ISSN 2348-3156 (Print)
International Journal of Social Science and Humanities Research ISSN 2348-3164 (online)
Vol. 7, Issue 3, pp: (179-190), Month: July - September 2019, Available at: www.researchpublish.com

The Effectiveness of Technology in Curbing Terrorism

[1]Nasha Learamo, [2]Doreen Omitto, [3]Professor Weldon Ng'eno Kwa

Emails: nlearamo@gmail.com, doreenomitto@gmail.com, ngenokwa@gmail.com

Abstract: **This paper examines the effectiveness of technology in curbing terrorism. It highlights the trends in terrorism from 1998 to 2019 in order to understand this more. The study argues that counter-terrorism efforts are partly focused on combating terrorism using developments in technology. It highlights success stories in responding to terrorism from Kenya, the U.S and New Zealand.**

Terrorists are increasingly adapting to new technologies therefore increasing the impact and the scope of their attacks. To curb these attacks, counterterrorism measures have therefore had to incorporate new technologies. Security forces have experienced challenges in adapting to new technologies to prevent future attacks. Nonetheless, when these technologies have been adapted, they have proven effective.

1. INTRODUCTION

Due to the evolving nature of terrorism, counterterrorism measures have had to frequently change. Additionally, advances in technology have changed the nature of attacks by extremists hence increasing the impact of their attacks and security forces have had to adopt to this. The extent to which the technology deployed to curb terrorism is effective, is however not focused on as compared to the role.

1.1. Background

Terrorism is a concept that is frequently evolving and lacks a standard definition. Terrorism involves targeting civilians in a violent manner in order to achieve a purpose that is political. Difficulty in defining the term comes about in its complex nature, with questions on whether extremism and incitement should be defined as terrorism. For example, with extremism, different groups will tend to have different ideologies (Ward, 2018). The evolving nature of terrorism has required that authorities use various methods to combat terrorism. One of these ways has been through adapting and advancing technology to tackle the crime.

Technology is defined as 'a*ny application of organized technical knowledge about the natural world for a practical purpose, or the capacity to develop and use such knowledge.*' This can range from space technologies, biotechnology or simple ones like latrines and cocaine (Weiss, 2015). Technology can also be defined as '*the application of science and innovation'* (Cornish, 2010).

Following the Second World War, the United States (U.S) began one of the first initiatives on science and technology which was sponsored by the state. This was successful seeing several other nations follow to get more developed (Committee on Science and Technology for Countering Terrorism, 2002).

Other than facilitating sectors such as trade and technology, science and technology has also greatly contributed to national security policies. Countries which invest in science and technology are more likely to protect themselves better from threats as opposed to those that do not (Committee on Science and Technology for Countering Terrorism, 2002).

This paper highlights the importance of using technology in curbing terrorism by looking at trends in this area in countries that have successfully incorporated these strategies. It also identifies existing gaps and challenges in experienced by governments in attempting to counter-terrorism and radicalization and why they have increasingly had to adopt new technologies to aid in these measures.

2. PROBLEM STATEMENT

Following the September 11th, 2001 attacks on the Twin Towers in New York, the National Academy of Sciences in the United States identified the crucial role that technology was likely to play with regards to curbing terrorism. With science and technology being used to respond to various things that could affect both human and state security, it acknowledged that new threats required a need for technical solutions to be quickly deployed in order to enhance security (National Research Council of the National Academies, 2002).

The National Academy additionally identified the field of Science, Technology, Engineering and Mathematics as historically having importance in war with regards to its effectiveness in responding to and mobilizing threats (National Research Council of the National Academies, 2002).

Terrorists themselves have significantly relied on technology to be able to carry out attacks. Three types of technology have been identified as being important to terrorist groups, these include: weapons technology, transport technology and communication technology. With regards to counterterrorism efforts, technology therefore plays and important role with regards to deter and to defend. Counterterrorism also benefits more quickly to technology than terrorist groups (Ghosh, Prelas, Viswanath, & Loyalka, 2009).

Several studies have been done on the role and types of technology used in counterterrorism but their effectiveness is not explicit. There has however been a decrease in the number of terrorist attacks with their intensity however seeming to increase (Institute for Economics and Peace, 2018).

3. METHODOLOGY

This paper researches on the effectiveness of technology in curbing terrorist attacks. It looks into the problem of the evolving nature of terrorism and technologies and how these technologies have been adapted in order to curb terrorism using qualitative methods. The paper will therefore involve studying reports, journal articles and other secondary sources that have been written on technology and counterterrorism. In addition to this, it will look at policies by counterterrorism task forces that incorporate the use of technology in bodies such as the United Nations as well as NATO. Due to lack of studies on the effectiveness of technology in curbing terrorism, the study will look at how the United States and Kenya have adapted technology in order to curb terrorism so as to determine the effectiveness. It will also look at the efforts taken by the New Zealand government to deal with the aftermath of the Christchurch attacks with regards to communications technology. Our concluding remarks will therefore be based on our findings.

4. TRENDS IN TERRORISM FROM 1998 TO 2019 IN DEVELOPED AND DEVELOPING STATES

The United States was initially a target for terrorists with their embassies in Kenya and Tanzania being attacked by extremists in 1998, followed by the New York, Twin Tower attacks in September 2001 (Institute for Economics and Peace, 2018). Allies of the country continue to be targeted but terrorist trends are constantly changing with a rise in domestic attacks by various extremist groups such as nationalists of far-right supporters. This highlights the importance of protecting critical infrastructure using technology as they remain targets by terrorist groups today.

Other key targets by terrorist groups have included commercial planes, pipelines with natural gas, power grids that transmit electricity, oil rigs which are found offshore as well as cyber or information communications elements which have crucial government or corporate records (Wardlaw, 2002). This shows that terrorist targets are focused towards harming as many people as possible.

From 2007 to 2011, there was an increase in terror attacks being reported worldwide. Between 2011 and 2014, terrorist incidents increased as well as the number of casualties. This was facilitated by the Arab Spring which occurred during the period and the emergence of groups like the Islamic State (ISIS) (Institute for Economics and Peace, 2018). This therefore showed the need for technology to enhance intelligence gathering even in developing states or states affected by conflict in order to reduce the number of attacks.

After 2014, terrorist incidents have significantly reduced especially in Nigeria and Iraq where Boko Haram and ISIS are the dominant groups respectively. This has been attributed to better counterterrorism strategies globally as well as improvement in political stability. Additionally, the number of foiled terrorist attacks has also increased showing improvement in counterterrorism strategies. This trend has been observed in countries affected by conflict and those that are not but the decrease in attacks has mostly been in non-conflict states (Institute for Economics & Peace, 2018). Adaptation of technology has continued to play a crucial role in counterterrorism through aspects like using social media analysis as well as data mining.

Despite this decrease in terrorist incidents, the intensity of the attacks has increased meaning that attacks are becoming more fatal with more casualties and in some instance's destruction of property. In 2017, 67 countries experienced at least one death as a result of terrorism compared to 79 counties in 2016 hence showing a decrease (Institute for Economics and Peace, 2018).

An increased impact of terrorism was however experienced in Africa in 2017 with the Middle East, North Africa and Sub Saharan Africa being the most affected areas (Institute for Economics & Peace, 2018). This is therefore indicative of terrorist groups being able to facilitate their attacks through improved tactics and perhaps technology by making more powerful improvised explosive devices (IEDs) or having access to arms. In addition, it also shows that countries in developing areas lack the same capacity to develop and enhance counterterrorism measures as compared to developed states.

With regards to the types of attacks, bombings account for most attacks with conflict states being affected as opposed to non-conflict states. Attacks involving assaults are the second most common types of terrorist attacks (Institute for Economics and Peace, 2018). This is perhaps due to the ability of extremists to access technologies that aid them in making these weapons.

Taking of hostages and assassinations increased from 2012 to 2017 (Institute for Economics and Peace, 2018). According to Warldaw (2012), taking of hostages, especially in attacks, tends to increase tension. There have however been instances where these hostages have been jeopardized by media who air live images during attacks that the terrorists get access to. There have also been instances where these images are shared by the hostages themselves which may in turn compromise their own safety.

Attacks on infrastructure also increased between 2012 and 2017. In the U.S for example, attacks on infrastructure increased among animal rights as well as environmentalist groups who also carry out attacks that can be classified as terrorism though emerging trends such as environmental terrorism (Institute for Economics & Peace, 2018).

In addition, there has been a noted increase in deaths caused by far-right groups from 2014 to 2017 (Institute for Economics & Peace, 2018). The Global Terrorism Report gives relevant insight in the trends in terrorism between 2014 and 2017. A shortcoming of the report is that it mainly focuses on terrorist attacks carried out by religious groups while leaving out other forms of armed violence. Far right groups seem to have access to better technologies as they are rarely flagged and if so, there is lack of follow up even when prior surveillance has been done. They therefore can more actively use the internet and depending on laws of a country, it may be easier for them to purchase arms or items needed in making Improvised Explosive Devices.

With regards to technology, enablers in this field that facilitate terrorism have barely been studied. Communications and computing technologies have however enhanced radicalization of individuals that wish to join terrorist groups through technologies such as encryption, private networks and the ability to access internet. Islamic State (IS) has especially benefitted from these technological advancements enabling them to carry out attacks that can be conducted by anyone anywhere with little preparation (Harrison, n.d.). Cheaper transport costs and advancements in the transport sector have also facilitated terrorism (Coates, 2016). Technology can also facilitate terrorist financing by elements such as using cryptocurrencies (Carroll & Windle, 2018), use of biological, nuclear, radiological or other chemical weapons that will enable these groups to carry out their attacks (National Research Council of the National Academies, 2002)

5. COUNTERTERRORISM MEASURES

The Cambridge English Dictionary (n.d.) defines counter-terrorism as '*action intended to prevent violence for political purposes*. The United Nations recognizes the evolving nature of terrorism and its capability to destroy political order and stability. Additionally, the United Nations also advocates for a single approach to dealing with terrorism (United Nations, 2018). There seems to be a lack of consensus regarding a unified approach to counterterrorism.

With regards to countering terrorism, the United Nations has emphasized that there is a need to collaborate with non-state actors such as those in the private sector. Access to information in a timely manner is critical in preventing terrorist attacks. This can be done through gathering intelligence, getting biometric data, passenger information and financial information. There is therefore the need to share information globally, nationally and locally but there is lack of trust between states. This then makes them reluctant to cooperate. In addition to this, there is need for more emphasis on the nexus between organized crime and terrorism (United Nations, 2018). Technology is a crucial aspect in facilitating this. Countries that are more developed with regards to technology can prevent terrorist attacks more quickly than those that are not. Wardlaw (2002), also highlighted the need for advancements in technology in countervailing as well as the defection of attacks by terrorist groups despite noting that this might interfere with human liberty.

6. COMBATING TERRORISM USING TECHNOLOGY

Terrorists have used technology to their advantage from radicalization, to recruitment to training and even to perpetrating attacks this has led to technology platforms to struggle between the balance of freedom of speech and privacy while working on curbing terrorism (Yan, 2017). Groups such as ISIS and Hamas are using the internet to spread their propaganda since it is easily accessible, has a vast reach and is affordable. In addition to recruitment, financing and spreading propaganda, the internet enables terrorists to gather information, get false documents, communicate more effectively, distribute software they have developed, know how to make weapons and to train new recruits (Jenkins, 2018). For terrorist and counter terrorist operations technology is central therefore it's an important incentive for the groups to master new techniques.

Naik (2009) points out that as much as human intelligence is relied on heavily by law enforcement to curb terrorism, technology will greatly help to detect, analyze and even eliminate terror attacks early. For example, the United States has been able to effectively stop terror attacks similar to the 9/11 attack by using technology to effectively monitorthreats through legislation and airport security. Interpol, for example, used technology to identify the Glasgow 2007 airport attack. Interpol's information sharing database has also been identified as a crucial breakthrough in helping states curb terrorist attacks (United Nations, 2018).

The UN Counter Terrorism Unit started an initiative with Facebook, Twitter, Microsoft and Google which came up with a new tool which uses machine learning to search and remove terrorism content online (Yan, 2017). Cyberspace being an environment without boundaries that terror groups can use to spread propaganda and social media being the modern platform for terrorists, there has been increased number of websites containing terrorist materials since 1998 where there were only 12 websites as compared to 2003 where there were 2,650 websites online , in 2015 the number increased to 9,800 (Jenkins, 2018). Cellebrite, a worldwide leader in digital intelligence, has come up with innovations that can unlock, extract, decode and analyze data from multiple sources which can enable investigators to curb attacks as well as arrest terrorists and their accomplices (Watson, 2019). However, through encryption and Virtual Private Sectors as well as the ability of terrorists to develop their software, pulling down terrorist content from various online sources still proves to be challenging.

Terrorist groups have also been quick to adapt new technologies hence newly emerging issues such drone terrorism. Drones are flexible in terms of their size and weight and are easy to use hence the alleged adaptation by terrorist groups such as Hezbollah and Islamic State. This is a worry as they may be used in attacks by dropping explosives as drone development continues to advance. Additionally, they may also be used by terrorist groups to survey areas that they want to attack (World Economic Forum; RAND Corporation, 2018). It is however difficult to use drones in states that have restrictions on their use, but they are easier to use in conflict prone areas.

To counter terrorism using technology the United Nations suggested 1) the implementation of resolutions 1373 (2001), 1624 (2005), and 2178(2014) which look at technology and terrorism 2) self-regulation in the technology industry, 3) strengthening of legal assistance when it comes to digital content and 4) countering messaging techniques including on online platforms (United Nations, n.d.). There is need to adopt these policies in local contexts in addition to further research on how effective these methods can be.

Noting the use of technology by terrorists, in 2001, the United Nations passed Resolution 1373, asking member states to facilitate exchange of information on how terrorists are using technology. In 2005, Resolution 1625 was passed to ensure that such measures would be under international law so that counter-terrorism efforts prevented the use of technology by terrorist groups. Human rights should also be protected while this is being done (United Nations, n.d.). This is because privacy rights and freedom of speech as well as press can be violated while this information is being looked for.

New technologies enable one to collect data in a more advanced manner, but it remains limited. Advancements in internet technology has enabled intelligence agencies to be able to collect data that was previously unavailable (Kilroy, 2017). A shortcoming with this is sometimes this technology is developed after an attack is carried out hence the need to study terror groups and their methodologies in order to develop technology that can help mitigate the effects of such attacks.

Data such as through emails or phone conversations, can be collected at any point as they are being transmitted. With smartphones, data can basically be collected and analyzed by phone companies. This is because the internet is not a secure communication tool, but it is instead meant to facilitate communication (Kilroy, 2017). A worry with this is that privacy rights of individuals may be violated, and data protection regulations may be broken which is a violation of human rights. It is however important to ask if this ought to be allowed if it means citizens are being protected despite their rights being violated.

The internet as a result has both negative and positive consequences. This ability to access data has enabled criminals such as terrorists to be kept off the internet. Governments therefore have a core role in accessing this data with limited regulations which ought to be introduced according to some people (Kilroy, 2017). The question however arises with regards to what extent these regulations can be limited.

Advancements in technology have also enabled security authorities to be able to track communications that have been encrypted by terrorist groups. The setback with this is that training individuals to track terrorists down via the internet tends to take time. Private companies developed tools that enhance digital intelligence via facilitating analysis and viewing of large amounts of data, extracting data from machines or technology that had been destroyed and quickly identifying images and videos related to terrorism and other forms of organized crime (Watson, 2018).

Additionally, with critical infrastructure being a core target for terrorists, Muggah (2018) adds that some cities are experimenting with innovative approaches of curbing crime and countering terrorism .These cities are known to deploy agile security which has a problem oriented approach and data driven .What the most successful cities have done to improve security is they have improved on intelligence gathering as well as policing and community outreach. For example, Paris' government started a 3D scanning programme for all public and private buildings. This program was meant for security forces to neutralize siege attacks easily. Protection of cities and their infrastructure remain crucial, as they are among the core targets for terrorist groups. Adaptation of technology has facilitated this.

Organizations such as NATO are also heavily investing in technologies that will help tackle terrorism. These include the development of technologies such as robots and computers to help detect explosives and radioactive materials (North Atlantic Treaty Organization, 2018).

With regards, to protection of airspaces against weapons such as missiles and Rocket Propelled Grenades (RPGs), NATO is looking into combining both technological and non-technological means such as training pilots to be able to avoid airspace attacks. Technologies that were being used to protect military planes are also being researched on to see if they can be used to protect civilian planes. In addition to this, the organization is also working on facilitating surveillance (Billingslea, 2004).

Technology plays a big role in curbing terrorism. Prediction software has been on the rise, a behavioural analysis tool known as Dfuze is used by over forty countries. In the United Kingdom during the 2012 Olympics it was used to identify high risk areas, this enabled the London Police to increase security in the identified areas. This software was also used to investigate the Boston 2013 bombing. The software stores data of all the attacks that have happened before. Governments are then able to access this data and analyze, predict terror threats or attacks as well as share information making the war on terror easy (Hooijdank, 2016).

The National Security Agency (NSA) Director in the wake of the Snowden leaks cited the number of terror attacks that have been prevented because of surveillance program as 54. Drones that are fitted with cameras for videos and still pictures have helped greatly to curb Al Qaeda organization and activities on the Pakistan-Afghanistan border. Surveillance programs are not only helping in curbing terrorism, but the program is helping keep countries safe and saving lives this then proves that technology is effective in curbing terrorism (Cayford & Pieters, 2018).

A shortcoming of the use of technology in combating terrorism is that a number of measures are yet to be implemented as they take time. It is however clear that technology plays a crucial role in counterterrorism measures especially as terrorists continue to adapt new technologies.

There have also been calls to incorporate other areas rather than technology such as behavioural science research which also includes the use of technology by enhancing data collection and analysis among attacks as well as perpetrators to be able to determine future trends. Behavioural science should also include development of technologies or facilitating the use of existing technologies in counter-terrorism efforts such as weapon detection as well as screening (Wardlaw, 2002).

To determine how effective technology has been in curbing terrorism, the paper is going to look at how security forces have incorporated technology with regards to fighting different terror groups.

6.1 USE OF TECHNOLOGY IN CURBING TERRORISM: SUCCESS STORIES FROM THE U.S, KENYA AND NEW ZEALAND

6.1.1 Use of Technology After the 9/11 Attacks: A Case Study of the United States

Several changes occurred in the U.S after the 9/11 attacks, internationally, several other changes were also observed. This included enhanced security in airports. Prior to the attacks it was difficult to identify things such as explosives and other weapons. Mitigation has been made possible through things like installing full body scans. There was an improvement in scanning systems after their failure which had resulted in the attacks (Freedman, 2011).

After the September 2001 attacks, the PARTIOT Act was introduced allowing intelligence agencies to adopt technology that would help prevent future terror attacks. This included using technology that would enhance things such as tapping wires, to be able to collect large amounts of data among other things such as being able to listen to international communications without getting warrants (Kilroy, 2017).

Additionally, data mining improved after the attack. This involves going through large amounts of data and analyzing it to know the likelihood of an attack. Social media was initially the main source of getting this data. Data by terrorist organizations was posted on different social media sites in several languages (Freedman, 2011).

Video surveillance also improved following the 9/11 attacks in a bid to track suspicious behaviour as well as to help in getting evidence. Surveillance however has a shortcoming as security forces cannot pick out criminals based on behaviour (Udice, 2018).

Due to availability of limited data on terrorist groups, a global database was developed to input data on terrorist attacks to help predict and mitigate attacks. As years went by, this data became more reliable and additionally helped researchers to understand other factors related to terrorism such as those that were psychological (ASIS International, 2011). This has been crucial as there had been calls to include behavioural sciences in order to help curb terrorist attacks.

Additionally, partnerships were formed to help develop new technologies with international organizations such as NATO and other states such as the United Kingdom. DNA technology was also developed helping advance forensics so that victims of attacks could be identified more quickly (ASIS International, 2011).

Other changes included the creation of the Department of Homeland Security to enhance national security, securitization of terrorism leading to the intervention of the United States in Iraq and Afghanistan, increased deportation for non-citizens with criminal records and increased international reporting as most news stations focused on their home countries before the attacks (Udice, 2018). Additionally, tips from the public also aided in monitoring jihadists and terror suspects (Bergen, Ford, Sims, & Sterman, n.d.). Terrorist attacks related to Islamist extremists have reduced in the U.S since then.

Domestic terrorism incidents by far-right groups as well as left wing ideologists have however increased in the U.S with the country experiencing 65 terrorist related attacks in 2017 (Romero, 2018). Technology therefore needs to be incorporated to curb such attacks as they continue to rise and the use of technology has proven effective in curbing Islamist extremists.

6.1.2 Use of Technology in Curbing Al Shabaab Activity: The Case of Kenya

Al-Shabaab group is based in Somalia, it's a jihadist group that is affiliated to the al-Qaeda. Al-Shabaab poses a major threat to Kenya and the East African region. This then led to the Kenyan government to initiate measures to combat the threat posed by the group (Megged 2015).

The aftermath of 9/11 led to Kenya becoming a major partner in the Global War on Terror. This led Kenya to be a target of al-Qaeda affiliates because of its role on the Global War on Terror and the military invasion to Somalia in 2011.Prior to

9/11 counter terrorism units existed in Kenya both in law enforcement and security arenas although the United States attack intensified the role of counter terrorism in Kenya (Aronson, 2013).

Following the Embassy bombing in 1998, Kenya become a beneficiary of the US Terrorism Assistance (ATA) Program, the National Security Intelligence Service was also created. This then led to more than five hundred Kenya security officials being trained by the ATA and this resulted in the creation of the Kenya Anti-Terrorism Police Unit, National Security Advisory Committee and the Counter Terrorism Center (Aronson, 2015).

According to the Standard (2015) Kenya has succeeded in counter terrorism efforts because of the National Strategy to Countering Violent Extremism in 2016.The 2016 policy stated that terrorism was a threat to national security and that it is symptomatic to any other threats or insecurities that individuals within the country could be facing. The center for implementing the policy was the National Counter Terrorism Center which provided support to different government ministries, departments and agencies.

The Kenyan government initiated counterterrorism measures against the Al-Shabaab group by deploying the Anti-Terror Police Unit to the Kenya-Somalia border, the porous border then prompted the construction of a perimeter wall, budget allocation to the defense agencies was increased this then saw the birth of “Nyumba Kumi initiative” which promoted collective security. The government also went ahead to freeze bank accounts of Al-Shabaab sympathizers (Megged, 2015).

The holistic approach undertook by Kenya to counter terrorism saw hundreds of arrests and trials of suspected Al-Shabaab members although there are few that got acquitted and were freed for lack of evidence .The security agencies in the country have contained some attacks, for example in March, 2014 a major attack in Mombasa was contained, a vehicle borne improvised explosive device was intercepted. In September the same year Kenya security forces working jointly with Uganda security forces thwarted twin suicide bombers that were to be carried in Kampala and Nairobi. A plan to attack Gikomba Market in Nairobi was contained. In 2018, police intercepted a vehicle from Somalia which had explosives and suspected Al-Shabaab members hiding in a thicket in Isiolo county. During this period hundreds of radicalized youths attempting to move to Somalia were arrested (Standard Digital, 2018). This was facilitated by technology through tracking of phone records, despite the fact that this has not necessarily been explicit.

Internationally countries such as the U.S aiding Kenya, have resorted to airstrikes including the use of drones. The number of airstrikes has increased under Trump’s administration. The use of technologies such as drones has however been criticised as they are unable to differentiate between militants and civilians. Furthermore, the use of drones is secretive making it difficult to regulate (Felter, 2019).

These airstrikes have also included the use of bombs in additional to using ships that are armed hence strengthening the capability of the armed forces fighting against the group in Somalia (Ismay, 2019). This shows capacity of the military to adapt technology in the fight against terrorism.

The use of drones to fight armed terror groups in Somalia has however not been as successful as in the case of Yemen and Pakistan. Nonetheless they have had an impact with former Al-Shabaab leader Ahmed Godane being killed by a drone strike in 2014. However, Al-Shabaab has not been completely crippled by the drone and air strikes. Drones have been used concurrently by the U.S military with other weapons such as helicopters and missiles. Increased presence of the United States in Eastern Africa has made it easier for the country to deploy drones. Restrictions around drones have however become less fringent with Trump’s administration as compared to Obama’s (Hansen, 2019).

Other arms created to deal with terrorism in Kenya included the Cyber Forensic Disposal Unit and the Bomb Disposal Unit. The National Intelligence Service as well as the Kenya Defense forces also had their capacities strengthened in order to curb terrorism (The Conversation, 2019). These sectors depend on the incorporation of technology to be able to detect, deter and respond to terrorist attacks.

Progress to curb Al-Shabaab activity in Kenya has been slow but it has also improved over the years. For example, during the 2013 Westgate attacks, agencies failed to collaborate and during the Garissa Attack, response was similarly slow (The Conversation, 2018).

Comparing this with the Dusit D2 terror attack in 2019, the multi-agency response was faster and better managed. There were regulations on social media and surveillance footage seemed to have helped in identifying the assailants.

Additionally, intelligence agencies were able to track the activity of the assailants following the attack via technology such as following their M-Pesa as well as banking trails.

Unlike during the Westgate and Garissa University attacks, media coverage of the attack was also limited. Journalists lacked access to the buildings while security forces intervened. However, international newspaper 'New York Times' shared a few explicit photos of the scene which had been discouraged as it may have helped in spreading propaganda. However, the government did not ask the newspaper to pull down the graphic images.

There have been calls to limit the ability of media bodies to report during terrorist attacks as they may jeopardize operations by putting the lives of hostages or security forces at risk or even making terrorists know techniques the security forces will use. Additionally, coverage helps spread extremist propaganda and fear among the public members in addition to increasing pressure on those dealing with the incident. Limiting the press has however been seen as something that will interfere with press freedom as well as freedom of expression (Wardlaw, 2002).

Kenya has cooperated with the United States in the fight against terror being one of only six countries taking part in the Security Governance Initiative, this initiative trains security services on management, accountability, oversight and countering terrorism. Kenya has also cooperated with the United Kingdom, the British Army since 2015 have trained 1,000 military officers and police officer on disposal of improvised explosive devices (Counter Extremism Project, nd).

The use of technology in Kenya to curb terrorism has been effective but this has been facilitated by partnerships will more developed countries and private telecommunication companies. Surveillance, media coverage, biometrics and data mining are areas in technology that have significantly improved since the Westgate and Garissa University Attacks. Response to terrorist attacks has also been much faster and better coordinated.

6.1.3. Far-Right Terrorist Groups and Technology: A Case of Christchurch Attack in New Zealand

A shooter attacked and killed 51 people in two separate mosques in Christchurch, New Zealand on 15th March 2019 (Kerdemelidis & Reid, 2019). According to the New Zealand Police, the shooter began by emailing the country's parliamentary security team his manifesto who in turn called the police (New Zealand Police, 2019). The shooter also shared this manifesto on other online platforms that have before been used by terrorist groups such as al Qaeda and ISIS (Tech against Terrorism, 2019).

While the police were being called, the terrorist had already begun shooting in one of the targeted Mosques and was doing a Facebook live stream as he shot and killed at innocent civilians (New Zealand Police, 2019). Once the terrorist shared the Facebook link, it was re-shared by viewers on several other sites while some newspapers from different parts of the world published his manifesto on their website (Tech against Terrorism, 2019).

The government attempted to calm the situation while working on the removal of the link that had been shared on Facebook and urging users not to share the images on other platforms such as Twitter and Youtube. By 16th March 2019, Facebook had removed 1.5 million videos of the attack and prevented users from uploading 1.2 million other clips. Other platforms such as Twitter and Youtube also removed videos of the attack that had been shared (Tech against Terrorism, 2019).

Smaller platforms such as Reddit took two days to remove the video while some had to be threatened with bans in order to remove the videos from their websites while a number acted responsibly by simply pulling down the video or the manifesto if they had been uploaded to their site (Tech against Terrorism, 2019).

Archived versions of the attack are however still available on some online platforms today with counter-terrorism specialists working on removing these versions (Tech against Terrorism, 2019). Following the incident, Facebook reviewed its streaming features and political leaders such as Teresa May urged technology companies to work together in order to curb terrorist content noting that the incident was a reminder that more needed to be done. In addition, she highlighted the negative use of technology to spread propaganda online (BBC, 2019).

The Prime Minister of New Zealand, Jacinda Ardern, and the President of France, Emmanuel Macron, also launched the Christ Church Call, urging governments and technology companies to work together in order to curb extremist content. They technology companies were also called upon to make the internet space safe by ensuring that human rights were observed on social media platforms (BBC, 2019).

The United States did not however join the Christ Church Call citing that freedom of speech had to be respect. It however mentioned that it respected the aims of the call and urged technology companies to deal with terrorist content (BBC, 2019).

Companies such as Microsoft, Twitter, Amazon, Facebook and Google committed to update their terms so that terrorist content would not be shared on their platforms noting the need for the technology industry in curbing the spread of terrorist content (BBC, 2019).

There have been questions on handling media with regards to counter-terrorism efforts and New Zealand set a good example on how to deal with various media platform during terrorist attacks so as to prevent further attacks of radicalization.

7. HOW EFFECTIVE IS TECHNOLOGY IN CURBING TERRORISM?

Technology is an effective method of curbing terrorism which has its shortcomings as well as its advantages. Several factors contribute to technology being an effective tool.

One limitation is that a country must have the financial capability and technical expertise to invest in technologies that will help in curbing terrorism. As a result, more developed countries such as the U.S and France quickly come up with technologies that enable them to complement other methods of curbing terrorism while developing countries must rely on assistance from these nations or private entities and regional organization which they belong to.

Technology is more effective when it is manufactured or located within the state that is affected by terrorism. For example, attacks by religious extremists have significantly reduced following measures such as improved surveillance following the 9/11 attacks. Nations like Kenya have struggled to catch up with improving surveillance systems, but relevant partnerships have ensured that this happens hence also leading to a decrease in attacks.

Technology is also more effective when information gathered is shared among nations as well as organizations as was with the example used by Australia and Israel in preventing attacks by terrorist group, ISIS. For example, member states of the United Nations' Global Counter-Terrorism Forum have noted that when the database by the International Police (INTERPOL) was integrated with national security systems, terrorists were more easily identified (United Nations, 2018).

Technology is tends to be effective if readily available to implemented immediately. An example is via removing graphic posts as was the case in the Christchurch New Zealand attack within a 24-hour period. However, there at times tends to be bias as was observed by the New York Times who refused to pull down graphic images of the Dusit D2 Riverside attack in Kenya despite their noted role in extremist which can have negative implications.

Additionally, technology is more effective when technology companies corporate with governments on countering the spread of terrorist content as noted by the United Nations' Global Counter-Terrorism Forum as well as the Christ Church Call. Lack of cooperation from technology companies hinder various counterterrorism measures despite their relevance.

According to Interpol, things that will likely affect policing in future include changes in the global divide, changing social divide, changing environment, workforce changes as well as changes in digitization and technology (Interpol, n.d.). It is therefore important to look at how these aspects can be incorporated when it comes to curbing crimes such as terrorism.

8. CONCLUSION

Technology is playing an ever-increasing role in curbing terrorism, but it also faces challenges such as limited funding, lack of expertise and taking time to develop or learn. The importance of technology in counterterrorism measures however continues to grow. Concerns are also raised as terrorist groups are quickly to able to adapt these technologies to facilitate attacks. The sector also has limited regulations hence the need to increase regulations as more innovations continue to come up.

Additionally, technology and terrorism is a broad area with several complexities that need to be studied together for more effective counterterrorism measures.

REFERENCES

[1] ASIS International. (2011). *How 9-11 has driven technology advancements*. Retrieved July 29, 2019, from Security Management: https://sm.asisonline.org/Pages/how-9-11-has-driven-technology-advancements-008650.aspx

[2] BBC. (2019, May 15). *Christchurch attacks: Facebook curbs Live feature*. Retrieved July 11, 2019, from BBC: https://www.bbc.com/news/technology-48276802

[3] BBC. (2019, May 15). *US says it will not join Christchurch Call against online terror*. Retrieved July 11, 2019, from BBC: https://www.bbc.com/news/technology-48288353

[4] Bergen, P., Ford, A., Sims, A., & Sterman, D. (n.d.). *Part IV: What is the threat to the United States Today?* Retrieved July 29, 2019, from New America: https://www.newamerica.org/in-depth/terrorism-in-america/what-threat-united-states-today/

[5] Billingslea, M. (2004). *Combating terrorism through technology*. Retrieved July 7, 2019, from North Atlantic Treaty Organization: https://www.nato.int/docu/review/2004/Interpreting-Istanbul/Combating-terrorism-technology/EN/

[6] Carroll, P., & Windle, J. (2018). Cyber as an enabler of terrorism financing, now and in the future. *Journal of Policing, Intelligence and Counter Terrorism*, *13*(3), 285-300. doi:https://doi.org/10.1080/18335330.2018.1506149

[7] Coates, J. F. (2016). A thriving future for terrorism. *Technological Forecasting and Social Change*, 76-78.

[8] Committee on Science and Technology for Countering Terrorism. (2002). *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism.* Washington DC: National Academies Press.

[9] Cornish, P. (2010). Technology, strategy and counterterrorism. *International Affairs*, 875-888. Retrieved from http://www.jstor.org/stable/40865000

[10] Directorate of Criminal Investigations. (n.d.). *Anti-Terrorism Police Unit (ATPU)*. Retrieved June 19, 2019, from Directorate of Criminal Investigations: http://www.cid.go.ke/index.php/sections/specilizedunits/atpu.html

[11] Doffman, Z. (2019, July 1). *Israeli cyber prevented Etihad Airline bombing and multiple ISIS attacks, PM says*. Retrieved July 9, 2019, from Forbes: https://www.forbes.com/sites/zakdoffman/2019/07/01/etihad-airline-bombing-and-multiple-isis-attacks-prevented-by-israeli-cyber-pm-says/#2248d0bfae29

[12] European Union. (2018, March 22). *How to stop terrorism: EU measures explained (infographic)*. Retrieved July 7, 2019, from European Parliament: http://www.europarl.europa.eu/news/en/headlines/security/20180316STO99922/how-to-stop-terrorism-eu-measures-explained-infographic

[13] Felter, C. (2019, April 3). *The controversy over U.S strikes in Somalia*. Retrieved June 19, 2019, from Council on Foreign Relations: https://www.cfr.org/article/controversy-over-us-strikes-somalia

[14] Freedman, D. H. (2011, September 9). *What has technology fixed since 9/11?* Retrieved June 10, 2019, from MIT Technology Review: https://www.technologyreview.com/s/425380/what-has-technology-fixed-since-911/

[15] Hansen, S. J. (2019, February 19). *Somalia drone strikes are a potent weapon, but not the game changer*. Retrieved June 19, 2019, from The Conversation: https://theconversation.com/somalia-drone-strikes-are-a-potent-weapon-but-not-the-game-changer-111845

[16] Hooijdonk, R. V. (2016, March 24). *Can Combat Terrorism with Technology ?* Retrieved from Richard Van Hooijdonk: https://www.richardvanhooijdonk.com/en/blog/can-combat-terrorism-technology/

[17] Harrison, S. (n.d.). *Evolving tech, evolving terror*. Retrieved July 24, 2019, from Center for Strategic and International Studies: https://www.csis.org/npfp/evolving-tech-evolving-terror

[18] INFOSEC. (2018, February 3). *The role of technology in modern terrorism*. Retrieved July 1, 2019, from INFOSEC: https://resources.infosecinstitute.com/the-role-of-technology-in-modern-terrorism/#gref

[19] Institute for Economics and Peace. (2018). *Terrorism index 2018: Measuring the impact of terrorism.* Sydney: Institute for Economics and Peace.

[20] International Institute for Strategic Studies. (2018, July 24). *Why we need a new strategy to tackle international terrorism*. Retrieved July 6, 2019, from World Economic Forum: https://www.weforum.org/agenda/2018/07/why-we-need-a-new-strategy-to-tackle-international-terrorism-69339dbe-8baf-41f9-a14d-553addbf1c88

[21] Ismay, J. (2019, March 27). *This new generation of weapons could mean more covert weapons around the world*. Retrieved June 19, 2019, from The New York Times Magazine: https://www.cfr.org/article/controversy-over-us-strikes-somalia

[22] Jenkins, B. (2018, February 3). *The Role of Technology in Modern Terrorism*. Retrieved from INFOSEC: https://resources.infosecinstitute.com/the-role-of-technology-in-modern-terrorism/#gref

[23] Kerdemelidis, M., & Reid, M. (2019, May 28). *Wellbeing recovery aftermass shootings: information for the response to the Christchurch mosque attacks 2019*. Retrieved July 9, 2019, from Cantebury District Health Board: https://www.cdhb.health.nz/wp-content/uploads/5fe3e197-rapid-literature-review-cdhb-response-christchurch-mosque-attacks-2019.pdf

[24] LaMorte, W. W. (2018, August 29). *Diffusion of Innovation Theory*. Retrieved July 27, 2019, from Behaviour Change Moders: http://sphweb.bumc.bu.edu/otlt/MPH-Modules/SB/BehavioralChangeTheories/BehavioralChangeTheories4.html

[25] Lister, C. (2019, March 18). *Trump says ISIS Is defeated. Reality says otherwise*. Retrieved July 7, 2019, from Politico Magazine: https://www.politico.com/magazine/story/2019/03/18/trump-isis-terrorists-defeated-foreign-policy-225816

[26] McCarthy, D. R. (2015). *Power, information technology and international relations theory*. London: Palgrave Macmillan.

[27] Megged, M. (2015, May 27). *Kenya Government Counter Terrorism Measures Against AL Shabaab Islamist*. Retrieved from Strategic Intelligence : https://intelligencebriefs.com/kenya-government-counter-terrorism-measures-against-al-shabaab-islamists/

[28] Muggah, R. (2018, June 15). *How Smart Tech Helps Cities Fight Terrorism*. Retrieved from World Economic Forum : https://www.weforum.org/agenda/2018/06/cities-crime-data-agile-security-robert-muggah/

[29] Naik, M. (2009, January 8). *How Technology Can Help Prevent Terror Attacks*. Retrieved July 16, 2019,a from India Today: https://www.indiatoday.in/declare-war-on-terror/story/how-technology-can-help-prevent-terror-attacks-36798-2009-01-08

[30] National Research Council of the National Academies. (2002). *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism*. Washington, BC: The National Academies Press.

[31] New Zealand Police. (2019). *Christchurch Mosque Shootings: Timeline of events 15 March 2019*. Retrieved July 11, 2019, from New Zealand Police: https://www.police.govt.nz/sites/default/files/publications/christchurch-shootings-timeline.pdf

[32] North Atlantic Treaty Organization. (2018, November 12). *New NATO scientific projects to help with the fight against terrorism*. Retrieved July 6, 2019, from North Atlantic Treaty Organization: https://www.nato.int/cps/en/natohq/news_160271.htm

[33] Pieters, M. C. (2018, March 8). The effectiveness of surveillance technology: What. *The Information Society*, pp. 88-103.

[34] Project, C. E. (n.d.). *Kenya: Extremism & Counter-Extremism*.

[35] Prunckun, H. (2011). A grounded theory of counterintelligence. *American Intelligence Journal*, 6-15.

[36] Romero, L. (2018, September 11). *Decades after 9/11, the American right is behind a terrorism surge*. Retrieved July 29, 2019, from Quartz: https://qz.com/1386318/9-11-anniversary-data-shows-us-terrorism-is-rising-on-the-right/

[37] Standard Digital. (2018, November 20). *Multi agency counter terror strategies bearing fruits, agencies argue*. Retrieved July 16, 2019, from Standard Digital: https://www.standardmedia.co.ke/article/2001303352/multi-agency-counter-terror-strategies-bearing-fruits-agencies-argue

[38] Starr-Deelen, D. G. (2028). *Counter-terrorism from the Obama administration to president Trump: Caught in the fait accompli war.* Cham: Palgarave Macmillan.

[39] Tech against Terrorism. (2019). *Analysis: New Zealand attack and the terrorist use of the internet*. Retrieved July 11, 2019, from Tech against Terrorism: https://www.techagainstterrorism.org/2019/03/26/analysis-new-zealand-attack-and-the-terrorist-use-of-the-internet/

[40] The Conversation. (2018, August 17). *How Kenya is managing security 20 years after the Nairobi blast*. Retrieved June 19, 2019, from The Conversation: https://theconversation.com/how-kenya-is-managing-security-20-years-after-the-nairobi-blast-101143

[41] Thompson, A. (2016, June 1). *Technology is crucial in the fight against terrorism.* Retrieved from Financial Times : https://www.ft.com/content/cc2f0052-eb70-11e5-bb79-2303682345c8

[42] Udice, K. (2018, September 10). *10 ways the world changed after the 9/11 attacks*. Retrieved June 10, 2019, from Insider: https://www.insider.com/world-changed-after-september-11-2018-9

[43] United Nations. (2018). *Report of the United Nations High-Level Conference on Counter-Terrorism.* New York: United Nations.

[44] United Nations. (n.d.). *Information and communication technologies*. Retrieved July 1, 2019, from Security Council Counter-Terrorism Committee: https://www.un.org/sc/ctc/focus-areas/information-and-communication-technologies/

[45] Ward, A. (2018, June 4). *How do you define terrorism?* Retrieved June 7, 2019, from The RAND Corporation: https://www.rand.org/blog/2018/06/how-do-you-define-terrorism.html

[46] Wardlaw, G. (2002). *Political terrorism: Theory, tactics and counter-measures.* Melbourne: Cambridge University Press.

[47] Watson, A. (2018, July 25). *The Ultimate Weapon in the Fight Against Terrorism, Digital Intelligence*. Retrieved July 2, 2019, from Cellebrite: https://www.cellebrite.com/en/blog/the-ultimate-weapon-in-the-fight-against-terrorism-digital-intelligence/

[48] World Economic Forum; RAND Corporation. (2018, August 20). *Drone terrorism is now a reality, and we need a plan to counter the threat*. Retrieved July 3, 2019, from World Economic Forum: https://www.weforum.org/agenda/2018/08/drone-terrorism-is-now-a-reality-and-we-need-a-plan-to-counter-the-threat/

[49] Yan, S. (2017, June 29). *Terrorist Use Tech to their Advantage but it is time to stop them UN expert Says.* Retrieved from CNBC: https://www.cnbc.com/2017/06/29/terrorists-use-tech-to-their-advantage-but-its-time-to-stop-them-un-expert-says.html