### Digitaliserade strider och deras inverkan på social hållbarhet i Kenya och Nigeria

**Sammanfattning**


**Nyckelord:** Afrika, digitalisering, digital transformation, strider, social hållbarhet, terrorism, al-Shabaab, Boko Haram, fredsbevarande, säkerhetsiserings, tyngdpunkt, cyberkrigföring, kryptovaluta, mörk webb, sociala medier
Roland Aszalós, Thesis report

Digitalised Combats and Their Impact on Social Sustainability in Kenya and Nigeria

Abstract

In our era, digital technology is one of the fastest-changing areas. It impacts our private life, well-being, economics, politics and warfare. This essay intends to answer how digital transformation affects combats and state and non-state actors and also how these digitalised combats compromise social sustainability. The findings include social media and online platforms, dark web and cyberterrorism, cryptocurrency, remote sensing and surveillance, machine learning and AI, and digitally enabled strategies. The analysis was done by the Centre of Gravity model, social sustainability and securitisation theory. The thesis follows a comparative case study approach about Kenya and Nigeria therefore the essay address al-Shabaab and Boko Haram as the two prominent terrorist groups and the empirical data are related specifically to these countries and these diasporas.

Keywords: Africa, digitalisation, digital transformation, combats, social sustainability, terrorism, al-Shabaab, Boko Haram, peacekeeping, securitisation, Centre of Gravity, cyber warfare, cryptocurrency, dark web, social media
# Contents

1. Introduction .................................................................................................................. 4  
   1.1. Literature Review ................................................................................................. 4  
   1.2. Research Problem and Research Questions ...................................................... 6  
2. Theoretical Framework ............................................................................................... 7  
3. Method .......................................................................................................................... 8  
   3.1. Limitations and Delimitations ........................................................................... 10  
4. Kenya and Nigeria ....................................................................................................... 12  
   4.1. Terrorism ............................................................................................................... 13  
5. Digitalisation in Africa ............................................................................................... 15  
6. Digitalised Combats .................................................................................................... 16  
   6.1. Social Media and Online Platforms .................................................................. 17  
   6.2. Dark Web and Cyberterrorism .......................................................................... 19  
   6.3. Cryptocurrency .................................................................................................... 20  
   6.4. Remote Sensing and Surveillance ..................................................................... 21  
   6.5. Machine Learning and AI .................................................................................. 22  
   6.6. Digitally Enabled Strategies ............................................................................. 23  
7. Discussion and Analysis ............................................................................................ 25  
   7.1. Centre of Gravity Model ..................................................................................... 25  
   7.2. Social Sustainability and Securitisation ............................................................. 30  
8. Conclusion ................................................................................................................... 32  
References ....................................................................................................................... 35  
Table of Figures ............................................................................................................... 37
1. Introduction

Africa is a continent that is well known for its developing countries, security issues, natural and humanitarian disasters and exploitation of natural resources but presumably less known for its development effort, prosperity, economy and visionary aspirations. There are many misconceptions about both faces of Africa, one could also ask if the continent is that far behind in development, and how it is possible to gather enough valid empirical data about events or even trace any impact of this diverse continent. Speaking from a European perspective there is far less knowledge built on Africa. This also means that more research is needed to address various African topics to reinforce knowledge and understanding about the continent and the impact of its issues. Representing only the raw image of the brutality of armed conflicts might raise awareness but does not bring an understanding of the situation behind the horrors.

Being the second largest and second most populous continent on the planet the importance from a global perspective, especially in natural resources, workforce and market is self-evident. Due to this importance, there is a growing interest from other nations, overseas actors and superpowers to utilise the possibilities of what Africa could offer. This interest strives for more research on specific topics about Africa to support investments, developments or commerce among other factors. Hence, there is a great number of reviews and reports from international organisations such as Interpol, the United Nations, and the International Committee of the Red Cross. Broadly, in the name of security knowledge, this essay addresses the combination of digital technologies with combat and warfare and their primary effect on social sustainability.

1.1. Literature Review

In the case of the issues of Africa, there are plenty of articles that address terrorist incidents and means of warfare, developmental challenges or the effect of globalisation but (based on the data collecting method of this thesis) fewer writings could be found about their interconnections or causal effects. Despite developed technologies such as drone warfare, advanced weapons and various identification methods, terrorist organisations are still resilient and still represent a threat. Due to the complexity of the question, fewer research papers offer solid answers on why are they still resilient to this advanced warfare and even fewer that address how the combats impact societies within their vicinity.

One of the most significant sources that were used for this thesis is the “Online African organized crime from the surface to the dark web” report from Interpol (2020). The scope of the review seeks to show the growing online criminal activity primarily on the dark web in connection
to Africa. The review follows an all-source intelligence analysis methodology with a regional approach. Data were drawn from available open and closed sources and presented how the different Organised Crime Groups active in Africa and how the internet fosters their illegal activities. Open sources embrace news articles, reports, international organisations and think tanks. The report also intended to support law enforcement strategies and cooperation among the five African regions and to show their dynamics. The report highlighted the growing impact of the internet and cyber-enabled crime on security and development. As long as socio-economic and security landscapes in Africa provide the opportunity, criminals will continue to take advantage of the Internet for their activities. For instance, the COVID-19 pandemic benefited criminals to exploit the crisis. Cyber-enabled crimes have increased due to the improvement of Internet coverage, the wide availability of cyber tools and the growing flexibility of cybercriminals. Criminals take advantage of online anonymity, and coding languages and with temporary tools they rarely leave a trace. The report shows the lack of investments in security measures and lack of public awareness as some of the main reasons that led to limited preventive capabilities. Cybercriminals will continue to exploit the web further for criminal gain (Interpol, 2020). Despite the report focusing on Organised Criminal Groups, the methods are still not just an important element of digital combats but in some instances the backbone of the adversaries’ tactics and thus also an important element of countermeasures.

The first and most significant finding indicates the importance of social media and online platforms or generally speaking the information technology that is available and daily used by each of us. This big role is also represented in this thesis based on various authors. Regarding al-Shabaab “Al-Shabaab and Social Media: A Double-Edged Sword” (Menkhaus, 2014) is one of the most detailed articles used. The article addresses the terrorist group’s activity mainly on Twitter and Facebook and the overall efficiency to build a brand by using media coverage. Al-Shabaab’s narrative and propaganda campaign increased due to online possibilities but as the goal shifted toward territorial combats social media became a primary tool for recruits and funds.

As for Boko Haram, “Information Technology as an Indispensable Security Tool: Nigeria’s Boko Haram Sect in Focus” (Chinda, et al., 2018) focuses on Information and Communications Technology (ICT) use. Social media is also amongst the most prominent findings in the article with great attention to ideology and global links and strategies influenced by ICT capabilities. The article suggests that the Nigerian government should solve its issues of corruption, and impunity and should strengthen accountability institutions furthermore stresses the importance of global synergy to counter online activities hence terrorist organisations forming alliances all over the world with other terrorist or criminal groups.
During the active years of the terrorist groups, there were many incidents yearly. The cases are helpful and could serve as the backbone of many analyses. In this thesis, there will be two cases mentioned to exemplify the importance and a milestone of social media usage. The two cases are the Westgate Mall attack in Kenya and the Chibok kidnapping in Nigeria. Due to the social media coverage, there are plenty of useful open sources as well in this thesis many authors (Jackson, et al., 2021; Muindi, 2020; Nthamburi, et al., 2018; Menkhaus, 2014) either mentioned or analysed these cases in their works.

1.2. Research Problem and Research Questions

Foremost, based on the aforementioned literature review it can be seen that the topic addresses relevant issues in this field of research and digitalisation indeed affects combats and actors directly and indirectly. There are common misconceptions and myths about African digital transformation and in some cases, the lack of knowledge raises more questions that need to be addressed. To create and develop strategies against online crimes or to increase counter-terrorism efforts it is inevitable to analyse the adversary and their capabilities compared to the defensive capabilities that are intended to mitigate the negative impacts. Nonetheless, there is a growing interest in the continent regarding overseas investments, technology transfers and international collaborations thus most of the research serves a more globalised effort to strengthen governments, development and security on the continent. This study intended to do a small case analysis that contributes to the understanding of the field of counter-terrorism and digitalised combats. Consequently, two research questions are stated and answered.

First, this thesis should trace the digital transformation within combats between state and non-state actors in Kenya and Nigeria. The emerging first question intended to deepen the knowledge about incidents and combats, precisely **how digital transformation and tools changed the warfare and strategies between the combatants**. Digital transformation can be traced by analysing the combats but also analysing the combatants thus the question also touches upon the actors and stakeholders meaning their perception of modern technologies’ role in combats. The answer to the twofold question should describe the impact of technology on the complexity of warfare in Kenya and Nigeria.

To further explain the importance of this topic and generally speaking the thesis, the second question looks into the sustainability aspects. Especially with systems thinking but simply with critical security studies terrorism and war are decisive factors in general welfare or development both in the short and long term. Thus, the second question asks **how and in what ways digitalised combats compromise social sustainability in Kenya and Nigeria**. This answer
should cover the issue of direct impacts with a narrow focus only on one aspect. This could also help to map the linkages between society and its vulnerabilities toward terrorist organisations in both diasporas.

2. Theoretical Framework

To gather and present the findings altogether, the Centre of Gravity model is used for the analysis from Strange & Iron (1996). The model consists of four main parts:

- **Centres of Gravity (CG)**
  - Description of physical or moral entities that can be considered as the primary components, representing strength, resistance and power. They are usually the leaders, specific military forces or even important infrastructures such as communication.

- **Critical Capabilities (CC)**
  - Description of the primary ability to destroy something, seize an objective or prevent from achieving a goal or mission. CG is described in a scenario, situation or mission accordingly capabilities variate.

- **Critical Requirements (CR)**
  - The required conditions, resources and means of war that are essential for a centre of gravity to achieve.

- **Critical Vulnerabilities (CV)**
  - Those components and capabilities of requirements that are vulnerable to neutralisation or defeat will contribute to a centre of gravity. Can be considered as significant weak points that offer tactical advantages if exploited.

The concept helps to explore the importance of digital technologies, means of warfare and the aims of both sides, it also allows to categorise the findings to spot the occurred differences and similarities. The Centre of Gravity design originates from Carl von Clausewitz and throughout history there were many different adoptions for instance in the Nazi-Germany it was called “schwerpunktbildung” and according to this operational design the armoured forces were put in the Centre of Gravity meanwhile in some other examples the line of communication could also be represented as the Centre of Gravity. At any given level or scenario of a war multiple CGs can exist and can be shifted thus Centres of Gravities can include a military force, an alliance or a set of critical capabilities and functions or even the national strategy. The model shows the relationship
between the Centre of Gravity and Critical Vulnerabilities thus they are not considered as individual elements (Strange & Iron, 1996).

The second phase is about social sustainability which can identify and specify positive and negative impacts on people or societies. The objectives are also blurred but among the overarching social concepts we can find public awareness, equity, participation and social cohesion (Hellberg, 2022). In a broader sense, it requires an overall resilience for human welfare meaning cultural needs, population growth, human health, clean environment or standards of living. These aspects have a direct impact on human well-being that should not be ignored thus digitalisation and combats, even separately, have a shaping force on the short- and long-term goals (Mohamed, et al., 2021).

To associate the findings with social sustainability, the securitisation theory will be used. The concept of sustainability and sustainable development can be considered as mixture of three pillars namely environmental, economic, and social (Purvis, et al., 2019). Since security is a speech act, social and intersubjective construction there are many different readings about this theory. This essay follows the logical explanation of normal, democratic policies in the realm of emergency politics in policy making. Securitisation will be used as an analysing tool to trace incidences, securitisation and political acts that are used to mitigate or counter the negative impacts that threaten society and security (Taureck, 2006). With this practical tool, the direct effect can be traced along with the countermeasures that can indicate long-term effects and addresses the answer to what securitisation and policy do to heal the compromised security.

These three theories were chosen to analyse both sides of digitalised combats. Since this paper has its limitations, a simple and flexible model was needed from military science. The Centre of Gravity model proved useful to address each question and was adjustable to the limitations and findings. It is a good framework for representing all the results in the same place while remaining transparent. Securitisation, as a concept is wide enough to narrow the scope into one segment. As for the backdrop findings should be consistent until the end because otherwise, it would have been challenging to draw clear conclusions. There is less consensus on the definitions of social sustainability and also many different descriptions of securitisation, therefore, previous clarification was needed. Securitisation, in this case, supports the understanding of digital combats in Kenya and Nigeria.

3. Method

Since the field of research within these topics is extremely broad to handle and to produce sound knowledge within a master thesis a comparative case study structure was chosen to narrow down the scope to two similar countries. In this way, digitalisation can be traced in similar situations but
in different conditions to draw consequences if some impacts are unique in a certain diaspora or not. For this approach, I followed mainly the guidelines from “The good research guide: research methods for small-scale social research projects” (Denscombe, 2021) and from UNICEF’s “Comparative Case Studies” (Goodrick, 2014). However, comparative case study approach could be used to compare the two countries this thesis does not analyse the countries themselves instead it grasps the phenomena and causal chains appearing in both countries. The challenges such as the need for extensive fieldwork and the complexity of cases were mitigated by delimitations and are carefully evaluated and analysed by the frameworks.

For the open-source data collection, the primary sources of knowledge are academic literature, research papers and podcasts while the thesis also used grey literature such as news sources and online articles. The relevant keywords were searched mainly on Google, Google Scholar and Anna Lindh Library. The findings were selected and sorted by their detailed information, reliability and relevance to the topic. Specific keywords were used to keep the focus on the main topic. The main keywords consisted of Africa, Kenya, Nigeria, terrorism, Boko Haram, al-Shabaab, digital transformation, securitisation, centre of gravity, social sustainability, cyber warfare, cryptocurrency, and social media.

The first figure below shows the brief logical structure of the report for the analysis. It was necessary to preserve transparency and also because the frameworks require different approaches.

![Logical structure](source: the author)

The first part could be called the setting because the findings do not exist in isolation, therefore, must be placed in the environment that needs to be stated and described. Thus, Chapter 4 describes the conditions in Kenya and Nigeria and introduces the main actors connected to the findings. Terrorism as a driving force must be addressed as well as the general concept of digital
transformation in Africa in Chapter 5. The empirical findings are presented in Chapter 6. Since the focus is on the two research questions every six elements of digitalised combats address not just the warfare but also the social aspects.

Chapter 7.1 is the analysis and discussion of the Centre of Gravity model which is based on the setting in which the findings take place and are affected by it. The model intended to show the linkages between actors, conditions and the elements of the digitalised combats. Chapter 7.2 analyses the social aspects but in this case, besides the setting and findings, the analysis uses the results and conclusions of the Centre of Gravity model too.

3.1. Limitations and Delimitations

Regarding my personal biases as the author this thesis is limited by a lack of personal first-hand and professional experiences of Africa. The possessed knowledge is based on personal interests and academic studies. Being a white European male, I cannot demonstrate first-hand experience on gender, racial or postcolonial issues of Kenya or Nigeria. Therefore, this thesis was written with a constructivist and qualitative approach prioritising motivations and understanding.

Although it was stated that there are useful empirical data about security issues, warfare, combats, and different organisations it is difficult to compare Kenya with Nigeria based only on the findings since these issues do not exist in isolation and might occur globally or at least continentally, the findings are not specifically about the two countries under study. Therefore, the analysis in some parts is based on a wider scope which also allows for better understanding. The empirical finding in most of the cases (with some exceptions for background information) should not be made before 2015 due to the relevancy to the main topic regarding digital technologies. This sector evolves at a really fast pace therefore most of the findings are outdated and thus irrelevant.

To successfully tackle the time limitation the study is solely based on open-source data. The collected material was evaluated and selected mainly by their level of description and perspective. Many findings addressed the same topics sometimes from different angles. At the end of the selection the more detailed topics were chosen that are represented the research from a perspective that can be related to this essay.

To address social sustainability and trace the impact of digitalised combats the study is focused only on the most prominent compromising effects. This way the answer should describe the main causal issue excluding the minor ones and those that have insufficient empirical data.

As for the shortcomings, there were more data found and collected on the cyber domain rather than the physical combats. From the side of different armed forces, it is clear that the defence sector, regardless of the nation, strives for more developed technologies such as drones or
automated weapons to increase the capability even against terrorist organisations in terms of surveillance and detection but less or no findings about the adversary’s advanced physical capabilities. On the contrary social media is deeply described from the perspective of crime organisations but less information about the countermeasures that are used to mitigate the impact on the other hand many articles raise awareness and stress more collaborative efforts.

Regarding the theories, both three should be useful for in-depth analysis but the individual application might not be sufficient to address serious, broad questions and issues. In this essay securitisation was used to address social sustainability on the surface level consequently this thesis does not intend to go into depth arguments regarding social security, policies, politics or theory-based considerations.
4. Kenya and Nigeria

At first glance, one might say that the only prominent similarity between the two countries is that they are situated in Africa. Despite these countries representing the eastern and western sides of the continent, there are lots of similarities. The first table compares Kenya and Nigeria by their index numbers supported by Global Positive Peace Reports, Global Terrorism Reports, and Global Peace Reports from the past 7 years. The values are based on the representative reports and the interactive maps from the Vision of Humanity website (Anon., 2022). These indexes are produced by the Institute for Economics & Peace and data were gathered from respected sources such as Terrorism Tracker. Through various qualitative and quantitative indicators indexes cover 99.7% of the world’s population. The table shows that both countries scored relatively the same place in Global Peace Index which measures the overall peacefulness by 23 indicators such as “internal conflicts fought, weapons export, terrorist activity,
They also have similar results in Global Positive Peace which is defined by the level of societal resilience and includes aspects like corruption or the free flow of information among others. These two indexes are weighted from 1 to 5. Regarding the third factor the Global Terrorism Index, both countries scored high but since this index consists of incidents, fatalities, injuries and hostages it is seen that Nigeria faces a bigger challenge in counterterrorism than Kenya but also indicates the ways of Boko Haram and al-Shabaab. There are influencing factors regarding the population and the size of the countries but also the fact that al-Shabaab is operating from Somalia meanwhile Boko Haram is in the northern part of Nigeria.

As for the actors, there are the Kenyan and Nigerian governments, their armed forces and security forces with law enforcement. In the close vicinity, we can find the neighbouring countries which have strategic importance. In a wider scope, the overseas actors consist mainly of the superpowers and the EU among other nations. Besides the countries, there are several international organisations like the United Nations, the International Red Cross and Red Crescent, the African Union, and Interpol. Both countries must deal with and suffer from terrorism which is represented by the al-Shabaab in Kenya and Boko Haram in Nigeria. These extremist groups impact not just the government but the entire diaspora which compromises the interests of the overseas actors regarding their investments and from the ideological side a war against Western culture and Christianity. Terrorist organisations pose a major threat to development and society too by causing insecurity and involving, relying on the citizens, businesses, communication, and infrastructure as their assets.

### 4.1. Terrorism

As it was mentioned previously both countries are highly affected by the terrorist threat represented by the two extremist groups. The second figure shows the severity of incidents by different Islamist groups in Africa. Since the main aim of this essay is to analyse the digitalised combats, it is important to state some basic background knowledge that helps to understand the aims because digital technologies are also tools to achieve certain goals.
Both of them are considered jihadist extremist groups whose aim is a theocratic rule under Islamic law which includes and according to their ideology killing infidels and the ideology of takfirism (advocates the killing of Muslims declared as disbelievers) are appropriate punishments. Since their agenda is to overthrow the current government, factors such as poverty, weak state and corruption are important assets for terrorists and building their strategies on those. In Kenya and Nigeria, nearly half of the population live below the poverty line.

Besides the societal aspects, the physical conditions ensure to hide and operate as they want. Ungoverned spaces and remote areas are good environments for cross-border crimes such as smuggling or illegal arms trade. The question for counter interventions is not an easy one since the groups are rooted in the socio-economic and political spheres, and merely policies and political will are inadequate to tackle the problem. For the governments to successfully step up against terrorists the use of military force or criminal law measures are not enough on their own because the groups prefer border regions, strong international cooperation is needed from the region including neighbouring states and international actors, and organisations (Babatunde, et al., 2021).
Boko Haram was formed in 2002 as an anti-corruption group but after the execution of its founder, Mohammed Yusuf in 2009, the group became violent and deadly by carrying out several attacks against schools, churches, state entities, and security forces. According to their strong belief, radical ideology, and the meaning of the name “Boko Haram”, western education is forbidden in every sense from basic culture to science and should be punished. The group today is an international terrorist organisation operating mainly from Nigeria, Benin Republic, Chad, Cameroon and Niger and has strong connections and allegiances with other Islamic groups around the world (Fineman, 2018; Babatunde, et al., 2021). Boko Haram primarily uses high-calibre-precision weapons and IEDs but also impacts the economy. To undermine the government, the group is trying to paralyse businesses, and companies and increase the security threat. In the media, among the latest incidents, kidnapping was the most significant type of attack against primary and secondary schools which represents a grave danger to the education system.

As for al-Shabaab, the group also tries to eliminate all foreign influence, Western culture and Christianity from Somalia but Kenya also became a primary target due to its military intervention. Besides Kenya, the group also expanded to Uganda, Djibouti and Ethiopia. According to their campaign, they are highly effective in recruitment and gathering revenues which is shown by the tough resilience that the group shows by steadily increasing its followers. Due to the access to the Indian Ocean and therefore to the trade routes, al-Shabaab represents danger by piracy and in return from Kenya’s perspective, the country’s strategic position is determined by the greater Horn of Africa and also by the Indian Ocean as the two main theatre (Babatunde, et al., 2021). In 2012 the KDF was able to end al-Shabaab’s financial position in Kismayo which meant an annual $25 million in revenue for the group by trade taxes and illegal transportation (Anderson & McKnight, 2014). The port shows the terrorist group’s economic strengths and the importance of some counter-terrorist operations in the area.

5. Digitalisation in Africa

The concept of digital transformation is a well-known term in our language such as the industrial revolution. But it is worth being aware of the steps of each phase of the industrial revolution because nowadays in most countries, technologies are helping to reach the “Industry 4.0” what we have not yet achieved. To grasp the essence of digitalised combats and to take away some misconceptions about Africa it is worth knowing the meaning of these milestones.

Industry 4.0 originates from Germany meanwhile in the United States it is known as “Connected Enterprise” or in Japan as “Society 4.0”. All these terms refer to an economic, and scientific transformation as a consequence of major industrial changes in society. While the first
and second milestones are well known from history books regarding the 18th and 19th centuries, the third step was the era of personal computers and the world wide web. The fourth milestone is characterised by technological innovations like cloud computing, bio- and nanotechnology or artificial intelligence (Daud, et al., 2020). The extensive use of cyber-physical systems allows economies to evolve within all sectors creating smart factories, AI-driven automation and storing a large amount of data to analyse or process cost-efficiently (IBM, n.d.). Many of the new digital structures require proper defence meaning cybersecurity which can be interlinked with insecurity and can be a driving force to foreign technology inflow. Private investors are keen on profitability therefore investments are decided upon if they are worth it or not and this creates opportunities for multinational cooperation as well (Uma & Ikpe, 2016). Developmental objectives are shaped by societies, and local and worldwide challenges such as pandemics. During and after COVID-19 the need for technology increased significantly with many positive impacts. It can ease inequalities, and differences in social groups, genders, language and age but also remains a double-edged sword because of global capitalism, developing countries are mostly consumers or passive receptors, it can increase inequalities, discrimination and have environmental and social consequences. Technology can be seen as a representation of power and technological inequality between developing and developed countries which allows a few to control many (Alzouma, 2005). Overseas nations such as China or the United States are quite dubious in terms of privacy, data management and surveillance by international firms (Daniels, et al., 2020). The growing interest in technology does not mean an immediate solution. A tool cannot solve long-lasting problems but, as it is usually said, in good hands it can make positive changes. Even with the proper use, it takes time and younger generations need to adapt and get those technical skills that will be essential in the future to eliminate the technology gap and to build technological capability in Africa (Alzouma, 2005).

6. Digitalised Combats

In this thesis, the concept of digitalised combat or warfare consists of means and methods of conventional warfare alongside digital tools and cyberwarfare capabilities to cause harm and to protect. Combats in the sense of digitalisation do not mean cyber terrorism, cyber warfare, cybercrime or hacktivism, still, the elements and methods are adopted as cyber-enabled incidents. Combats in this paper are handled as a phenomenon in Kenya and Nigeria that consists mainly of terrorist incidents but embrace criminal behaviours in the digital domain and cyber-enabled crimes regardless of their connections to terrorist groups or other criminal organisations active in these countries.
As it was discussed technology is a two-edged sword because it also represents new vulnerabilities. Having more complex systems the number of black boxes and linkages is also increased. The vulnerability can scale from small incidents like hacking a phone to large attacks on power grids or transportation systems. Crime and terrorist organisations now are enabled to carry out distant attacks, eliminate physical borders in communication and gain new kinds of weapons to wage a different kind of warfare. On the other hand, counterterrorism aims to tackle criminals to access developed weapon technologies and increase the cyber robustness of affected countries by adopting new technologies of Industry 4.0 (Daud, et al., 2020).

The findings in this thesis confirm that the combats expanded into the cyber domain. This study will present social media and online platforms, cryptocurrencies, the dark web, remote sensing and surveillance, machine learning and AI, and digitally enabled strategies. Evil is not an invisible force, it leaves traces, and it can be followed. The logical flow behind these elements is an imaginary way from the surface web to the countermeasures. The last aspects intended to describe the new theoretical strategies and plans for the future including major and minor technologies.

6.1. Social Media and Online Platforms

Starting with the most prominent aspect, social media and online platforms are probably the first channels that we use to keep in contact with our friends, read news from various agencies, watch relaxing videos or simply go on a date. It sounds not just pleasant, but normal and might feel safe, but as we outsource most of our life to the online world, we willingly lower our shields and give away many details of our habits, hobbies and interest among many other things. Since most of those are publicly available by anyone that is the first place where we, as individuals could be targeted and later victimised. Vulnerabilities do not result in actual attacks but can be exploited at any time and criminals, including terrorists have a wide repertoire of tools and are skilful enough to cause harm.

The narrative behind the global jihad against Western culture legitimates attacks as natural self-defence acts. With these attacks, they want to catch the attention of anyone who sympathises with their movements or their ideology. Because fundraising and recruits are always needed, they spread their extremist messages on online platforms. For example, on YouTube, al-Shabaab was very active in creating jihadi rap songs as a hidden calling or creating videos to encode messages (Menkhaus, 2014). Similarly, Boko Haram also exploited the use of online platforms by uploading videos but their scope was limited to local media outlets. Later as the popularity of the internet grew Boko Haram created more videos in multiple languages like Hausa, Kanuri, Arabic and
English. After its allegiance with ISIS, its propaganda greatly developed in quality and content (Jackson, et al., 2021).

In spite of that anyone could upload anything, online platforms constantly upgraded their policies and became more aware of new content thus al-Shabaab decided to post more videos on multiple websites at the same time. With the mass communication al-Shabaab and Boko Haram achieved worldwide competence by weaponizing the information, proclaiming its ideology, war, and beliefs influencing state and non-state actors (Menkhaus, 2014).

Mass media communication has its advantage for Africa like BBC or CNN amongst many other news sources they can broadcast several issues globally like in cases with Syria, Yemen, Ethiopia or recently Sudan. During the COVID-19 pandemic, the civil population preferred to access information through online channels to gather more personal and reliable information. But the wide selection also means that we can choose which news source we want to listen to. In the era of hate speech, mis- and disinformation we have to be careful who to believe (Demeyere, et al., 2020). Usually, we do not know who is behind some opinions that we sympathise with.

Terrorist organisations are familiar with online platforms and online tools such as messaging applications or Voice over Internet Protocol (VoIP). The primary use of these is to lure, recruit, blackmail, advertise and many other things within social engineering. Taking one step further, through hacking, our manipulated search engines can lead us to cloned websites or worse. This shows that criminals have not just strong computer skills but also strong interpersonal skills (Interpol, 2020). In short, social media is used to bypass the middleman and directly communicate with the terrorist on the other side (Ogunlana, 2019). As individuals, we can be found through social media but we can also find them for example through religious guidance (Nthamburi, et al., 2018). Once individuals sympathise with the ideology, they can look for other materials regarding the virtual jihad like videogames where the “hero” is a holy warrior whose aim is to kill the enemies of Islam (Ogunlana, 2019).

The true power of social media can be traced by two significant events which are the Westgate Mall attack in Kenya and the Chibok Kidnapping in Nigeria. In both cases, social media was in the middle of the events. The 2013 Westgate Mall attack in Nairobi with seventy-one dead people was characterised by massive media coverage by domestic and international agencies and also social media coverage by citizens and terrorists. This prove a major challenge to government officials by heavy critics from civilians who claimed that domestic news agencies were incompetent together with security units. Losing credibility also favoured al-Shabaab which was seen as more believable. The case highlighted issues in counterterrorism, lack of in-depth reporting by news agencies, flaws in governmental strategies, and the importance of social media in Kenya (Muindi,
2020). Similarly in Nigeria but with a different case, the kidnapping of 276 Chibok schoolgirls in 2014 was almost directly streamed by Boko Haram and draw wide international attention. Media and communication were always important for militarisation but also important to undermine the efforts of governments. The Twitter campaign #BringBackOurGirls challenged Nigeria’s strategy but the aftermath of the incident caused significant changes. The government realised that young generations should be informed and supported through social media and during but also after the case a counter-campaign was started by posting successful raids and highlighting counterterrorism efforts (Jackson, et al., 2021).

Terrorists can reach people that they did not before meanwhile avoiding online surveillance by law enforcement. Nigeria and Kenya also spending large amounts of money to tackle terrorists in this new battleground and develop their strategies (Ogunlana, 2019) (Nthamburi, et al., 2018). Undoubtedly future challenges require further development of new technologies to gain and preserve technical superiority against terrorist organisations and to protect citizens who are mostly unaware of the constant gaze of lurking criminals on the surface web and below.

6.2. Dark Web and Cyberterrorism

On the internet, we can encounter many wicked and dangerous things and without proper protection, our channels can be easily compromised. The same goes for the dark web. A common misconception about its illegality is not entirely true. To raise awareness, similarly to the surface web, the dark web should be explored to look at the roots of digitalised combats and step down to these virtual trenches of the new battleground.

To distinguish the basics, the surface web is what we access immediately as soon as we have access to the internet. The deep web is the area that we can call the invisible web, where our standard search engines and methods are insufficient because we need specific URLs to find a website or data, otherwise, we cannot search at all, like a completely blank page. Now, between the two we have the dark web. It can be considered as a small part of the deep web but more like a hybrid area because the access is available for anyone and quite easy to use. As soon as we download a required browser and use an appropriate search engine, we can find many “hidden” things. The access is not illegal but trades and materials mostly are. The dark web as its name indicates is mostly unseen area by the public but even though governments and law enforcement are aware these online spaces cannot be regulated. To successfully victimise a person or a company, terrorists and criminals need legitimised tools on the surface web to gather necessary information about the target’s location, interests, contacts, images, social situation, personal taste, pedigree or to exploit
emotional vulnerabilities. That is also one of the reasons why online dating apps, phishing emails, and computer malware are widespread in Africa (Interpol, 2020).

Illegal businesses and attacks fall within the definition of cyberterrorism which is hard to define and usually depends on the person who defines it and the actor who is carrying it out. For this essay, the important aspect is that the countermeasures are counterterrorism responses (Ogunlana, 2019) which connect to digital combats. Regarding online crimes we can distinguish two types, cyber-enabled crimes (such as fraud or theft) and cybercrimes (such as attacks against information systems). On the new battleground, we can be victimised through cyber-enabled crimes mostly by phishing attacks for stealing but on a more sophisticated level organisations run their illegal businesses on the dark web like trafficking of stolen arts, drugs, diamonds or human beings. The first contact usually takes place on the surface web but later traces lead to the dark web sites where local and international buyers and sellers reach each other. The illegal dark web trades are an important backbone of finance, communication and the market like it was with the Silk Road which was shut down by the FBI in 2013 and continued to operate under different names until a new operation managed to shut down (Interpol, 2020).

Despite of the successful operations, the need is still high thus new sites will emerge. Like in conventional warfare, eliminating supply lines is a strategic objective here eliminating dark web sites could mean less capability of terrorist organisations and might decrease the severity of crimes from small robberies to piracy due to lack of firearms. Undoubtedly modern-day warfare requires knowledge to stop terrorism. The dark web enables us to evade censorship, control, surveillance and legal measurements. To catch, to monitor illegal trades we can always follow the way of money, even when they are in digital forms.

6.3. Cryptocurrency

Cryptocurrency is still a hot topic today since its start in 2009. Without going into the very details, for terrorism, the biggest advantage is the provided anonymity due to blockchain. Whatsoever the controversial fact is that these currencies do not provide full privacy, they are not entirely anonym. As in many cases on the internet anonymity depends on the user’s action so basically most of the personal information in a transaction can be stored, be traced back and deanonymized (Dyntu & Dykyj, 2021). Every data related to a transaction can be seen by anyone at any time.

As it became more popular and accessible it steadily spread across Africa. Regardless of crime organisations, cryptocurrency offered a decentralised currency that is unaffected by political changes and was a good way to tackle inflation for example in Kenya and also in Nigeria. The online valuta could even bypass certain embargos and geopolitical restrictions of a country.

20
its availability, individuals can enjoy its benefits, they only need an electronic device and internet connection. As we go further, startups and businesses favoured cryptocurrency to protect themselves from criminals and it was believed to solve developmental issues, increase economic growth and improve infrastructure (Interpol, 2020). Blockchain can even prevent data deletion, tampering and allow complete transparency for all data interactions (Jenny, et al., 2018). In good hands, it can help a lot of people like in a scenario where there is an urgent need for financial aid for people in need who are victims of wars or violence. With one simple procedure, millions of people could enjoy immediate aid (Demeyere, et al., 2020). If the trend goes on, more people have internet access and more people will be available through online transactions.

On the other hand, cryptocurrency poses a serious security threat, basically because of the same properties. On the dark web, this form of payment became the most popular. From the technical side, limited skills are required to use thus not only criminals can use it easily but individuals as well and, in this way, they were less aware of stealing and hacking. As being a grey area there are fewer policies and regulations (Interpol, 2020). For terrorists, it is a good way to run their online businesses and centralising or regulating cryptocurrency takes a lot of effort and time if ever going to happen.

6.4. Remote Sensing and Surveillance

Online activities do not completely invisible whatsoever most of the data are stored for long periods. Terrorists and criminal organisations also leave digital footprints on the internet. Online spaces, just like physical ones, can be monitored in real-time. Several ICT tools such as biometry, social network analysis, data mining, profiling, satellite imagery, geo-location and so on (Chinda, et al., 2018) can be used to track criminal behaviours.

As we already know, funding is essential for crime and terrorist organisations to exist. Thus, the primary aim of law enforcement is to investigate transactions but extensive work is needed. To gather intelligence, agencies require a centralised database that contains personal data and details which are used for identification. Although this process in developing countries can be more difficult because of unregistered births and lack of ID measures (Chinda, et al., 2018). Operations like PANGEA (Interpol, 2020) can manage to fight against online sales but more data means more possibilities to connect transactions to actual persons.

Communication channels such as phone calls have a long history of intelligence gathering, spying or eavesdropping. With digital technologies, most of the smart devices are suitable to spy on someone and this is true for terrorists and civilians. If our phone gets hacked by criminals, we can be sure that their phone can also be hacked, the difference is the awareness and time. A close
Watch from agencies allows more capable surveillance (Chinda, et al., 2018) to track someone either in digital or physical space by wearable devices.

Despite digital technology has increased surveillance, developing countries cannot enjoy all the benefits due to the lack of ICT infrastructure and many other factors. Surveillance cameras are helpful in rural areas. However, insurgents are situated in remote areas or attack villages in the countryside. Drone warfare on the other hand is another step forward because, with that, security forces can reach those areas that are too dangerous to approach physically (Daud, et al., 2020) (Odeniyi & Abdullahi, 2022). Many advanced tools can be mounted on drones from voice to facial recognition or if the aim is to eliminate or destroy, drone warfare offers many weapons to be used. There is also an eye in the sky or in this case a little bit above because satellite technology can detect criminal activities and monitor areas affected by conflicts. Movements, especially vehicles, generate noise. Besides mountable visual sensors, auditory and seismic sensors can detect (sometimes even classify) vehicles from a distance (Jenny, et al., 2018).

With the tools more data is generated and even if we cannot find solutions we can at least prepare and create early warning systems. For example, a Nigerian church managed to create an online system through which the community can be informed, assisted and alerted (Chinda, et al., 2018). Machine learning is extremely useful to handle big data and to further increase surveillance data should be processed much faster than humans do.

6.5. Machine Learning and AI

Human receptors and cognitive capabilities have their limitations. Outsourcing our senses and several tasks to machines proved as a good solution to enhance processes. Surveillance and tracking require a huge amount of centralised data to be processed and analysed. Machine Learning (ML) can and already does help in many ways.

With ML models and Big Data, security agencies can gain more insights. The overall purpose of collecting data is not just for identification but for prevention. With ML models such as random forest, classification models, and decision trees (Huamaní, et al., 2020) states can visualise future terrorist attacks. As data would be collected from real-life events, cases, historical progression, social media and so on, possible cyber threats could be detected as well. In the physical domain, according to research, the system could determine the probability of region and the type of attack. The probabilistic results were quite accurate between ~75%-90% (Huamaní, et al., 2020).

The main advantage of ML is to accomplish certain tasks with low or without human interactions (Jenny, et al., 2018). However, we humans represent the risk because of our biases.
regarding our existing racial, political or gender aspects. Even a smart system with more complexity can generate misleading or false results (Demeyere, et al., 2020).

The risk of biases with simple early warning systems might not be that important but on a national level for example when weapon systems are based on the same ML models the targeting systems might make mistakes to distinguish civilians from criminals based solely on their behaviour. However, if the aim is not to militarise this data and method, ML is pretty successful in detecting war crimes based on evidence and also uncovering fake videos or doctored evidence (Demeyere, et al., 2020).

AI systems and especially ChatGPT as a recent breakthrough are a big if not the biggest technological achievement in the history of mankind. Regarding combats, AI technology influences many branches on both sides. For the security forces, as was discussed, is highly useful to handle Big Data simply to process and keep track of certain activities and individuals but also for “nudging” to influence actors’ decision-making and behaviour in favour of freedom and peace (Sætra, 2019). But from the criminals’ side, they can create deep fake videos, manipulate and clone voices, increase coding capabilities, create better messages with large language models to increase propaganda and many more. Even our computer systems in front of us use visual feedback and mechanical inputs to allow us to give commands and maintain control. Without those the device still functions perfectly but for us humans it becomes a black box, something we cannot fully rely on. If we implement the same logic into data and information, if someone, somehow manipulates it in the digital domain we can only see the result, we cannot look further behind with our eyes and propaganda and manipulated news can distort our reality. As for digitalised combats in both countries propaganda and ideology were amongst the most significant factors next to social media and reliable news. If terrorists become more convincing and can exploit technology even further more harm could be done.

6.6. Digitally Enabled Strategies

Standard strategies are not sufficient to defeat the adversary in both physical and virtual domains. Digital technologies also have an impact on decision-making. This section discusses a rather theoretical approach of digital technologies in strategic considerations.

Regarding terrorist organisations, we cannot really discuss theories of decision-making or strategies in a classic sense, because first of all the assumptions are due to a lack of credible data and because of their hostility. Their aim is not to raise awareness and create a robust organisation they focus more on attacking and causing harm while remaining undetected. To achieve this, they are forced to reach out to as many resources and knowledge as they can. For instance, technology
Transfer in the case of al-Shabaab is very important. The early Improvised Explosive Devices (IEDs) of al-Shabaab were too simple but later as a result of an intense collaboration with Al-Qaeda in the Arabian Peninsula (AQAP) they became more developed. Bombs in trucks and laptops are also the results of the same collaboration thus it can be noted that the development of technology requires international connections for terrorist groups. Another tactic from al-Shabaab is to send warriors to other countries, preferably in conflict areas, from where, after their return, can increase their capability (Muibu & Nickels, 2017).

Through the local media, terrorists can have the opportunity to further exercise their fear tactics. As it was with the Chibok kidnapping, Boko Haram raised fear, and international alarm and tried to intimidate security agencies by showing off their capabilities. In the eyes of citizens, they aim to upkeep their mystery of appearing without any signs and disappearing suddenly like an unknown entity (Chinda, et al., 2018).

Technology alone is not a game changer; its successful implication is determined by many factors. As an example, there are many ways how to increase border control which can include surveillance, cybersecurity and other aspects. To successfully tackle the technology transfer and cross-border crimes of terrorist groups a border could use the most advanced technology but if placed in the wrong place it is simply useless.

Certain strategies and all government efforts are needed for proper funding and legislation. On the other hand, various industries and companies that represent telecommunication, bank systems, or economics, should be involved in the fight to form a synergy (Chinda, et al., 2018). Governments and neighbouring countries could have shared databases of IDs, registrations, accounts, biometrics and so on to identify criminal behaviour on a larger scale (Odeniyi & Abdullahi, 2022). Political will is undoubtedly important but also the infrastructure as a technical backbone which would be provided by other non-state or overseas actors. Without proper internet services and infrastructure for ICT, the fight in the digital sphere is difficult if not impossible. Shared trust is also needed between the actors and thus corruption and a weak state are poisonous.

Digital technologies also have a deep impact on psychological warfare with digital media and as was mentioned earlier, ideologies and religion are the essence of the war on terror. Religious representatives like Imams, and community leaders have the role to raise awareness for citizens within their community, and the same goes for journalism. Psychological warfare can be tackled by strengthening the awareness of citizens. Radio broadcasts are two-edged swords as well because those that are not owned by terrorist groups represent a threat to their ideology (Chinda, et al., 2018).
Within the cyber domain organisations need to build up a capacity to protect themselves and to aid people affected by armed conflicts (Jenny, et al., 2018). Cybercrime laws would strengthen the security of national information and data systems. Computerisation for government infrastructure is necessary to engage in digital combats (Chinda, et al., 2018). Government can decide upon shutting down entire mobile communication systems in states which for example in Nigeria in 2013 resulted in a successful operation against Boko Haram by luring them out from their hideouts to communicate and regroup. They were rid of their ability to use their explosive devices from a distance but also civilians were cut off from almost all sorts of communication (Chinda, et al., 2018). It was a solution but cannot be maintained for long thus other, more sophisticated methods are needed.

A more visionary effort, by the United States, is a smart army approach that would result in a robust, cloud-based structure, supported by AI, big data, and cybersecurity monitoring tools. This modernisation strategy would enable extended capabilities for armies to protect in the virtual domain (Anon., 2021). While this approach has its advantages, international peacekeepers have their concerns (United Nations Peacekeeping, 2021). With increased reliance on technology, their vulnerability is also increasing. In both cases, the strategy would ensure greater capability but optimised leadership is needed to continuously implement new technologies and consider digital transformation as an ongoing process that cannot be stopped. Decision-making should be supported by the constant cycle of training for capacity-building on technology (Hansen & Miyashita, 2021). Usually, criminals are ahead in terms of weaponization of digital technologies thus the first, most important step is to make the organisations robust and to ensure their own protection first.

7. Discussion and Analysis

The analysis will be focused on the Centre of Gravity separately first for the terrorist and criminal organisations and secondly for security forces, military and peacekeeping organisations. The second part addresses social sustainability and securitisation from a social science perspective.

7.1. Centre of Gravity Model

To answer the first question the Centre of Gravity model will address the digital transformation thus criminals and terrorists will be combined as actors with digital capabilities. The same logic will be followed in the case of security forces, military and peacekeeping organisations. In some cases, findings do not distinguish between criminals and terrorists and due to the international connections with criminal networks, the combats include the entire network. Mitigating attacks and
protecting, security forces on their own cannot represent a complete defensive effort. They work together and the strategy builds on collaboration between state and non-state actors hence in this model they will be represented as one force with digital capabilities similar to terrorist groups.

Table 2: Centre of Gravity model on terrorist and criminal groups (source: the author)

<table>
<thead>
<tr>
<th>Centre of Gravity (CG)</th>
<th>Critical Capabilities (CC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terrorists or criminals with digital skills and artefacts</td>
<td>Communication without physical limitations allows direct impact, technology transfer, and international allegiances.</td>
</tr>
<tr>
<td>(social media and online platforms, dark web and cyber capabilities, cryptocurrency,</td>
<td></td>
</tr>
<tr>
<td>AI, digitally enabled strategies).</td>
<td>Anonym attacks by distant attacks and cyber capabilities.</td>
</tr>
<tr>
<td></td>
<td>Can target almost anyone by stealing personal data.</td>
</tr>
<tr>
<td></td>
<td>Lethal terrorist acts for example with explosives, firearms or kidnapping.</td>
</tr>
<tr>
<td></td>
<td>Psychological warfare including fear tactics, ideology and religion.</td>
</tr>
<tr>
<td></td>
<td>Undermine and weaken state governments and national security efforts.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Critical Requirements (CR)</td>
<td>Critical Vulnerabilities (CV)</td>
</tr>
<tr>
<td>• Good skills in social engineering and the smart use of propaganda and ideology to</td>
<td>• If citizens are aware and able to protect themselves.</td>
</tr>
<tr>
<td>exploit social media for direct approach and eliminate the middleman.</td>
<td></td>
</tr>
<tr>
<td>• Extended use of the dark web to fundraise, trade and communicate.</td>
<td>International efforts can take out illegal sites slowing down the process or compromising the entire network.</td>
</tr>
<tr>
<td>• Familiarity with cryptocurrency.</td>
<td></td>
</tr>
<tr>
<td>• Remain undetectable by state identification methods.</td>
<td>If cryptocurrency is being regulated. Data of transactions are traced due to online monitoring.</td>
</tr>
<tr>
<td>• Get familiar with and use new technologies as soon as possible to gain an advantage.</td>
<td>Digital devices have IDs to detect and track.</td>
</tr>
<tr>
<td>AI can boost propaganda messages and digital capabilities.</td>
<td></td>
</tr>
<tr>
<td>• Rely on the weak state characteristics like corruption and use the weaknesses,</td>
<td>If AI and new technologies remain secured or monitored not to be misused.</td>
</tr>
<tr>
<td>vulnerabilities and weaponize information.</td>
<td></td>
</tr>
<tr>
<td>• Awareness of unmanned vehicle systems that can compromise hideouts.</td>
<td>If governments are more transparent in financial spending and inform citizens through</td>
</tr>
<tr>
<td></td>
<td>conventional news sources and social media.</td>
</tr>
<tr>
<td></td>
<td>If modern tactics are deployed on a larger scale with intensive pre-emptive strikes,</td>
</tr>
<tr>
<td></td>
<td>visual superiority, and neutralise capabilities.</td>
</tr>
</tbody>
</table>
Critical Capabilities shows that digital skills can support existing strategies and aims such as propaganda, funding or weakening the government. On the other hand, which is a relatively new trend is the focus on communication and distant capabilities. Isolation was a disadvantage for terrorist groups limiting their ability to effectively collaborate with other international organisations but digital technologies lifted these physical barriers. For instance, technology transfer is way easier to share knowledge. Communication has many channels and, like al-Shabaab, ideology and propaganda allow the worldwide branding of the organisation itself. Without borders, they can raise global attention which is important for their cause.

The Critical Requirements consequently prioritise digital skills. Exploiting new technologies as soon as possible requires early familiarity with the tools that criminals use for illegal businesses in this case the dark web and cryptocurrency are the most prominent examples. Even the illegal sites are taken down or cryptocurrency will be more regulated the early success and profit are already there with the increased criminal network. In the long term, a small window of opportunity is enough to enjoy its benefits. Terrorists are aware of the vulnerabilities but they can also rely on the lack of synergy between the actors and the weak state. Also, they have to make sure not to compromise their own hideouts or virtual actions. Hit-and-run tactics and guerrilla mentality can help to apply the same logic in cyberspace by evading monitoring and surveillance. On the surface web, they must be aware that illegal behaviour is rather suspicious than in other channels. They have to remain clear of any physical and virtual IDs including accounts and digital devices.

A direct approach through social media is vital for their activity. This capability demonstrates that they can reach almost anyone, they are active and this effort is represented well by recruitments from overseas countries. As was stated digital technology without skills and proper use means nothing and this indicates that both al-Shabaab and Boko Haram are quite strong in social engineering and interpersonal skills. This also explains why AI systems would boost terrorist organisations because they can have access to more advanced coding capabilities, and increase messaging and propaganda to support the virtual jihad. Hence, we are not in the same situation as a fighter of a terrorist organisation and the fact that they still demonstrate a high level of resilience it is really difficult to even predict how can such a technology be misused on a larger scale.

Seemingly digital technology did not change the goals or strategies of terrorists but undoubtedly changed their priorities and behaviour. Many vulnerabilities come from the fear of revealing their cover or implementing more policies to increase their isolation. They can tackle many of these aspects but even when they are one step ahead the technical superiority is in the hand of the security forces and can be achieved through international collaboration.
Table 3: Centre of Gravity model on security forces, military and peacekeeping organisations (source: the author)

<table>
<thead>
<tr>
<th>Centre of Gravity (CG)</th>
<th>Critical Capabilities (CC)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security forces, military, and peacekeeping organisations (social media and online platforms, cryptocurrency, remote sensing and digital surveillance, machine learning and AI, digitally enabled strategies).</td>
<td>• Eliminate terrorist leaders, destroy hideouts and lure terrorists out of remote areas.</td>
</tr>
<tr>
<td></td>
<td>• Strengthen democracy and governments.</td>
</tr>
<tr>
<td></td>
<td>• Gain the upper hand in cyberspace to detect illegal online behaviours.</td>
</tr>
<tr>
<td></td>
<td>• Protect citizens and aid victims of armed conflicts.</td>
</tr>
<tr>
<td></td>
<td>• Disrupt communication channels and criminal networks.</td>
</tr>
<tr>
<td></td>
<td>• Pre-emptive strikes in physical and virtual space.</td>
</tr>
<tr>
<td></td>
<td>• Counter messaging to raise local and global awareness.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Critical Requirements (CR)</th>
<th>Critical Vulnerabilities (CV)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Strong use of social media to inform citizens, raise awareness and mitigate false or disinformation.</td>
<td>• If somehow ideologies can be advertised legally or divide citizens.</td>
</tr>
<tr>
<td>• Use of cryptocurrency to send immediate financial aid to even millions of people.</td>
<td>• If cryptocurrency is not more protected against thefts.</td>
</tr>
<tr>
<td>• Laws and regulations against cybercrimes.</td>
<td>• If the system becomes corrupt.</td>
</tr>
<tr>
<td>• Centralised ID database and big data.</td>
<td>• If gathered data is useless against criminals or data cannot be shared between nations or data is mishandled.</td>
</tr>
<tr>
<td>• Effective deployment of remote sensor devices.</td>
<td>• If hideouts are too far away for effective use or cannot cover large remote areas.</td>
</tr>
<tr>
<td>• ML should be precise and used with care.</td>
<td>• Human biases remain in the system.</td>
</tr>
<tr>
<td>• Strong infrastructure for ICT tools.</td>
<td>• If nationwide coverage is not manageable.</td>
</tr>
<tr>
<td>• International collaboration in the area with neighbouring countries and also good synergy with state and non-state actors.</td>
<td>• Fragile contribution and collaboration in the long term.</td>
</tr>
<tr>
<td>• Effective use of unmanned vehicles.</td>
<td>• If somehow drones would be compromised during operation or still cannot penetrate hideouts.</td>
</tr>
<tr>
<td>• Funding for security measures.</td>
<td>• Corruption is still high.</td>
</tr>
<tr>
<td>• Continuous digital transformation.</td>
<td>• Terrorists are one step ahead.</td>
</tr>
</tbody>
</table>
In the case of defence, one of the main aims is to isolate terrorist groups by disturbing the communication channels and paralyse their movements both physically and virtually. If their capabilities could be curbed, terrorist organisations will be more predictable when they are lured out from hideouts. Another priority, to protect citizens is also changed because of the new battleground. The physical defence is not enough but it is almost impossible to protect everyone individually. The direct approach of terrorists created a situation where the citizens also have to be part of their protection in a similarly direct way. Thus, if we think about only the actual combats government and national efforts should be supported to mitigate the effects of the weak state but such negative aspects cannot be solved easily.

As for the requirements for countermeasures, especially military forces should adopt new technologies and develop not just their arsenal but also their strategies on how to use them effectively. Thinking of drone warfare with remote sensing, such operations require extended tactical considerations to seek and destroy. Creating a robust army like the smart army approach requires continuous transformation and cycles of training but also relying on technology comes with the need for better protection on all sides.

Terrorists are known to evade the gazing eyes of security forces but digital technologies offer new tools for monitoring. In case of every method that can be used to identify or follow online terrorism generate an enormous amount of data. Handling Big Data is beyond human capabilities but with the help of ML a system of shared information, a national ID system, international collaboration and cyber policies could form effective countermeasures to identify not just cross-border crimes and physical movements but also digital behaviours.

International collaboration is an important aspect to increase capability but also domestic state and non-state actors should agree on the same goals and efforts because without proper infrastructure ICT tools cannot be fully efficient. For digitalised combats, the all-government digital transformation framework is needed.

Social media also plays a significant role to gain trust and inform the citizens and also to raise awareness. Referring back to the involvement of citizens in defence strategy if security forces could make the population more resilient to online terrorism that would greatly mitigate the divisive impact of the organisations. This effort requires transparency of funding, reliable and in-depth news reports and counter campaigns where the government can highlight successful operations and their efforts.

To sum up, digitalisation created a new battleground where citizens are directly affected and should be involved to achieve a comprehensive national defence. Al-Shabaab and Boko Haram had some differences in their characteristics and methods but as technology evolved and
international communication boosted allegiances due to the technology flow terrorists shared many
tactics with other terrorist or criminal organisations thus the most prominent difference lies in their
lethality, economy and propaganda in terms of priorities and quality. As for the two countries, both
of them had to realise that they have to adapt to the new warfare and consequently to certain
terrorist incidents they started to exploit the possibilities offered by these new channels of
communication and mass media. They had different weaknesses and different government policies
but the counterterrorist measures nowadays, just as the terrorist methods, are getting more and
more similar due to international collaborations. Even with digital technologies security forces lack
the decisive capabilities to end wars in the short-term thus long-term efforts should rely not just
on the force but on how to create a safe online environment. As the saying goes you can kill a man
but cannot kill an idea is also true for terrorism because the idea or ideology of terrorism still
remains even when terrorists are defeated. If wars continue virtually, any physical victory would
mean less because these combats can live as long the ideology remains and the situation is the same
on the other hand because the online isolation could cause more severe and lethal attacks to
represent their strengths. Terrorist organisations realised that they have to win the people on social
media and that they also have to be aware of the new battleground. The different actors also realised
that these wars are not isolated from the world. The virtual jihad and terrorist allegiances show that
they stand by each other and the phenomena are the same in regards to the actors behind defence
forces and efforts. Globalisation and digitalisation together transformed these combats from a local
war into a global one where actors with interests are already involved regardless of distance.

7.2. Social Sustainability and Securitisation

The Centre of Gravity model and the findings stressed the role and importance of the local
population who are directly affected. To rely on and raise awareness of the population their
perspective and perception is also important for the long-term solutions. Social sustainability
includes many developmental aspects such as overall resilience, cultural needs, public awareness
and social cohesion (Hellberg, 2022). Terrorism affects all of them. Besides social media, the major
impact is represented by Boko Haram in terms of kidnappings and attacks against churches.
Religion plays a significant part in communities in Africa. Islamist extremist groups effectively use
religion to attract more people and the legitimised attacks can imply more fear in communities of
churches also their virtual jihad has the same effect by advertising their radical views openly.

Attacking schools have long-term effects. Kidnapping hundreds of children is not just
terrible for the victims and their parents but an important asset for recruitment, human trafficking,
slavery, blackmailing and many more. As a consequence, if schools become unavailable first of all
children will be left further behind in skills and if the state lacks skilful workers that can affect generations and slows down overall development efforts. Those children who wander the streets or just simply try to get work are highly vulnerable to terrorists (Chinda, et al., 2018). The promise of work even if it is illegal still a preferable choice over just searching for something that pays as well. Without education, young people can be controlled more easily and it is also good to belong somewhere, to friends, group or ideology. Terrorists can be seen as a welcoming community with common goals, similar to a brotherhood where children can find their purpose. With or without brainwashing, propaganda and ideology is not always about violent killing instead to convince and influence young minds that their effort is legitimised through religion or the will of the people.

Young people in rural areas and schools are also vulnerable to online platforms. Thinking about social media and dating applications a vast number of people experienced suspicious behaviours, swindlers or recruitment efforts. These platforms were created to start conversations and meet with unknown people. Online platforms became an organic part of the culture and are essential for young people to be active in the online world. The impact of combats can make this comfortable way of living uncomfortable and insecure. This is one of the main reasons why public awareness is a key aspect. In the case of online monitoring tools privacy is a key element because cryptocurrency has its advantage, personal data cannot be accessed legally and sharing data brings up the fear of misuse and distrust meanwhile on online platforms people willingly give their private data. The centralised database of accounts, biometrics or any other IDs could be a good countermeasure but undoubtedly expanded online capabilities for security forces would increase efficiency in more sectors.

We also have to highlight and address the concept of information itself. Westgate attack and the Chibok kidnapping showed that local and global media, news agencies, and journalists have important roles. Terrorists can also weaponize information spread misinformation, manipulate data, videos or recordings, confuse citizens and distort reality. In terms of democracy, freedom of speech, security and society, information can represent control. If terrorists are more credible during an attack that deeply undermines government efforts and their power. The Twitter campaign during the Chibok kidnapping also showed that information is mediated through different narratives and for governments, securitising information and social media should be considered. One of the primary channels of communication between the civilian population and the state government is through social media platforms. A weak state has many negative characteristics and these can be exploited by not just criminals but also citizens who are disappointed by the government. Emergency politics to mitigate security threats and the slow process of decision-making regarding policies means that many efforts can threaten some elements
within the state legislature system. To make real and effective changes all government efforts should be synced with civilian needs and with a shared understanding security issues can largely mitigate.

Digitalised combats indeed greatly impact social sustainability aspects. The accessed online information by citizens can be manipulated and changed by different narratives which in the end will not reflect reality. I would argue that certain securitisation efforts should be considered regarding information, social media and news sources but the movement is complicated. Securitisation does not necessarily a positive or negative act and greatly depends on the actors and other interests. As was stated in this report the overseas actors and especially the superpowers increase their influence on the continent which has an effect on power dimensions deeply rooted in colonial and post-colonial dependency (Fasakin, 2021). The marginalisation of African people occurs not just between the civilian and the government but also between African states and other powerful nations. War on terrorism and securitising certain aspects such as communication channels might increase the dependency and might be decided by overseas actors who have greater power over the region and the infrastructure. Otherwise even though securitisation would not be the solution, taking out certain aspects of communication and information from the normal political agenda might be a step forward to mitigate the effects of digital combats. Speaking of Africa, a continent is well known for its extremely diverse environment with various tribes, ethnicities, cultures, heritages and beliefs, social sustainability embraces many of these features that are represented by the society and if these features are compromised that affects not just individual factors but the entire social system. Seemingly young people are the true victims of these combats now and later. They are vulnerable to being recruited or victimised but later new generations will face other challenges as a consequence of a lack of skilled workforce, development and overall welfare.

8. Conclusion

As the report was narrowed down to two countries the comparative case study approach allowed us to pay attention only to the specific countries and with the keywords the open-source data were easily manageable. Since technology in general evolving at a fast pace some of the findings were partially outdated or even contradicting on some occasions. Due to the lack of digitalised aspects of the physical domain the Centre of Gravity model represents the virtual domain that made the compromising effects less traceable regarding social sustainability. The clear consequences can be seen after incidents such as kidnappings or armed assaults but for instance, in the case of online recruitment, the negative impact was not that well described or highlighted in the collected
empirical data. Besides the findings, the personal biases also made the analysis of social sustainability and securitisation more challenging due to the lack of personal experience so it was needed to remain objective and rely only on the empirical data rather than individuals’ own experiences and opinions. These difficulties could have been tackled with different methods and approach such as interviews on contradicting topics or in regard to sustainability topics.

In this essay, two research questions were stated. How digital transformation affects combats and state and non-state actors? And how digitalised combats compromise social sustainability? To find answers to the first question the Centre of Gravity model was used which described and correlated the centres of gravity with their vulnerabilities including capabilities and requirements. The model concluded the findings of digitalised combats such as social media and online platforms, dark web and cyberterrorism, cryptocurrency, remote sensing and surveillance, machine learning and AI, and digitally enabled strategies. The answer highlights the new, virtual battleground which just like the physical aspects is also an element of combats and digitalisation affects many existing strategies and goals and also created new ones. According to the findings, social media and online platforms as communication channels proved to be the most significant tools both for criminals and defence forces.

With the help of securitisation theory and the concept of social sustainability the answer to the second question indicates that combats that take place in cyberspace impact our private communication channels and this direct approach of citizens became part of the virtual jihad and global propaganda. Technologies that would make development processes more fluid and comfortable are compromised by these combats. Based on the findings young people are the main targets and while previously they were already in the centre now through online channels they can be targeted, influenced or victimised on a larger scale. Kidnappings and attacks against schools have a negative impact not just on the victims but in the long term for the upcoming generations if young people will lack required skills that are needed to find their places in the globalised environment in the future. As a way forward to mitigate the impact of digitalised combats, certain securitisation acts were discussed regarding communication channels and information. In summary, any securitisation acts would be ambiguous in terms of power dimensions, dependency and marginalisation.

In the case of the comparative case study structure Kenya and Nigeria were addressed by the findings and examples even though digitalisation and the phenomena became similar enough to consider the digitalised combats as one whole threat where countermeasures are also shared. Al-Shabaab and Boko Haram represented differences in terms of how they prioritise certain aspects
such as ideology, propaganda and violence. This essay did not go in-depth analysis of the findings and did not intend to further discuss securitisation.

As for the main takeaways digital transformation is needed and will be misused in many instances. Digital technology caused that communication is no longer limited by physical barriers thus international collaboration increased capabilities for both sides. Social media has the biggest role and the civilian population and governments should share awareness and trust. Other methods than the used ones could provide more understanding in the same or different areas and also securitisation is a useful theory for in-depth studies.

For further studies, AI systems, ChatGPT and large language models could be great topics to be analysed in the sense of militarization and security. As the importance of social media was stressed in this essay, it could be analysed further in the sense of democracy and future possibilities in control, awareness and limitations. Any research on these topics would increase global understanding and worldwide attention.
References


Interpol, 2020. *Online African organized crime from surface to dark web*, s.l.: INTERPOL.


### Table of Figures

**Figure 1**: Logical structure (source: the author)

**Figure 2**: Distribution of active militant Islamist groups in Africa (source: https://africacenter.org/infographics/)

**Table 1**: Global Index Numbers based on reports from "Vision of Humanity" website (source: the author)

**Table 2**: Centre of Gravity model on terrorist and criminal groups (source: the author)
Table 3: Centre of Gravity model on security forces, military and peacekeeping organisations
(source: the author)