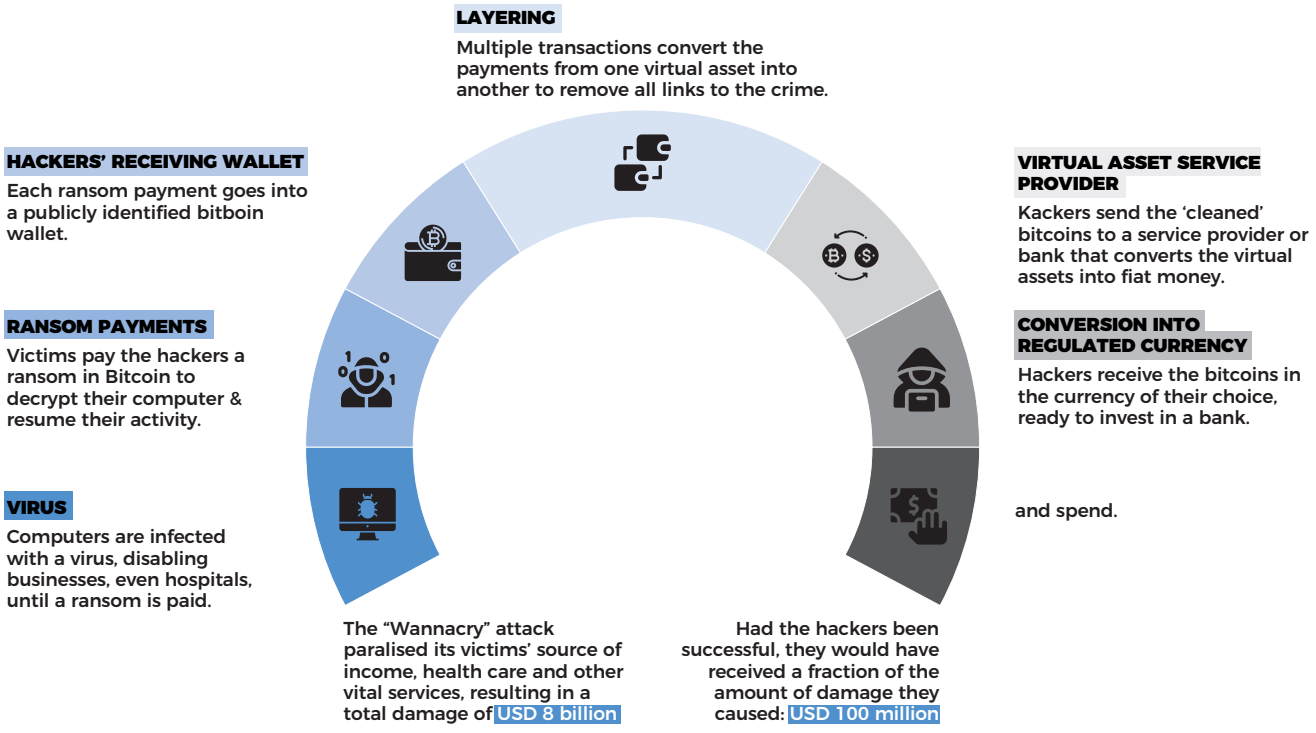
Task Force (MENAFATF)34, highlights that terrorist financiers continue to use social media platforms mainly as a communication tool to solicit funds and disseminate financial information[29]. However, the report[34] highlights that these activities are highly visible and can be accessed without a sophisticated understanding of computing and use of encryption tools.

Therefore, detecting these activities should not be challenging for prosecutors and online service providers. With initial search in January 2020 by the Counter Extremism Process focused only on individuals and entities involved in terrorist financing and sanctioned by the UN Security Council on its ISIL and al-Qaeda sanctions list revealed that several individuals had active social media accounts on several platforms[35]. Although not entirely new, crowdfunding websites create an additional risk due to their specific designs to solicit funding and donations.

In 2015, the European Securities and Markets Authority (ESMA)[36] highlighted the risk posed by investment-based crowdfunding platforms: with a possibility of misuse of the platform especially where the platform has limited or no due diligence on project owners and the projects.

Furthermore there is a risk associated with the combination of the misuse of crowdfunding platforms and misuse of the charitable donations for terrorist financing[29]. The misuse of charitable donations for terrorist financing is one of the core funding streams for many terrorist organizations[29]; block chain, bitcoin, crypto assets and virtual currencies (as shown in Figure 1 below) are innovative technologies used to swiftly transfer value around the world[29]. The fast-evolving block chain and distributed ledger technologies have the potential to radically change the financial landscape; but, their speed, global reach and, above all, anonymity also attract terrorist financiers.

Figure 1: How criminal actors can misuse virtual assets.



[34] "APG/MENAFATF Social Media and Terrorism Financing Report," Asia/Pacific Group on Money Laundering, dated 23/01/2019 (http://www.apgml.org/methods-and-trends/news/details.aspx?pcPage=1&n=1142)

[35] "UN Designated Individuals Maintain Social Media Presence," Counter-Extremism Project (https://www.counterextremism.com/blog/un-designated-individuals-maintain-social-media-presence), dated 22/01/2021. Since the publication and at the time of writing of this issue paper, Facebook removed most of the accounts notified in the press release.

[36] "Questions and Answers: Investment-based crowdfunding: money laundering/terrorist financing," European Securities and Market Authority (https://www.esma.europa.eu/sites/default/files/library/2015/11/esma_2015_1005_qa_crowdfunding_money_laundering_and_terrorist_financing.pdf), dated 01/07/2015

Several cases of terrorist organizations – from extremist Islamist to extremist right wing groups, attempt to solicit funds in cryptocurrencies[37]. In 2015 and 2017, ISIL members were arrested and convicted in the US for attempting to support the group in adopting this technology and attempting to solicit funds in cryptocurrency[38]. Therefore, while this type of asset may not be the major terrorist financing tool yet, the advantages cryptocurrencies offer for illicit activities[29], along with the regulatory gaps and inadequate technical expertise within regulatory bodies, especially in the Eastern Africa region, pose challenges to counter the virtual assets.

In Kenya, the mobile money transfer system commonly known as M-Pesa, has revolutionized the financial banking system in the country. However, such technology can be abused and used for crowdfunding activities to solicit and transfer funds quickly and effectively. A report by the Columbia Business School[39] highlights that the Kenyan mobile money transfer system, Safaricom M-Pesa, may have been used as a substantial financing tool during the terrorist attack at the DusitD2 hotel in Nairobi on 16 January 2019, with multiple news sources reporting that the court papers allegedly accused the suspects of financial fraud. In the last three months of 2018 before the DusitD2 attack, one mobile money agent registered dozens of M-Pesa accounts (52 in total) and received Ksh. 9 million (approximately $90,000). On a single day in January 2019, the agent used Diamond Trust Bank to withdraw 13 tranches of Ksh. 400,00 ($3,984) for a total of Ksh. 5.2 million ($51,793)[39]. The bank branch manager was charged with failing to report suspicious withdrawals as required by regulations.

With these developments, terrorists might have found a safe conduit of transferring illicit cash flow across Kenya's financial system without raising suspicion[40]. Increased usage of digital mobile credit constitutes to an increased risks of money laundering, terrorist financing, and technology risks. Following the 2015's terror attack on Garissa University, the Kenya government implemented a crackdown against the Hawala systems, which led to thirteen (13) being shut down for being suspected as conduits for terrorists financing[40].

Alternatively, In Somalia and other parts of Eastern Africa, Hawala has been linked to a number of terrorist organizations, including al Qaeda and Islamic State[41], and often been used as modern online banking systems, with an estimated 258.9 billion pounds transacting through the network every year[42]. Such systems can be used by terror groups because of its trust within the group while avoiding high banking fees and evading the administrative process associated with standard banking verification of practices, as senders are not required to provide any personal identifiable information. As such, the process of identifying suspicious persons is untraceable, making the investigation process more difficult. For this reason, criminals and terrorists have often abused these online services.

The adoption of social media, crowdfunding and cryptocurrency technologies by terrorist groups and organizations to finance their activities within the region, is not surprising. Terrorist groups have always adapted new technologies to circumvent control and restrictions on their activities. Prior to 2001, al-Qaeda began using email accounts[42]. However, current industry awareness and capabilities as well as regulatory framework have not sufficiently adjusted to counter the new threats that these technologies pose to counter terrorism financing. Therefore, progress between internet providers, including public-private partnerships, is necessary to ensure that the current threats are weakened.

---

[37] Yaya Fanusie, "Hamas Military Wing Crowdfunding Bitcoin," Forbes, 4 February 2019, (https://www.forbes.com/sites/%20yayafanusie/2019/02/04/hamas-military%20wing-crowdfunding-bitcoin/#5327df034d7f); Yashu Gola, "Breaking: ISIS Used Bitcoin to Fund Horrific Sri Lanka Easter Bombings, Research Claims," CCN Markets, 2 May 2019, (https://www.ccn.com/isis-bitcoin%20fund-sri-lanka-easter-bombings/); Far-Right European Terrorist Group Crowdfunding Cryptocurrency," Counter Extremism Project, 28 August 2018 (https://www.counterextremism.com/blog/far-right-european-terrorist-group%20crowdfunding-cryptocurrency).

[38] Nikita Malik "How Criminals and Terrorists Use Cryptocurrency: And How to Stop It," Forbes, 31 August 2018, (https://www.forbes.com/sites/nikitamalik/2018/08/31/how-criminals-and-terrorists-use-cryptocurrency-and-how-to-stop-it/#21a6f8493990)

[39] Columbia Business School Report on Mobile Money Transfers in Kenya by Michael Wechsler (https://dfsobservatory.com/content/mobile-money-transfers-suspected-financing-dusit-d2-terror-attack), dated 30/01/2019, retrieved on: 27/05/2021

[40] The Standard News Report by Dominic Omondi on Mobile Cash Transfers pose headache for security agencies and local banks (https://www.standardmedia.co.ke/financial-standard/article/2001311163/mobile-cash-transfers-pose-new-headache-for-security-agencies-local-banks), dated 29/01/2019, retrieved on: 27/05/2021

[41] Forbes Report by Nikita Malik on the Hawala Payment Systems (https://www.forbes.com/sites/nikitamalik/2019/04/29/does-the-hawala-payment-system-still-benefit-terrorists/?sh=48ab698d51bf), dated 29/04/2019, retrieved on 27/05/2021

[42] Al Qaeda used Hotmail to Plan Attacks, CBC News, 1 May 2009, (https://www.cbsnews.com/news/al-qaeda-used-hotmail-to-plan-attacks/)

Investigations into terrorist related offences[42] have revealed the use of Hawala networks to transfer money. For example, In Iraq, two Kurdish individuals were arrested for using Hawala networks to transfer $148,000 to Ansar al Islam (Islam supporters). In its latest move to counter the terror threat in Kenya, the government has banned at least 86 entities and individuals it accuses of financing or supporting terror activities in the country[43].

Although this is a fairly new provision, online service providers as well as regulators will have to ensure the availability of appropriate mechanism for verifications. Despite this progress, the uneven regulatory framework around the globe[44] creates additional problems as users can move wallets and use exchanges in several jurisdictions.

Therefore, while regulators and investigators may be aware of attempts to finance terrorism[29], it is hard to stop the transactions and freeze the assets due to lack of jurisdictional authority. For example, Hamas terror group exploited this weakness during one of its crowdfunding campaigns; the group switched its campaign from a regulated US-based exchange[45] to unregulated markets.

Finally, new technical development will present additional threats to the fight against terrorist financing. For example, privacy coins such as Monero offer even more enhanced user privacy protection[46], Non-custodial or decentralized wallets[47] and exchanges[48] allows pure peer-to-peer (P2P) transaction without the provision of an intermediary. This approach would require developing significant technical capabilities and expanding specialized monitoring capacities within regulatory authorities, which presents enormous challenges for the existing limited resources within the region.

2.1.5. EXECUTION

As described in section 2.1.1, 2.1.2, 2.1.3 and 2.1.4 above, the use of the internet for acts of terrorism shows how terror insurgent groups plan, finance, radicalize and recruit supporters. For example, explicit threats of violence[5], including the use of weapons, may be disseminated through the Internet to cause anxiety, fear or panic in a population subset or an entire population. In many member states, issuance of such threats, may be an offence and prosecuted under the states' law. Internet communication may be used as a communication means with potential victims, or to coordinate the execution of physical acts of terrorism[5]. For example, the Internet was used by participants to coordinate the 9/11 attack in the United States.

The internet can be used to offer logistical advantages[5], reducing the likelihood of detection, or obscuring the identity of responsible parties and facilitating the acquisition of items online for execution of attacks. For instance, terrorists may procure individual items necessary to perpetrate violent acts of terrorism through E-commerce platforms. Furthermore, forged credit cards or other compromised electronic payments may be used for such transactions.

Another form of attack execution, is the use of mobile phones in Improvised Explosive Devices (IEDs) to target citizens or as part of a larger attack. The unlawful use of IEDs- particularly by non-state armed groups and rogue individuals is spreading quickly[49]. Such IED attacks deliberately target civilian crowds to achieve maximum effect of lethality, terror and societal disruption; and are currently on a scale of hundreds per month globally[49]. The spread of communication technology has greatly

[43] Quartz Article by Alinoor Moulid Bosh on Kenya's Remittance to Somali Community (https://qz.com/379060/kenya-is-stopping-remittances-of-70-million-a-month-reaching-its-somali-community/), dated 08/04/2015, retrieved on: 28/05/2021

[44] Cryptocurrency Regulations Around the World," ComplyAdvantage, (https://complyadvantage.com/blog/cryptocurrency-regulations-around-world/)

[45] Brenna Smith, "The Evolution of Bitcoin in Terrorist Financing." Bellingcat, 9 August 2019 (https://www.bellingcat.com/news/2019/08/09/the-evolution-of-bitcoin-in-terrorist-financing/)

[46] Monero: A Resonably Private Digital Currency, Monero, (https://www.getmonero.org/)

[47] Jamie Redman Report on The Difference Between Custodial and Noncustodial Cryptocurrency Services, Bitcoin.com, 29 November 2018, (https://news.bitcoin.com/the-difference-between-custodial-and-noncustodial-cryptocurrency-services/)

[48] Andrew Gillick, "The importance of non-custodial decentralized exchange," Brave New Coin, 17 January 2019, (https://bravenewcoin.com/insights/the-importance-of-building-a-non-custodial-decentralized-exchange)

[49] United Nations Office for Disarmament Affairs on IEDS – a growing threat (https://www.un.org/disarmament/convarms/ieds-a-growing-threat/)

influenced IED knowledge-sharing, as online groups share instructional videos or materials, both on IED construction and on execution of attacks.

Because IEDs are multi-dynamic, regulation is complex - For instance, it is difficult to enforce on items that can also be used as technology. If an IED is activated using a cell phone, how will the law enforcement agencies differentiate between a cell phone for personal use and one for criminal purpose?

Al-Shabaab's biggest threat to peace in Somalia and the rest of Eastern Africa region is their frequent use of IEDs, especially vehicle-borne IEDs (VBIEDs), and making its use, common modus operandi for the terrorist group[50]. The terror group also have the capacity to manufacture their own IEDs due to its inexpensive assembling process. This can be illustrated by looking at the recent history of Al-Shabaab terror attacks, especially, the worst terrorist attack in October 2017 bombing of Mogadishu[50] where two truck bombs exploded in Mogadishu, killing at least 587 people and wounding several people. As of today, no terror group claimed the responsibility of the attacks, which is unusual for these kind of attacks, but, the bombing details suggests it was executed by the A-Shabaab terror group.

2.1.6. CYBERTERRORISM

The threat posed by cyberterrorism denotes unlawful attacks and threats against computers, networks, and information stored therein, to intimidate the government systems or its people for propagating hidden political or unlawful and religious agendas. For example, including Distributed Denial-of Service (DDoS) attacks, Man-in-the Middle (MITM) attacks and Phishing[5].

Simply, the use of computers, network systems and the internet connectivity, to launch a terrorist attack – in short, cyber terrorism is just like other forms of terrorism[51], the only difference is the change of attack setting. In fact, it is highly unlikely for cyber-terrorism to result to death as compared to offline terror attacks, like the use of bombs. However, significant economic damage, communication disruptions, supply chain disruptions, and degradation of the national infrastructure are all quite possible to execute through the internet.

With these tactics, cyber terrorists cause fear and panic to victims; as their activities range from computer hacking, spreading viruses and ransomware to obtaining information illegally and destroying computer networks. Examples of cyber-terrorism include:

- Accessing, disabling or modifying the signals that control military technology;
- Foreign governments using hackers to spy on other intelligence communication to learn about the country's troop location or otherwise gain tactical advantages at war;
- Global terror networks disrupting major websites, to create public nuisances or inconveniences – to try stop website traffic to content they disagree with.

Technological advancements and innovations have contributed to the rise of cyber-attacks; indirectly and unknowingly these advancements have benefitted the terrorists. For example, Younis Tsouli, better known by his Internet code name "Irhabi 007" (translated as 'Terrorist 007)[28], posted videos depicting terrorist activity on various websites.

Younis was sentenced to 10 years in prison for pleading guilty to inciting people to commit murder through their extremist websites[52]. For nearly two years before his arrest in October 2005, Younis transformed the internet into a sophisticate multimedia propaganda and recruiting machine for jihadist groups[52]. This is the first successful case prosecution based entirely on the distribution of extremist materials on the internet.

With global reach, conspirators no longer need to meet offline as they have found a sanctuary

[50] Institute for Politics and Society – Policy Brief on Terrorism in East Africa: Rise of Al-Shabaab and How to Counter it by Jan Havlicek (https://www.politikaspolecnost.cz/wp-content/uploads/2020/08/Terrorism-in-East-Africa-Rise-of-Al-Shabaab-and-How-to-Counter-It-IPPS.pdf), August 2020

[51] SolutionWeb page on Cyberterrorism (https://www.solutionweb.in/cyber-terrorism/)

[52] The Guardian Report on the Internet Jihadist jailed (https://www.theguardian.com/technology/2007/jul/05/terrorism.uknews), dated 05/07/2007, retrieved on: 28/05/2021

on the web[53]. For Younis case, the British Police investigations revealed the extent to which operational planning are conducted on the internet. Younis may be behind bars but the number of extremist websites are growing daily and such threats should be monitored frequently.

The cyber capabilities that the criminals could provide the terrorist organizations are more dangerous and effective. For instance, terrorists could open the valves at a chemical plant near population centers or amplify the destructive power of a physical attack by creating fear and panic and not having internet could greatly hamper government response to a series of massive and coordinated terrorist incidents. For example, a terrorist group might try to disable the 911 emergency system during an active terror attack.

2.2. Case Study One: The Dusit Al-Shabaab Terror Attack

Terrorists within the Eastern Africa region plan relatively complex attacks, quickly and effectively, including those on multiple targets[54] at the same time. The al-Qaeda affiliated terrorists allegedly planned the Dusit attack to coincide with the previous El Adde military base attack in 15 January 2016[55]. The scale and impact of lone-actor terrorist attacks might increase, with the use of modus operandi engaged in Syria and Iraq[54], such as the use of car bombs. In Kenya, during the DusitD2 Riverside Hotel attack on 15 January 2019, at around 14:30, the explosion was the first phase of attack[56]. Before the onset of attack, one of the terrorist, using a mobile phone, communicated with the rest of the group, then blew himself up near the secret garden within the complex.

Around the same time, four gunmen drive towards the compound entrance – the militants are forced to abandon their car, after two nearby police officers shoot at them. Moving on, the attackers threw grenades, setting ablaze three cars parked by the entrance gate[56]. This second explosion, in another location, was designed to create chaos and confusion. From the complex's CCTV camera, the insurgent terror group dressed in black, armed with assault rifles, with extra magazines of ammunitions.

The attackers were organized – splitting into two groups and making their way to the first office block. At this time, news of the attack began to spread on Twitter, as the militants made their way up to the top floor of the first office block, shooting and throwing grenades on the way. The other two gunmen moved to the back of the building, as people began to flee the building while taking precautions.

Within ten minutes, dozens of security forces began to arrive at the front of the compound, including some of the members of the Kenyan police special forces, Kenyan General Service Unit's RECCE Company (GSU/RECCE) tactical counterterrorism teams and the U.S Embassy's Special Program for Embassy Augmentation Response (SPEAR) team[57]. Several armed civilians also joined the operation as the paramedics began to treat the wounded and help with the evacuation.

By the time the gunmen reached the far end of the complex, most people had escaped the main office block, but at least 17 people were still trapped inside. The attackers moved floor to floor, identifying themselves as members of the militant group al-Shabaab[56], before shooting dead six people[56]. The militant group then moved onto the five-star Dusit hotel; many guests still seeking refuge inside their hotel rooms.

[53] BBC News Report by Gordon Corera on the world's most wanted cyber-jihadist (http://news.bbc.co.uk/2/hi/americas/7191248.stm), dated 16/01/2008, retrieved on: 28/05/2021

[54] EUROPOL Report on changes in Modus Operandi of Islamic State (IS) revisited (https://www.europol.europa.eu/publications-documents/changes-in-modus-operandi-of-islamic-state-revisited), dated, November, 2016

[55] Anadolu Agency News Report on the Dusit terror attack (https://www.aa.com.tr/en/africa/kenyans-recall-dusit-terror-attack-one-year-later/1704005#), dated, 15/01/2020

[56] BBC News Report on Kenya terror attack: What happened during the Nairobi hotel siege? (https://www.bbc.com/news/av/world-africa-47202313), dated, 12/02/2019

[57] DSS-trained police help neutralize terrorists, rescue score of civilians in Nairobi hotel attack (https://www.state.gov/dss-trained-police-help-neutralize-terrorists-rescue-scores-of-civilians-in-nairobi-hotel-attack/), Report by Roberto Bernando, Acting Director of the Office of Antiterrorism Assistance and Supervisory Special Agent, dated, 21/03/2019

The Islamist militant group al-Shabaab claimed responsibility for the attack[58] through their now closed Twitter account. They are the same group who were behind the Nairobi Westgate mall attack in 2013, in which 67 people were killed[56]. That siege went on for four days with a security response that was disorganized and uncoordinated; compared to Dusit, where, at around 18:00 at 14 Riverside, the majority of people had been rescued from the office blocks, with the militants inside Dusit hotel and one remaining office building in the line of fire[56].

The now former head of Kenyan police, Joseph K. Boinnet released a press statement[59] detailing that six of the Dusit's seven floors had been secured, Police officers were still in contact with some of those trapped inside the complex, through their mobile phones, internet-based messaging applications and social media platforms.

At around 22:48, the government announced that all the affected buildings had been secured[57] but the testimonies of those inside casted doubts on this, with gunfire and explosions continuing overnight and many people still trapped inside, now in the dark, still hoping to be rescued. Scores of people continued to escape overnight. The police then confirmed that fighting continued throughout the night[56], and the attackers were killed by 08:00 at the latest. Two hours later the Kenyan President, Uhuru Kenyatta, confirmed that the siege was over and more than seven hundred (700) were safely evacuated from the complex.

With terrorist attacks, the question for many citizens now is not just about how their government respond to such attacks, but whether such attacks can be prevented from happening in the first place.

2.2.1. AFTERMATH OF DUSIT TERROR ATTACK

This attack was carried out with simple means and was even more difficult to predict or foresee, let alone prevent. Pro Al-Shabaab account on social media celebrated the attack in Nairobi[58], and also in other parts of the world like the attack in Nice, France, leaving eighty five (85) dead and several hundred wounded[60]. The related messages, many of which were coordinated, expressed the belief that Islamic State (IS) was responsible for the attack, before any group claimed the attack[58].

The modus operandi jihadists employ in Syria and Iraq[54], however, may have been exported to Africa especially within the Eastern Africa region, as witnessed during the Dusit terror attack. One example is the use of suicide bombing, as seen in the Paris and Brussels attacks in 2015 and 2016, which was similar to Dusit attack where the suicide bomber detonated within the 14 Riverside compound, showing similarities in tactics, techniques and procedures employed in Syria and Iraq[54]. This shows the devastating potential of a lone-actor attack[60] employed by IS or insurgent terror groups.

Because Kenya has become a frequent target of terror attacks, the Kenyan government has taken steps to prevent and contain the attacks; Since the Westgate attack in 2013, Kenya has put in place stringent measures to counter-terrorism. This has included state of the art surveillance equipment, counter-radicalization strategies, capacity building activities and the establishment of the National Counter Terrorism Centre[61] in 2004. This centre is a multi-agency initiative responsible for strengthening and coordinating the counter-terrorism efforts, established in law under the Security Law Amendment Act 2014, to serve as a focal point for all counter-terrorism engagement with bilateral, regional and multilateral partners.

Additionally, the centre has a dedicated anti-terrorism police unit specifically mandated with detection, prevention and neutralization of terror threats as well as a programme to counter violent extremism including deradicalization and rehabilitation projects for potential and deplored terrorists.

[58] Combating Terrorism Center Report on East Africa's Terrorist Triple Helix: The Dusit Hotel Attack and the Historical Evolution of the Jihadi Threat (https://ctc.usma.edu/east-africas-terrorist-triple-helix-dusit-hotel-attack-historical-evolution-jihadi-threat/), dated July, 2019

[59] Press Statement on the Dusit Hotel Attack by the Kenya National Police (https://www.nationalpolice.go.ke/2015-09-08-17-56-33/news/270-press-statement-on-the-dusit-hotel-attack.html), dated 16/01/2019

[60] Journal Report on Forensic answers to the 14th of July 2016 terrorist attack in Nice, dated Jan, 2019, (https://pubmed.ncbi.nlm.nih.gov/29666997/) DOI: 10.1007/s00414-018-1833-5 , retrieved on 20/05/2021

[61] The National Counter Terrorism Centre Kenya Webpage (https://www.counterterrorism.go.ke/), retrieved on: 31/05/2021

As a result, Kenyans are more informed about terror attack countermeasures as witnessed in the recent DusitD2 attack where it was possible for the rescue operation to conduct a safe evacuation process as compared to the Westgate attack of 2013[62]. The DusitD2 operation was hugely successful due to the effective, precise security response and proper inter-agency cooperation. The first responders were quick to support the security agencies with ambulances, evacuation assistance, and standby personnel and medical staff[62]. The coordination between the various security response agencies was well coordinated as compared to previous attacks. For example, trapped hostages were able to communicate with security officers using their mobile phones through social media and internet-based messaging applications like Twitter, Facebook, and WhatsApp[63].

A centralized command centre under the paramilitary General Service Unit (GSU)[64] ensured smooth response coordination and minimized causalities, unlike Westgate, where all the teams in different multi-agencies coordinated the terror operations.

Additionally, a simplified communication approach, where the government officials engaged in a sparse press briefing, deploying two main communication channels: periodic press briefings and regular social media posts[64] created a centralized information channel which was a reliable and authoritative source, providing more clarity on the operation status. During a terror attack, it is important for communication to be centralized to ensure consistent narratives, information credibility, and to limit public or media speculation.

In the aftermath of the DusitD2 attack, Al-Shabaab terror group issued a statement claiming that it had staged the operation in accordance with an Al-Qaeda command demanding retaliation for the US embassy relocation to Jerusalem from Israel[64].

After claiming responsibility, the group said it had control of most parts of the Riverside building complex. However, there was little information on Twitter from Al-Shabaab as compared to the Westgate attack, the group instead used traditional media forms targeting the ethnic Somalis and international audiences. The group claimed the attack by issuing a statement in Somali on 15 January 2019 and publishing in a Somali website[64], linking the attack on the Palestinian issue aimed at the wider Muslim population and ranking the group on the global terrorist networks.

However, the group later issued an audio recording on 15 July 2019 in Somali featuring its spokesman, Sheikh Ali Mahmud Rage, applauding the attack. The recording was posted on the website of the Somali pro-al-Shabaab site, Calamada, seemingly directed at Somali audiences inside and outside Somalia. Besides linking the attack to the Palestinian cause, the recording also attributed the incident to Kenya's continued military presence in Somalia.

Later, on 15 January, the group's mouthpiece, Radio Andalus, broadcasted an extensive report on the Kenya attack and the content was published on the pro-al-Shabaab website, Somali Memo[64]. In retrospect, Al-Shaaab's media operations appears to be at low levels since 2013 and much of its propaganda focused on an audience in Somalia, until recently on 24 May 2021, where Al Shabaab allegedly released a video of Kenya Defence Forces (KDF) Soldier captured during the El Adde attack65 in Somalia In the 14-minute long video shared by the terrorist group's propaganda channels; the soldier retaliates that the Kenyan government withdraw troops from Somalia[66], and explains that the Kenyan government would step in and free the soldiers from Al-Shaaab's captivities. However, the video footage released by Al-Shabaab might be an online propaganda machine tool aimed at causing panic within the Kenyan government. While the groups have utilized high-tech platforms

[62] The Conversation News Report on the Kenya's Security Forces Response to DusitD2 terror attack (https://theconversation.com/kenyas-security-forces-did-better-this-time-but-there-are-still-gaps-110039), dated 20/01/2019, retrieved on: 31/05/2021

[63] BBC News Report on Dusit Attack (https://www.bbc.com/news/world-africa-46890332), dated 16/01/2019, retrieved on: 31/05/2021

[64] International Centre for Counter-Terrorism: DusitD2 Attack, Mitigating the Impact of Media Reporting of Terrorism Case Study of Government Communication during the Westgate and DusitD2 Attacks (https://www.jstor.org/stable/pdf/resrep27526.8.pdf?refreqid=excelsior%3Ad1d013675d829628250a6160d8a8804a), dated 01/12/2020, retrieved on: 31/05/2021

[65] International Peace Institute Report on El Adde Attack by Paul D. Williams (https://www.ipinst.org/wp-content/uploads/2016/07/1607_Battle-at-El-Adde.pdf), retrieved on: 31/05/2021

[66] Daily Post News Report on Al-Shabaab video of captured KDF Soldier (https://kenyan-post.com/2021/05/senior-kdf-soldier-who-was-captured-by-al-shabaab-5-years-ago-pleads-with-uhuru-in-an-urgent-message-to-him-look/), dated, 26/05/2021, retrieved on 31/05/2021

like YouTube, Facebook, Instagram, and Twitter[67], the use of lower-tech media devices are still increasingly effective in spreading their radical Islamic teaching, transit propaganda, and incite followers, particularly those living abroad. For instance, Islamic State's (IS) English magazines Dabiq and Rumiyah, as well as Al-Qaeda English-language periodical, Inspire, are examples of low technology-based channels spreading terrorist messages[67].

2.3. Case Study Two: Westgate Mall Attack in Nairobi, Kenya

The September 2013 Al-Shabaab attack on Nairobi's Westgate Mall was fully captured on the mall's security cameras and broadcasted across the world[68] - the attack was seen as response to Kenyan military activities in Somalia against Al-Shabaab. At the time, the attack became, for the developed world, the face of jihadi terrorism in Africa[68]. The attack highlighted the incapacity of the Kenyan security services. That said, the improved coordination of different security agencies can be noted, during the recent DusitD2 attack.

The Somali-based Islamist group Harakat Al-Shabaab al-Mujahideen (aka Al-Shabaab, aka the youth, aka mujahidin Al-Shabaab Movement, ala Mujahideen Youth Movement, aka Hizbul Shabaab, aka Hisb'ul Shabaab, aka Youth Wing)[69] claimed the responsibility for the attack through its now closed Twitter account.

During the on-going terror siege, the Al-Shabaab terror group, through an associated Twitter account, tweeted, ''The Mujahideen {holy warriors} entered Westgate mall at around noon and they are still inside the mall, fighting the Kenyan kuffar {Infidels} inside their own turf,''[70] – with this information, the Kenyan government and the international community were in crisis to neutralize an active terror attack. At the same time, the mainstream media used the tweets to report on the on-going terror attack.

Al-Shaaab's press office proceeded to create and disseminate on Twitter justifying the attack, generating fictional threats, and providing its version of news throughout the terror operation – This was the first time a terrorist group claimed responsibility for an attack using Twitter and provided coverage in real time throughout the entirely of the assault[70].

As outlined above, the weaponization of social networks as information hubs is a preferred tool amongst terrorist organizations operating in today's cyberspace, with 90 percent of organized terrorism on the internet executed through social media[70]. In particular, Twitter allows terrorist groups to concisely disseminate messaging and facilitates international communication before, during, and after attacks.

The terrorist organizations simultaneously utilize tendencies in mainstream media, which signals a growing validation and in-depth analysis of real-time coverage, to methodically exploits this shortcoming for propaganda and recruitment purposes.

With this trend, the mainstream media often use the terrorist tweets as legitimate news sources in cases where mainstream media coverage is limited. The terror group choose to cover their attacks in real time using the internet as an enabler, thus posing a distinct challenge to security agencies, first-responders, counterterrorist strategic communications, and the public, in general. It is evident that the majority of tweets reveals that

[67] The Best of Africa News Report on The Propaganda Machine: Al-Shabaab's Radio Andalus, (https://thebestofafrica.org/content/the-propaganda-machine-al-shabaabs-radio-andalus), dated 30/10/2020, retrieved on: 31/05/2021

[68] Council on Foreign Relations Article on Justice, Terrorism, and Nairobi's Westgate Mall by John Campbell (https://www.cfr.org/blog/justice-terrorism-and-nairobis-westgate-mall), dated 9/10/2020, retrieved on: 10/06/2021

[69] The Westgate Terrorist Attack and the Transformation of Al-Shabaab: A Global Jihadist Perspective by Daniel E. Agbiboa (https://www.researchgate.net/publication/261711378_The_Westgate_Terrorist_Attack_and_the_Transformation_of_Somalia's_Al-Shabab_A_Global_Jihadist_Perspective), March 2014, retrieved on: 10/06/2021

[70] Tweeting Terror Live: Al-Shabaab's Use of Twitter during the Westgate Attack and Implications for Counterterrorism Communications by Victoria Fassrainer (https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MA-20/Fassrainer-Tweeting-Terror.pdf), March –April 2020, Retrieved: 10/06/2021

the Al-Shabaab's intention was to further their ideology, justify the attacks, and provide periodical news updates. According to David Mair report[71], the Al-Shabaab relied on Twitter for publicity, propaganda, psychological warfare, and command and control.

In 2020, the minds behind the Westgate Mall attack were sentenced to 18 years in prison for helping and providing support to Al-Shabaab terror group, through possession of propaganda materials promoting terrorism ideologies. Although, there was no specific evidence, the convicted pair provided propaganda material help, and the court were content that the suspects communication with the attackers constituted to supporting the Al-Shabaab terror group, and justified the guilty verdict for conspiracy[72]. In retrospect, the Westgate Mall terror attack provided the law enforcement agencies with devised tactics to handle terror attacks. For instance, the availability of digital evidence during and after the attack, assisted the law enforcement with crucial information to prosecute the suspects and build capacity on handling digital evidence, especially in relation to terrorism cases.

2.4. Conclusion

The use of internet for acts of terrorism is a trans-border problem, which requires an integrated response across borders and with the effort of international criminal justice systems. By facilitating discussions and sharing good practices among Member states, as well as building agreements on common approaches to counter the use of the internet by terror insurgent groups in Eastern Africa.

As discussed in section 2 above, the relevant applicable international legal framework related to counter-terrorism is detailed in a number of sources, including the General Assembly and Security Council resolutions, treaties and international laws. As such, the internet is often utilized to promote and support acts of terrorism, in particular related to online propaganda (including social media recruitment, radicalization, and incitement to terrorism), training, financing, planning, cyberterrorism and executing such acts. However, the internet also provides the opportunity to prevent, detect and deter acts of terrorism, including through open source intelligence.

[71] David Mair, "#Westgate: A Case Study: How al-Shabaab Used Twitter during an Ongoing Attack," Studies in Conflict and Terrorism 40, no. 1 (25 February 2016): 24–43.

[72] Aljazeera News Report on "Kenya court finds two guilty in deadly Westgate Mall attack" (https://www.aljazeera.com/news/2020/10/7/kenya-court-finds-two-men-guilty-of-role-in-deadly-mall-attack), dated 7/10/2020, retrieved on: 10/06/2021

3. Methodology

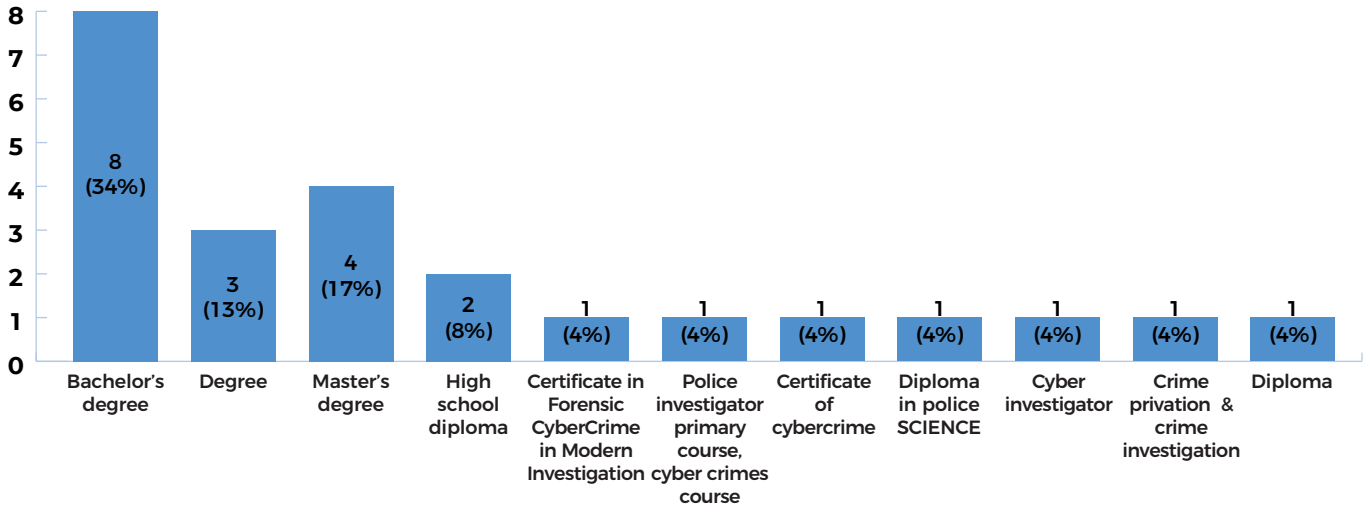
To achieve above objectives, this research paper presents an evidence-based research technique, with data collected through one questionnaire. The Use of Internet for acts of Terrorism questionnaire was completed by twenty-six (27) officers representing Kenya (5), Somalia (7), Rwanda (5), Tanzania (5) and Ethiopia (5), who attended a hybrid-online UNODC- ROEA Regional workshop on Strengthening Investigations, Open Source Intelligence (OSINT) Capabilities to Counter-terrorism and Transnational Organized Crimes, held on 28-30 June 2021.

The abovementioned questionnaire incorporates a combination of structured and open-ended questions, and the responses will be used for analysis purposes, to understand how internet can be used for terrorism purposes. Additionally, a five-level liner Likert item was used to measure the links between the internet, digital platforms, digital devices and terrorism.

3.1. Background of respondents

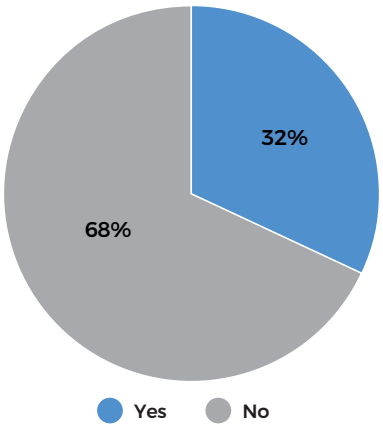
From the responses, the officers tasked to perform counter-cybercrime activities in their respective units, the majority of officers have completed university-level education, with additional specialized cybersecurity qualifications. This shows expert-level capabilities in tackling counter-terrorism cases. The ***Figure 2 below*** shows each respondent' level of education.

Figure 2: shows highest qualification, with majority mentioning Bachelor's degree



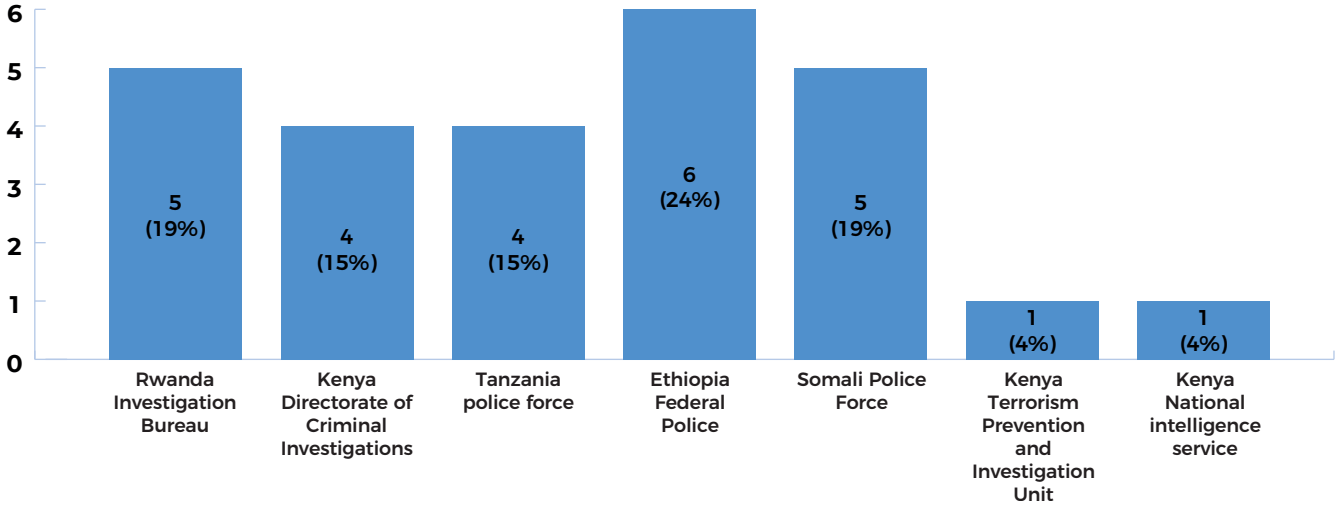
As cybersecurity tends to be complex in nature, and as detailed in ***figure 2 above***, the officers were able to understand basic concepts in relation to Digital Forensics and Cybercrime. With basic understandings, the officers can advance their skills without any difficulty, and understand the complexity of cybercrime investigations.

Figure 3: Shows additional qualification in Cybersecurity, with 68% as yes, and 32% as no



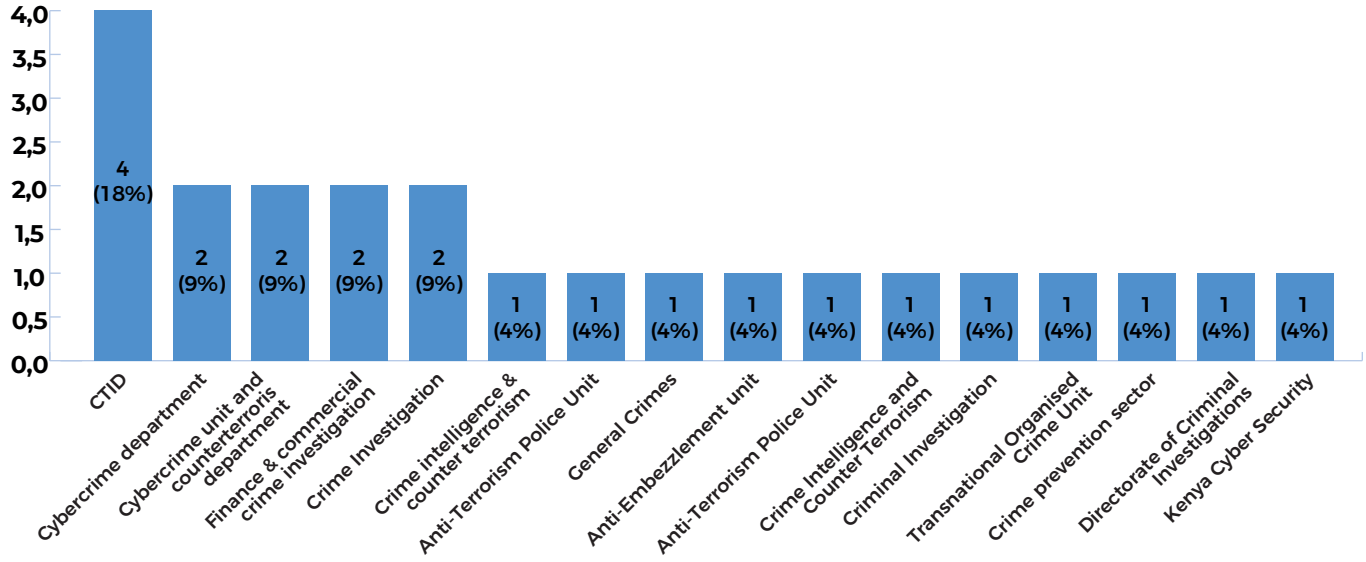
From the responses, the additional qualifications, include certificates in Forensic Cybercrime for Modern Investigations, Cybercrime Courses, FBI Cybercrime Investigation courses, law enforcement GIS and GPS technology, Surveillance anti-terrorist, Open Source Intelligence, CeH, and CHFI. The representation of the respondents' different organization is shown in ***Figure 4 below***.

Figure 4: Respective unit Agency names (Directorate of Criminal Investigation, Ethiopia Federal Police, National Intelligence, Tanzania Police, Rwanda Investigation Bureau, Somali Police Force



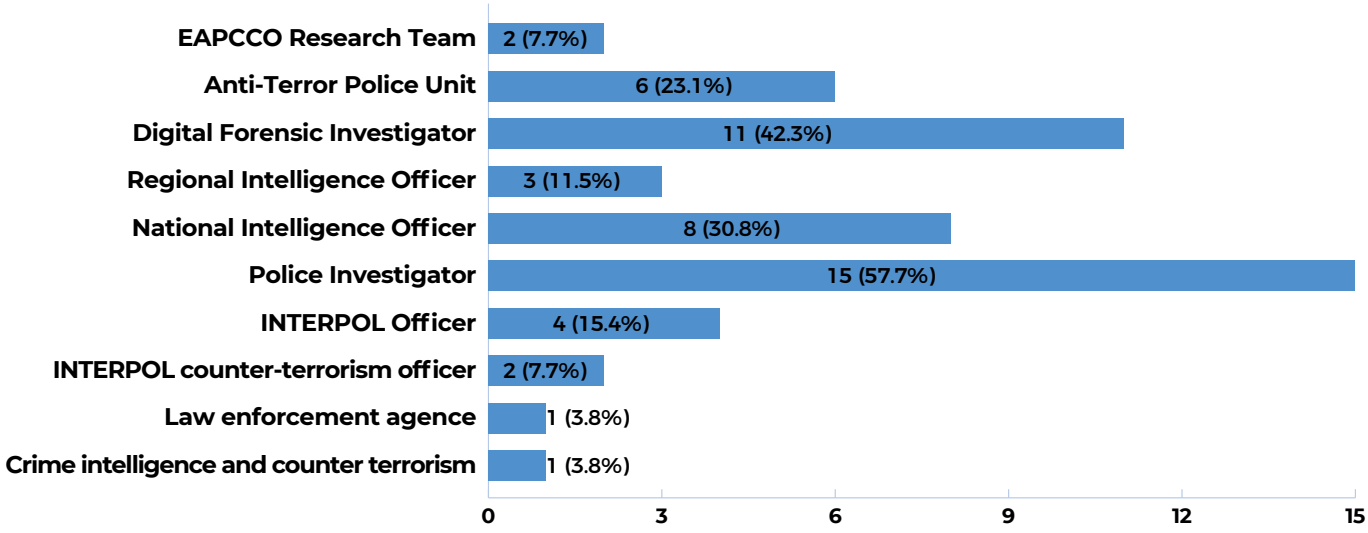
Also, noting that most of the officers were from the cybercrime investigation units, especially on counter-terrorism cases, as shown in ***Figure 5 below***.

Figure 5: shows the representation of different unit in respective countries



To understand, each individual responsibility within the unit, the following ***Figure 6 below***, shows each respondent's job function.

Figure 6: shows each respondents' individual responsibility in their respective units, with majority being police investigators at 57.7%



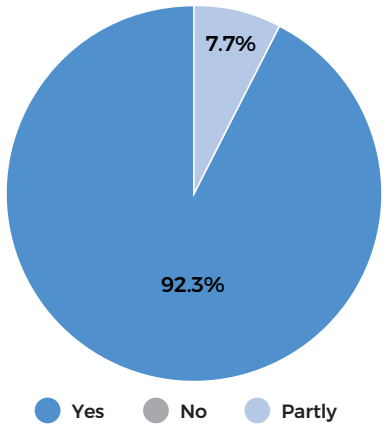
As shown above, the questionnaire was completed by a diverse group of individuals within the respective units, with majority being police investigators at **57.7%**, the Digital Forensic investigators at **42.3%**, the national intelligence officers at **30.8%**, the anti-terror police unit at **23.1%**, INTERPOL officers at **15.4%**, Regional Intelligence officers at **11.5%**, INTERPOL Counter-terrorism at **7.7%**, EAPCCO Research Team at **7.7%** and lastly, other law enforcement agencies at **3.8%**.

3.2. Understanding the Use of Internet for Acts of Terrorism in Eastern Africa

From the respondents' feedback, the use of internet for acts of terrorism in Eastern Africa is evident by previous terror attacks within the region, especially in Kenya and Somalia. The internet and other digital platforms have been directly or indirectly used to commit acts of terrorism, either through planning, financing, execution, propaganda, training or cyberterrorism.

To understand the different links between terrorism and the internet, the ***Figure 7 below*** shows respondents' responsibility in investigations, especially counter-terrorism investigations.

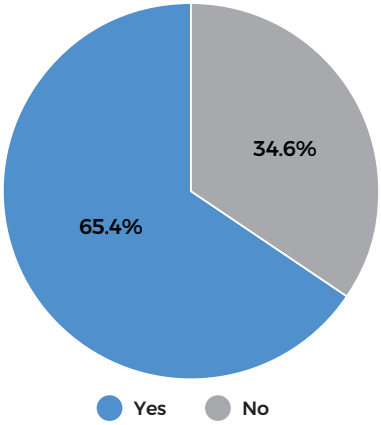
Figure 7: shows majority of respondents are involved with investigations, as part of their duties, with 92.3% as yes and 7.7% as partly being involved



From above mentioned and with respondents' responses, this includes investigation of all cases, from evidence collection, evidence analysis, prevention, crime detection, criminal profiling, crime data analysis, intelligence collection, financial crime investigations, terrorism investigations, information sharing, and investigation of cyber- related crimes.

To further understand the aspects of digital investigations, the different units within the region responded that a dedicated Digital Forensic Lab (DFL) is in place, which is being used primarily for digital investigations, as shown in ***Figure 8 below***.

Figure 8: Shows that the units have a dedicated DFL at 65.4% and 34.6% as without a functioning lab

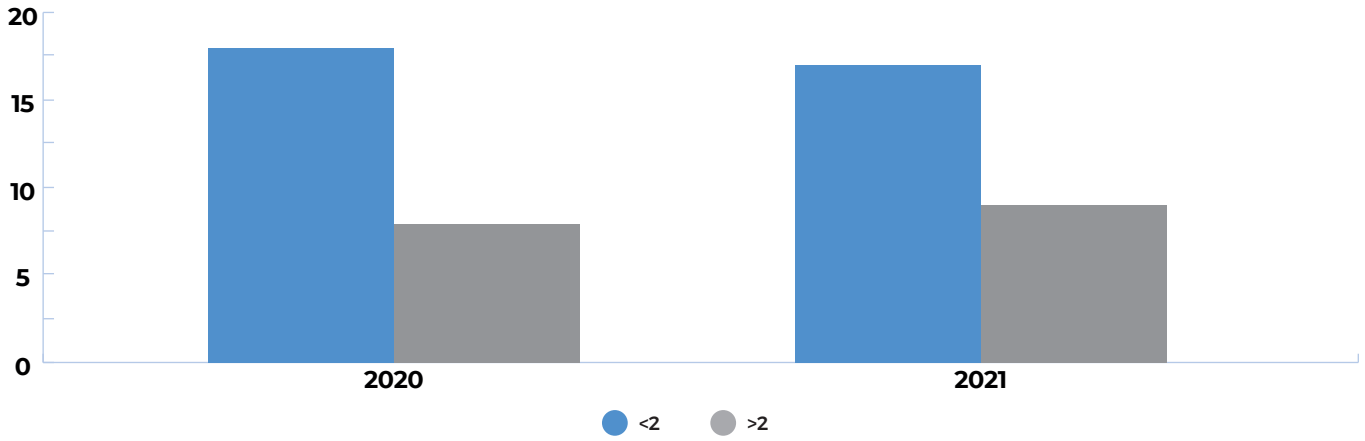


From the responses, the digital forensic lab in respective units is equipped with forensic tools like Cellebrite, Oxygen Forensics, Forensic Toolkit (FTK), Encase, Sleuth Kit, Extraction Software, MOBILedit, Getac system and fingerprint or DNA machine.

To further understand the number of counter-terrorism digital investigation cases, the respective units detailed the cases handled in 2020 and 2021 respectively as shown in ***Figure 9 below***.

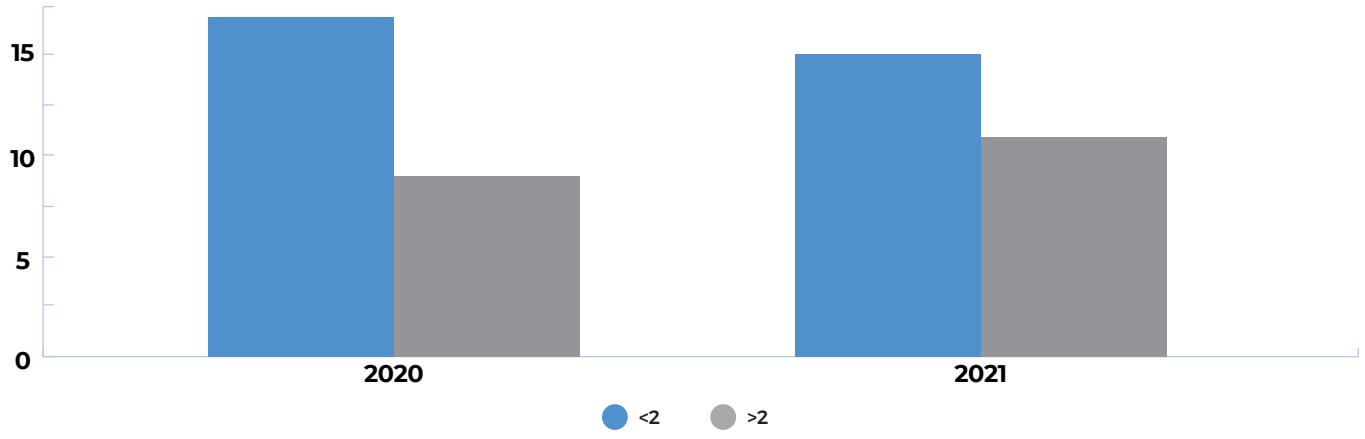
Figure 9 below detailed that counter-terrorism cases, especially in relation to digital investigations are present in almost all respective units, in each country.

Figure 9 below: shows that in 2020, investigated cases were less than two and similar in 2021



For further analysis and understanding of how each unit investigates digital devices and platforms, and if it involved the use of forensic tools, ***Figure 10 below*** shows the number of cases in 2020 and 2021 that involved the use of specialized digital forensic tools.

Figure 10: shows the number of cases involving the use of digital forensic tools, in 2020, with less than 2 indicating the number of cases, and in 2021 the cases shows less in the number of cases investigated

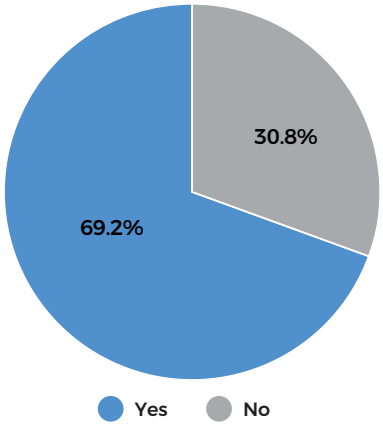


From the cases handled by the respective units, the most common communication channels used by the terror insurgent groups, include phone calls, text messages, internet based messaging applications like Facebook Messenger, WhatsApp, Signal, Telegram, Emails exchange and YouTube. Also, noting that Rwanda respondents did not encounter any terror alerts or cases in 2020 and

2021. Additionally, as shown in ***Figure 11 below***, responses show **69.2%** of cases relate to the use of internet for acts terrorism related incitement or communication through social media sites (Facebook, Twitter, TikTok, YouTube, Instagram, WhatsApp, Telegram or other platforms.

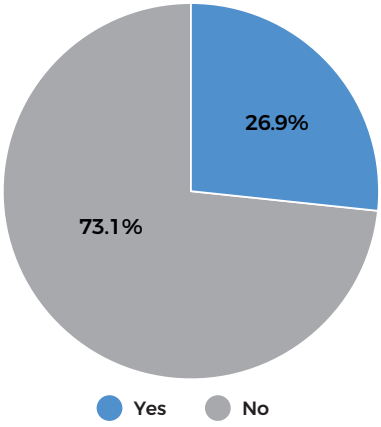
The internet-based technologies are used for communication, either as a planning and logistic tool to allow the terror groups execute their acts effectively. As such, it offers a wider audience for the terror group to communicate without a limitation of geographical area, allowing the group to communicate seamlessly and anonymously using encryption technology. Also, the internet and social media is used to radicalize and recruit youths or supporters in the region, as mentioned by the respondents, the most commonly used social media sites include WhatsApp, Telegram as well as dark web forums, YouTube, Facebook, TikTok, Websites forums and Twitter.

Figure 11: shows that at 69.2% the use of internet for communication purposes (through either terrorism-related incitement)



Another important aspect is the use of drones as a target monitoring tool, and for surveillance, executing and launching attacks. However, it is not common in the Eastern Africa region as compared to other regions. From respondents' responses, majority have not intercepted drones, and its use cannot be conclusive in this report. The ***Figure 12 below*** shows the percentage of drone interception as 26.9%, with digital data like memory cards, imagery and videos found.

Figure 12: shows the percentage index of intercepted drones within the region



3.3. Understanding links between Terrorism and the Internet

Mutual Legal Assistance (MLA) is an important tool in countering cybercrime, allowing law enforcement agencies to request and preserve digital evidence. From respondents' responses, majority of the law enforcement agencies have little understanding on drafting a detailed MLA and how to send online law enforcement requests., for example Facebook online law enforcement requests[73], TikTok Law enforcement guidelines[74], Google YouTube Law Enforcement Request[75], and Twitter Law Enforcement Request[76], among others. ***Figure 13 shows*** at **38.5 %** having used social media emergency to request and preserve digital evidence, while **65.4%** did not request for any assistance.

Figure 13: shows the number of requested assistance from the respondents'

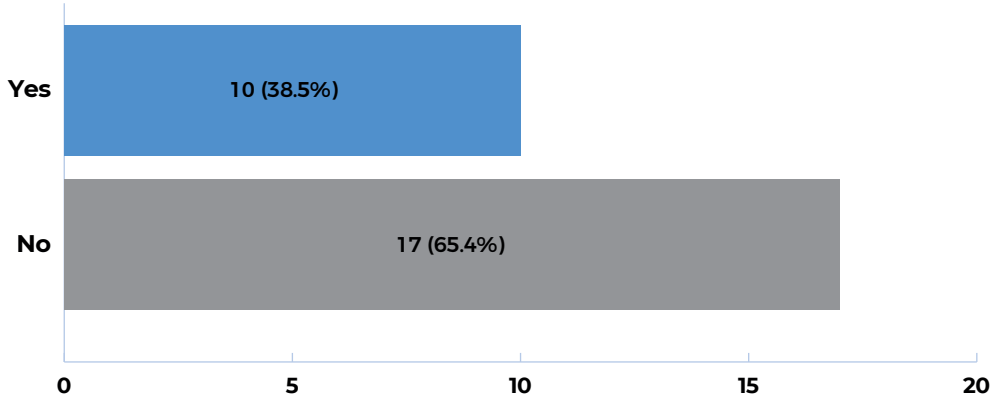


Figure 14 helps to better understand the responsibility of technology companies, internet service providers, and mobile service providers in responding to terrorist and violent extremist misuse of their platforms, and how the responses were acted upon the aforementioned companies. ***Figure 14 below*** shows how the technology companies responded to law enforcement requests, in terms of response time, with **57.7%** as no response, **30.8%** as quick response and **11.5%** as slow response. As MLA are important to law enforcement agencies, the response time might be attributed to poorly drafted requests or the use of unofficial channels to request or preserve digital evidence.

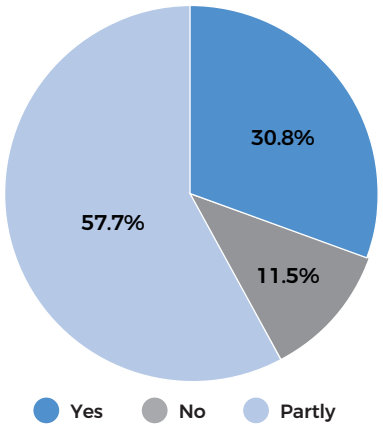
[73] Law Enforcement Online Request (https://www.facebook.com/records/login/), retrieved 08/07/2021.

[74] TikTok Law Enforcement Guidelines (https://www.tiktok.com/legal/law-enforcement?lang=en), retrieved 08/07/2021

[75] Google YouTube Law Enforcement Online Request (https://support.google.com/legal-investigations/contact/records), retrieved on 08/07/2021

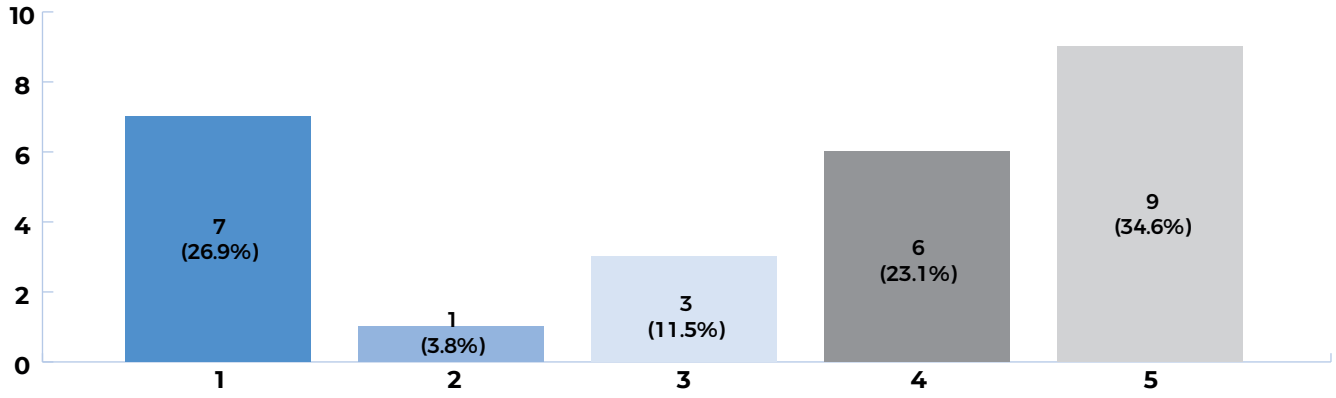
[76] Twitter Law Enforcement Online Request (https://help.twitter.com/en/forms/law-enforcement), retrieved 08/07/2021

Figure 14: Mutual Legal Assistance Response Time



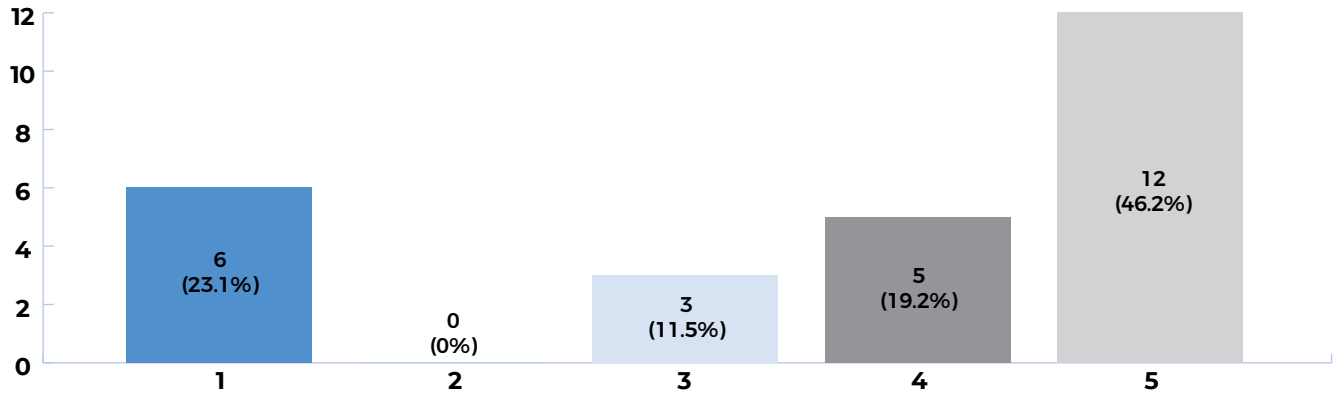
As discussed in section 2 above, the internet can be used for acts of terrorism, including planning, online propaganda, training, financing, execution and cyberterrorism. From each element, the Likert responses include, on a scale of one (1) to five (5), how each element is likely being used by the terror group within the region. As shown in ***Figure 15 below***, terror groups likely use the internet for planning purposes either through encrypted communication or open-source intelligence gathering, at **34.5%** being highly likely and **26.9%** being less likely.

Figure 15: shows at 34.6% the likelihood of the internet being used for planning purposes



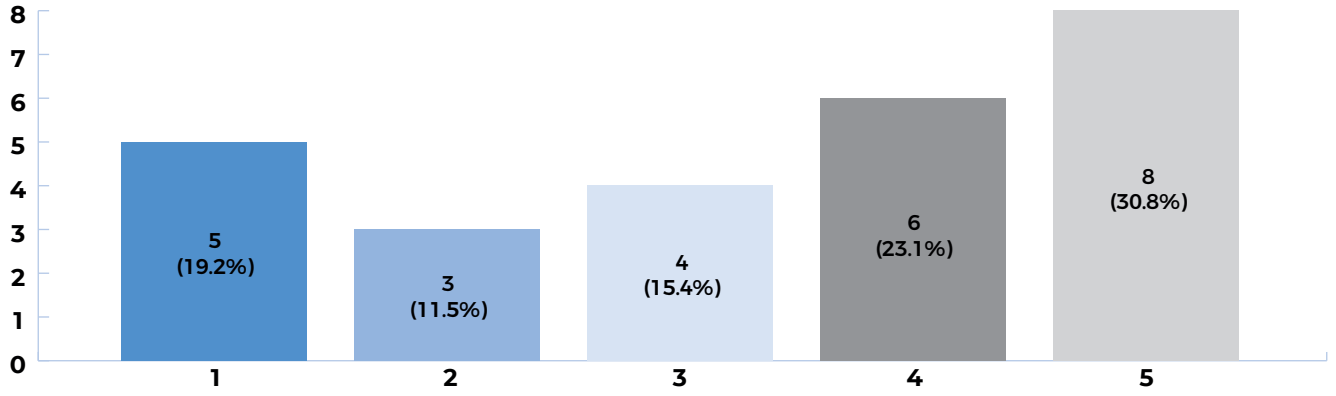
The internet and social media technologies are likely being used by terror groups for online propaganda purposes, either through social media recruitment, radicalization, tailored messaging targeting potential new recruits or propaganda dissemination by spreading ideologies and justifying terror attacks. As shown in ***Figure 16 below***, and the respondent' analysis, and one (1) being less likely and five (5) being highly likely, showing at **46.2%, and 19.2%** of propaganda is likely posted on the internet.

Figure 16: shows at 46.2% the likelihood of the internet being used for propaganda purposes



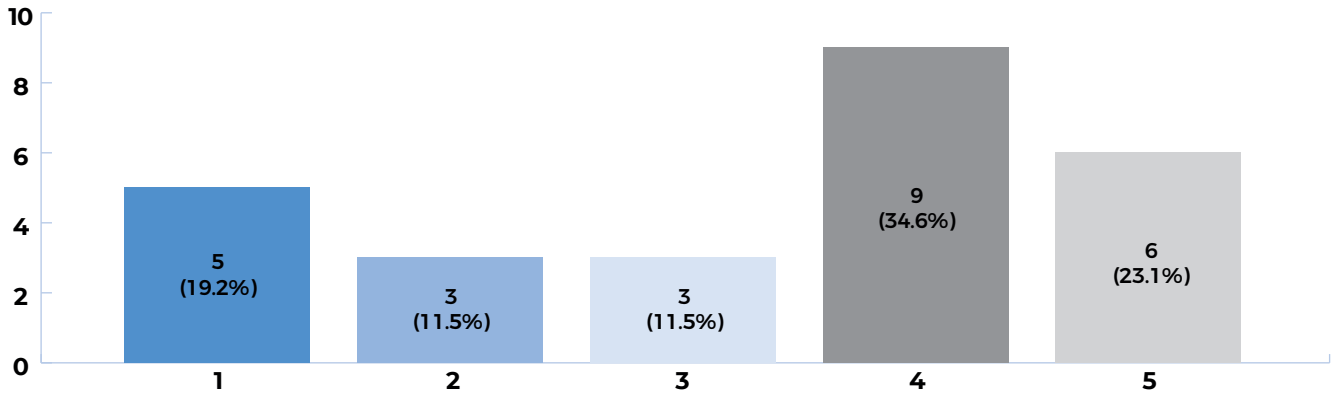
The internet can be used as a virtual training ground for terror groups, through knowledge-based sharing platforms, dissemination of training guides, and sharing resources on internet-based messaging platforms. As shown in ***Figure 17 below***, it is highly likely that the internet is used for training purposes.

Figure 17: shows at 30.8% the likelihood of the internet being used for training purposes



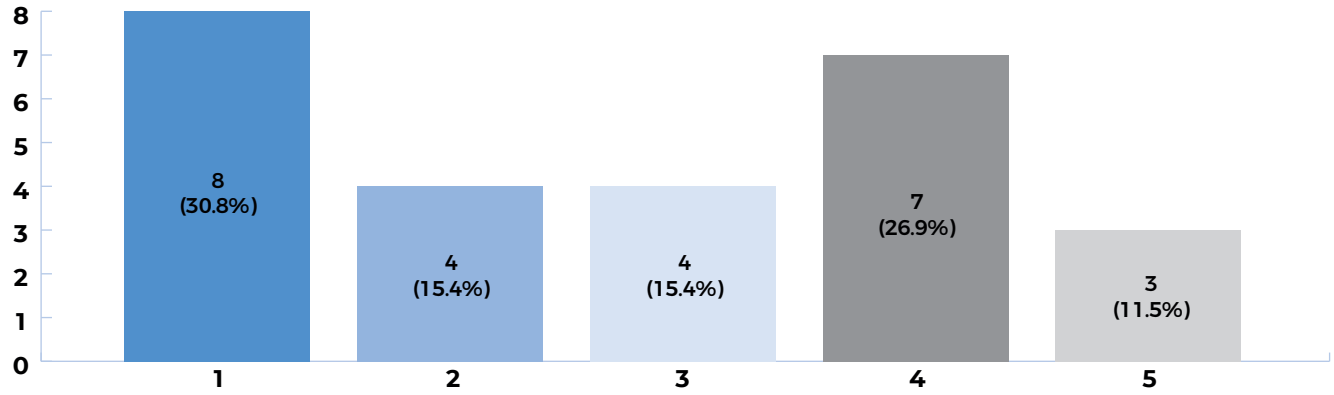
The internet and digital platforms are likely being used for financing purposes, including the use of the internet to raise and collect funds through direct solicitation, mobile money transfers, online payment exploitation tools, Hawala systems, cryptocurrency fraud, charitable organization, front companies and E-commerce. Respondents account for the use of the internet for financing purposes at **34.6%** and **23.1%** as highly likely being used for this purpose, as shown in ***Figure 18 below***.

Figure 18: shows at 30.8% the likelihood of the internet being used for financing purposes



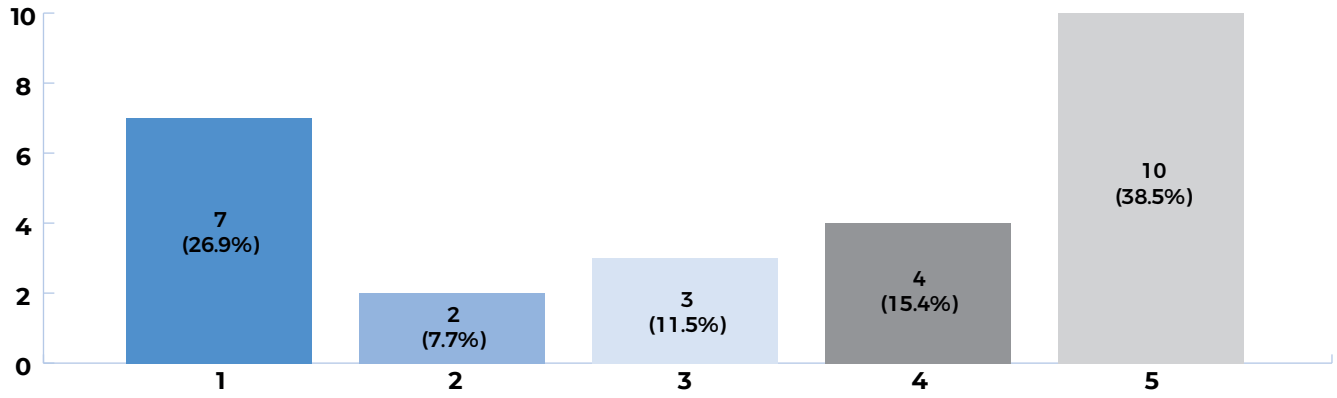
Mobile phone devices are used to detonate IED's in Somalia and parts of Northern Kenya, and sometimes the use of drones. As aforementioned, drones are not common within the region, and the law enforcement have been able to intercept a number of drones. As accounted by the respondents, as shown in ***Figure 19 below***, with most responses being less likely, while Somalia responding high to the use of IEDs.

Figure 19: shows at 26.9% and 11.5% the likelihood of the internet being used for execution purposes



Cyberterrorism is a new concept within the region, the internet and digital platforms are likely used to facilitate it, for example phishing attacks, Distributed Denial of Service (DDoS) attacks, or Man-in-the-Middle (MITM) attacks. As such, respondents' account for a number of incidents in the region, as shown in ***Figure 20 below***.

Figure 20: shows at 38.5% and 15.4% the likelihood of the internet being used for cyberterrorism purposes



To successfully prosecute cyber-related and other terrorism cases, each country should follow common laws, regulations and acts. For example, In Somalia, a special penal code law is used to prosecute terrorism cases, In Kenya, Prevention of Terrorism Act 2012, Firearms Act and Cybercrime Act, In Ethiopia, the Proclamation Code Number 652/2009, In Rwanda, prosecutors use the criminal code law to prosecute terror activities and in Tanzania, there is the Prevention of Terrorism Act of 2002. This counter-terrorism legislation was first introduced after the 11 September terror attacks. Some officers are not familiar with specific laws to prosecute terror suspects, as most of them deal with other aspects of cybercrime investigations.

With effective criminal justice systems, cybercrime cases can be prosecuted within the current law system. However, due to emerging technologies, some of the laws within the region do not cover cybercrime and cyber-enabled crimes, making the law enforcement agencies devise or use existing laws that might not be appropriate to prosecute terror cases. As accounted by the respondents', the laws have not been updated to cover cybercrimes, cybercrime extradition cases and how to prosecute cyber-enabled crimes.

However, in Kenya, the 2012 Prevention of Terrorism Act (PTA) criminalizes any person who conspires to commit a terrorist act abroad while in Kenya or if a person in Kenya commits an offense, they are liable to twenty (20) years in prison.

4. Recommendations

Following an extensive literature review and respondents' accounts, the research paper addresses the use of internet, digital platform and other digital devices to commit or support acts of terrorism within the Eastern Africa region. The main purpose of this study is to present recommendations based on evidence-based research, addressing the challenges in dealing with terrorism cases, specifically digital evidence and social media or internet- based evidence.

The recommendations will be important for policymakers, law enforcement agencies, UNODC, as well as public-private companies, including international organizations, on how to better build international cooperation to tackle the use of internet by terror groups.

The recommendations are important to address challenges including those presented in the report, which includes, how to effectively draft Mutual Legal Assistance (MLA) requests, end-to-end encryption technology, inadequate evidence collection techniques, unavailability of digital forensic tools, anonymous online identity, unavailability of legal procedures to prosecute online terrorism cases, and lack of specialized training.

4.1. Mutual Legal Assistance to counter the use of internet by terror groups

As detailed in Figure 13 above, only 38.5% of the respondents requested for social media law enforcement emergency requests. Digital evidence is a key issue in countering cybercrime, especially in relation to terrorism cases. Preservation and collection of digital evidence have become key elements in ensuring that cyber-related crimes are prosecuted effectively.

There is a growing need for international and national cooperation between internet and social media service providers, through strengthening cooperation to help track offenders and providing the requested evidence against perpetrators of terrorist crimes.

Another aspect to requesting digital evidence is the legal aspect of requesting evidence across the borders. Online terrorism is a cross-border crime, and requires collective efforts between law enforcement agencies, officials and social media service providers, to obtain electronic evidence. Furthermore, working with the private sector to strengthen compliance with international law, in particular international human-rights standards, is also important in addressing and prosecuting online terrorism cases.

The need to engage the private sector is important to counter organized crime and terrorism, which advocates for self-regulation and encouragement for internet service providers to take more responsibility in preventing misuse of their platforms and services.

To further establish regional partnership between respective law enforcement agencies, Open Source Investigation Techniques (OSINT) should be up scaled, by doing this, it strengthens initiatives to enhance partnership between different member states to effectively prevent, investigate and prosecute counter-terrorism cases, especially in relation to the use of internet by terror insurgent groups.

4.2. Countering Use of the Internet for Terrorist Purposes

As discussed in the section above, it is evident that terror groups use the internet for planning, recruitment, radicalization, online propaganda, communication, financing, logistics, execution and cyber-terrorism. To achieve the objectives, the following measures should be followed:

- Monitoring online activity, and collecting information and open source led intelligence to support counter-terrorism efforts;
- Shutting down online activities that terrorists engage with;
- Undertaking appropriate measures to counter terrorist narratives and terrorist online activity and support;
- Denial of services by destroying terrorist cyber networks.

These measures are often necessary and used by law enforcement; however, they can also raise serious human rights issues and questions about the protection of the freedom of speech. It is important to continue to seek law enforcement solutions that protect and respect human rights and the freedom of speech.

1. Monitoring and Intelligence Collection

With regard to monitoring and collection, it is critical to collect information about adversary intent and capabilities in a timely, safe and effective manner. For example, both Twitter and Facebook generate greater opportunities for network analysis and geo-location capabilities. Further, given the anonymous nature of the internet, and the use of honeypot techniques, terrorist networks can be disrupted easily. On the other hand, law enforcement must take precautions while accessing online forums during the monitoring phase, to avoid exposing their identities online.

2. Shutting Down Terror Networks

By shutting down terrorist activity online, terror groups' activities will be disrupted. It is important to consider each jurisdiction's laws before engaging with internet or social media providers. When service providers push the content out of their platforms, they make it harder for terror groups to access the content online. However, some terror groups devise ways to access the content online.

3. Investigations and Intelligence-gathering

Effective internet investigations rely on a combination of skilled personnel, knowledge of open source tools to conduct anonymous investigations, and the development of best practices targeted to identify, apprehend and prosecute the perpetrators of such acts. A proactive approach to investigative strategies includes providing specialist tools to disrupt the evolving internet resources, thus promoting efficient identification of data and information to the benefit of investigation. The availability of open-source tools allows for acquisition of digital evidence and preserving data integrity that can be used in a court of law. Owing to the fragile nature of digital evidence, its assessment, acquisition, and examination must be effectively performed by specialized and trained forensic experts.

4. Penetrating the Deep and the Dark web

With the advancement of anonymous communications, the internet facilities are increasingly abused by terror groups. Law enforcement agencies within the region should have systems that support actions against abuse or the use of the internet by terrorist. This can be achieved by searching through and filtering operational databases, that can be further processed either by fully automated or by semi-automated tools. To achieve this level of investigation, counter-terrorism focused search engines need capability to handle normal internet data, and also to access data from the deep and dark webs. The forums can be accessed by specific forms and tools applied during data processing, depending on the type of internet abuse by terrorists, as discussed above.

4.3. End-to-End Encryption Technology

The development of increasingly sophisticated technologies has created a network with global reach, and relatively low barriers for entry. For instance, internet technology makes it easier for terror groups communicate with relative anonymity, quickly and effectively across borders, with an almost unlimited audience. Encryption technology poses significant challenges to public safety, including terrorism and online child abuse cases. The technology is applied in a way that it precludes any legal access to digital content. As such, technology companies should work with different government agencies to take steps, and provide reasonable solutions to tackle encryption issues. For example, allowing law enforcement agencies to access content in readable and usable formats where an authorization is lawfully issued, and facilitating legal access in a substantive and genuinely influence design decisions.

Law enforcement agencies have the responsibility to protect citizens by investigating, prosecuting and safeguarding their rights and preventing terror attacks. As such, technology companies have the responsibilities within their terms of service to provide agencies with appropriate information by identifying and responding to terms of service violations. Violations include child sexual exploitation and abuse, violent crime, terrorist propaganda and terror attack planning.

The open nature of the operating systems, especially android systems, complicates regulation of the development of backdoors into encrypted messaging programs. For example, android systems, allow users to download materials from all websites using compatible code, and any law or policy limits the encryption technology. This makes law enforcement counter-terrorism efforts more difficult in tackling information available in surface and dark web.

If law enforcement agencies have limited ability to detect criminal activity because of lack of communication between subjects, data in motion, data held by subjects, or data encrypted in such a way that makes the content inaccessible, even with a lawful order, citizens cannot be protected accordingly. Therefore, service providers and law enforcement must continue to collaborate together to explore possible technical solutions that would provide security and internet privacy. Lastly, terrorism remains a problem and a challenge in undermining the digital security of the society and will continue to be a problem if the capabilities of security services are not improved.

4.4. Capacity Building

Capacity building is the key to the fight against terrorism. The Eastern Africa region is faced with an increasing threat in cyberspace, cohesive and as such comprehensive policies are essential in building an effective cyber defence. The changing phases of cyber-attacks and sophistication of attack methodologies presents new and emerging cyber security changes. Consequently, there is a necessity for law enforcement, criminal justice systems and judiciary to keep pace and be prepared to prevent and respond to these security risks.

This paper has recognized the serious threats posed by cybercrime and the need to prosecute cybercriminals effectively, specifically the capabilities of law enforcement agencies need to improve in detecting, handling and prosecuting cybercriminals. Further, the judiciary must advance their understanding in terms of the technicalities and complexities of cybercrime cases presented in courts. It is therefore imperative to develop a coordinated approach in developing a National Cybercrime Strategy in each country within the region.

The National Cybercrime Strategy will provide an insight into how each government approaches and responds to the fight against cybercrime. This will provide a swift response to cybercrime through improved law enforcement capability, an effective criminal justice framework and active international engagement.

In addition, collaboration between key players in both the public and private sectors to safeguard national cyberspace is critical. To achieve this, six high priority areas are identified that will help in strengthening the national response to cybercrime, especially in relation to counter-terrorism.

Priority Areas:

i. ***The development of an effective criminal justice and legal framework to detect, handle and prosecute cyberterrorism:*** This will enable and facilitate new law enforcement, with regard to different types of cybercrime and its prosecution, and also provide legal practitioners and judicial officers with capacity and expertise to deal with digital evidence.

i. ***Building capacity to better address the use of internet by terror groups:*** The capacity and capability of legal professionals and the judiciary, in enhancing the technical aspects of cybercrime, such as digital evidence examination.

i. ***Counterterrorism Intelligence, Open-Source Intelligence Techniques and Cyber Defense:*** The value of collecting open-source intelligence or other forms of intelligence about possible cyber threats cannot be underestimated. To tackle terrorism, it is important to collect, gather, exchange and share intelligence from the public, businesses, social media, law enforcement, and government agencies.

i. ***Public and Private Partnership:*** The active and dynamic participation of the public and private sector is a key component in countering cybercrime. Public-private engagement is important in different forms while addressing awareness raising, training, technological improvement and advancements, vulnerability remediation and recovery operations. For example, public and private partnership with internet and social media providers should be improved.

i. ***International Collaboration:*** Terrorism is an international problem that requires a coordinated and cooperative international response. The purpose of strengthening partnerships in countering terrorism is through signing multilateral agreements and mutual information exchange practices.

i. ***Advocacy and Public Awareness:*** With public awareness raising, the public will be more educated about possible radicalization or propaganda messages, or cyber threats through tailored education programs on the responsible use of the internet and the societal impact of cyberterrorism.

Capacity building is an important approach to countering cybercrime by responding to needs, combined with increased cooperation to create an immediate impact. These can be achieved through cybercrime investigation, forensic examination of digital evidence, cybercrime assessment exercises, educational campaigns, and promotion and development of best practices on cybercrime.

- **Digital Forensic investigation:**

To effectively investigate cyber-enabled crime requires new knowledge and skills to be acquired by the investigation team within the law enforcement agencies, through developing cybercrime investigation expertise within the unit dealing with digital evidence.

- **Forensic Examination of Digital Evidence:**

Digital evidence forensic examination is a key component in the investigation and prosecution of cyber-related crimes, especially terrorism cases. This process requires trained personnel because digital evidence is fragile and can easily be tampered. For this a specialized training programme in digital forensic for police officers through regional workshops, bilateral meeting and equipping units with digital forensic tools, is necessary.

- **Cyberterrorism Assessment Exercises:**

Regular practical assessment exercises in the form of cybersecurity trainings or boot camps to assess and evaluate the capabilities of law enforcement agencies and other stakeholders in dealing with terrorists' use of the internet. This is an effective way in countering cybercrime at international and regional levels through information sharing, investigation and capacity building. Also, through regional mentoring programmes, which enables the law enforcement officers learn in a country with well-established capabilities, learning from their experience and the ability to implement relevant best practices.

- **Educational Campaigns:**

Educational campaigns targeting diverse groups in the society will be important in raising awareness on counterterrorism issues and the measures required to protect the entire cyber ecosystem.

- **Promoting and Developing Best Practices on Counterterrorism:**

By encouraging service and internet providers to adopt best practices aimed at promoting secure online behavior throughout the wider community, and the distribution and development of low cost tools to help businesses to prevent and detect online threats.

Finally, combatting cybercrime is a shared responsibility and requires a broad range of stakeholders and law enforcement to successfully prosecute such cases through capacity building to improve law enforcement capability and enhance the criminal justice framework.

Funded by the Kingdom of Norway through its annual voluntary contribution to UNODC Regional Office for Eastern Africa and its Countering Transnational Organised Crime, Illicit Trafficking and Terrorism Programmes.

UNODC: United Nations Office on Drugs and Crime, Regional Office for Eastern Africa; UN Gigiri Complex, Block X; PO Box 30218, 00100 Nairobi, Kenya; Tel.: (+254-20) 762-3739; Fax: (+254-20) 762-3667; Email: unodc-easternafrica@un.org; www.unodc.org/easternafrica.