KICTANet
The Power of Communities

www.kictanet.or.ke

Surveillance Laws and Technologies Used in Countering Terrorism and their Potential Impact on Civic Space

January
2024

In Partnership with

ARTICLE 19

HAKI AFRICA

CHRIPS
Centre for Human Rights and Policy Studies

Supported by:

Civic Futures

The Fund for Global Human Rights

Imprint

Published by:
Kenya ICT Action Network (KICTANet)
Email: info@kictanet.or.ke
Web: www.kictanet.or.ke
Twitter: @kictanet
Facebook: @kictanet
Instagram: @kictanet
LinkedIn: @KICTANet
Youtube: @kictanet8886
tiktok: @KICTANet

Lead Author: Victor Kapiyo
Co-Authors: Cherie Oyier and Francis Monyango
Editor: Dr. Grace Githaiga

Design & Layout:
Stanley K. Murage - stanmuus@gmail.com

Year of publication:
January 2024

Photo (Title):
www.freepik.com

Acknowledgements:

This research was supported by the Fund for Global Human Rights (FGHR) as a contribution to Civic Futures. Civic Futures is a philanthropic initiative co-founded by the Funders Initiative for Civil Society (FICS) and FGHR to enable collaboration between a wide range of funders and civil society to counter national security overreach harming civic space. https://civic-futures.org/

Table of Contents

Abbreviations

ACA	-	Anti-Counterfeit Agency
ACHPR	-	African Charter on Human and People's Rights
ATPU	-	Anti-Terrorism Police Unit
BTS	-	Base Transmission Station
CA	-	Communications Authority
CCTV	-	Closed-circuit Television
CIPIT	-	Centre for Intellectual Property and Information Technology Law
CORD	-	Coalition for Reform and Democracy
CT	-	Counter Terrorism
CVE	-	Countering Violent Extremism
DCI	-	Directorate of Criminal Investigations
DMI	-	Directorate of Military Intelligence
DMS	-	Device Management System
DNA	-	Deoxyribonucleic acid
DSS	-	Diplomatic Security Service
EAC	-	East African Community
EIR	-	Equipment Identity Register
GPS	-	Global Positioning System
GUI	-	Graphical User Interfaces
ICCPR	-	International Covenant on Civil and Political Rights
ICT	-	Information, Communications and Technology
IMSI	-	International Mobile Subscriber Identity
IPOA	-	Independent Policing Oversight Authority
IPSCSS	-	Integrated Public Safety Communication and Surveillance System
IS	-	Islamic State
JTTF	-	Joint Terrorism Task Force
KDF	-	Kenya Defence Forces
KeBS	-	Kenya Bureau of Standards

KFCB	-	Kenya Film Classification Board
KHRC	-	Kenya Human Rights Commission
KICA	-	Kenya Information and Communication Act
KIPI	-	Kenya Industrial Property Institute
KNCHR	-	Kenya National Commission on Human Rights
KRA	-	Kenya Revenue Authority
LTE	-	Long Term Evolution
MUHURI	-	Muslims for Human Rights
NCIC	-	National Cohesion and Integration Commission
NCTC	-	National Counter-Terrorism Centre
NIIMS	-	National Integrated Identity Management System
NIS	-	National Intelligence Service
NMS	-	Nairobi Metropolitan Services
NPS	-	National Police Service
NSA	-	National Security Agency
NSAC	-	National Security Advisory Committee
NSIS	-	National Security Intelligence Service
ODPC	-	Office of the Data Protection Commissioner
SLAA	-	Security Laws (Amendment) Act, 2014
UDHR	-	Universal Declaration of Human Rights
UK	-	United Kingdom
UN	-	United Nations
UPI	-	Universal Personal Identifier
UPR	-	Universal Periodic Review
US	-	United States

Executive Summary

This paper is part of a three-part research study by a panel convened by ARTICLE 19 Eastern Africa with the support of The Fund for Global Human Rights, constituted by HAKI Africa, The Kenya ICT Action Network (KICTANet) and The Centre for Human Rights and Policy Studies (CHRIPS), to carefully interrogate the impact of counter-terrorism (CT) and the prevention of violent extremism (PVE) and similar national security measures on civic space in Kenya to inform interventions that enhance greater accountability for violations and ensure an open civic space free from unjustified restrictions under the guise of security.

The three-part study constitutes:

Part I, titled:
Protecting Kenya's Civic Space in the Context of Securitised Responses to Terrorism and Violent Extremism' by CHRIPS which provides a deep dive into the historical context of civic space in Kenya and its evolution alongside Kenya's experience with terrorism and counter-terrorism efforts over the years.

Part II, titled:
Surveillance Laws and Technologies Used in Countering-Terrorism and their Potential Impact on Civic Space' by KICTANet provides insights on the role of digital technologies and tools used by the government in enhancing surveillance under the guise of security and their implication on civic space.

The paper includes an analysis of the applicable legal framework and case studies of the various tools and technologies that have been cause for concern for civil society actors.

Finally, Part III, titled:
'Perception Survey on the Impact of Prevention of Violent Extremism, Counter-Terrorism and National Security on Civic Space in Kenya' is a field study conducted by HAKI Africa, among civic space actors and human rights defenders in 8 counties; Bungoma, Isiolo, Kisumu, Kwale, Mandera, Mombasa, Nairobi and Nyeri seeking to assess their perceptions and/or knowledge of the existing CT architecture and its impact on civic space actors including from their lived experiences.

This study documents the use and misuse of digital laws, technologies and infrastructure to surveil civic actors, silence dissent, and restrict online civic space; review the role of key stakeholders; understand the potential use of digitised government services to restrict civic space; assess the impact of COVID-19 in surveillance; and identify the opportunities to disrupt, reform and transform the influence of security in the civic space.

The methodology included a desk review of various literature, including policies, laws, regulations, strategies, reports, analyses and technologies that impact Kenya's counter-terrorism efforts.

The key findings show that Kenya has in place elaborate measures, infrastructure and mechanisms to facilitate communication interception and surveillance that have a significant impact on civic space.

The study also notes that there are historical and systemic challenges in the manner in which security agencies operate and how civic space is treated that continue to bedevil the enjoyment of civil rights in the country.
Further, despite the existence of a robust constitution and commitments to international human rights standards, the erosion of civil rights continues unabated with limited oversight.

Whereas terrorism incidents were on the rise in the past decade, cyber and terrorism laws, including technical investments to facilitate communication interception and surveillance have created an environment for abuse to target activists, bloggers, journalists, and the political opposition.

Also, the study notes the role of enablers such as the implementation of mass data collection programmes such as National Integrated Identity Management System (Maisha Namba Digital ID programme), mandatory SIM card registration, national CCTV systems and other social media monitoring measures.

In conclusion, the study states that while ensuring national security, preventing terrorism and countering violent extremism are in the public interest, the response measures adopted should not come at the expense of fundamental rights and freedoms they seek to protect.

Therefore, it recommends that surveillance measures should be carefully calibrated, targeted, transparent, accountable, and implemented judiciously in line with constitutional edicts and international human rights standards.

More specifically, the study makes several key recommendations:

a) The government should put in place concerted and coordinated efforts to deal with root causes of radicalisation and terrorism in the country through intentional, integrated and human rights-respecting government policies that also target and address poverty, inequality and discrimination in access to resources and opportunities.

b) Parliament should review and reform Kenya's legal and institutional framework for surveillance including laws such as the Computer Misuse and Cybercrimes Act, Evidence Act, Mutual Legal Assistance Act, Prevention of Terrorism Act, and National Intelligence Service Act to ensure they are consistent with and implemented in line with constitutional and international human rights standards. Further that principles of transparency and accountability are embedded, guarantee, adequate and independent oversight mechanisms, provide redress mechanisms to victims, and are limited and proportional to control the state surveillance practices.

c) The Civil society should monitor, document and report on human rights violations by developing reports and research on the abuse of laws and incidents such as arbitrary arrests, detentions, torture and extra-judicial killings of human rights defenders arising from the application of surveillance laws and technologies in counter-terrorism operations.

d) Civil society should advocate and demand that the private sector tech companies comply with human rights standards, and expose the companies that are complicit in aiding and abetting unwarranted surveillance by selling equipment and services to government bodies.

e) The private sector such as operators of national telecommunication networks, mandate carriers, social media platforms and vendors of surveillance equipment to National Security Organs should comply with international human rights standards, including the United Nations Guiding Principles on Business and Human Rights and conduct due diligence to identify, disclose, and address their human rights impact, including within their businesses and supply chains.

f) The academia should research communication interception and surveillance to highlight gaps in existing surveillance and counter-terrorism laws and practices by security agencies, the extent to which they incorporate human rights principles, and their impact on civic space and make recommendations for policy reform.

g) The media should raise public awareness by conducting investigative reports, writing articles and opinion pieces covering human rights abuses by security agencies; the policies, laws and practices relating to communication interception and surveillance; and the impact of counter-terrorism and cyber laws on civic space.

1.0 Introduction

1.1 Civic Space in Kenya

Civic space is defined as "the environment that enables civil society to play a role in the political, economic and social life of our societies."[1] Further, civic space allows individuals and groups to contribute to policy-making that affects their lives, including accessing information, engaging in dialogue, expressing dissent or disagreement, and joining together to express their views.

To be effective, civic space should be an open and pluralistic environment that guarantees freedom of expression and opinion as well as freedom of assembly and association.

British colonisation had imposed upon most Kenyan communities violent restrictions on their freedoms of various forms. Civil society, the media and political organisations played a prominent role in the struggle for independence.[2] However, they faced violent repression as the colonial government sought to limit movements calling for the independence of the country.

The colonial government cracked down on political dissent including by arresting, torturing, killing and detaining at least 90,000 critics and persons associated with the Mau Mau rebellion during the state of emergency between 1952 and 1960.[3] It had also adopted the Kipande (national ID) system and the Public Order Act (1950), which severely restricted freedom of movement, assembly and association in a bid to prevent the spread of nationalist movements.

The colonial authorities strictly controlled the media by censoring news or banning publications and widely discriminated against Africans in various aspects of public life.

These tactics and approaches were largely retained by successive post-independence administrations since 1963. The work of civil society and the political opposition gained heightened prominence in the 1980s as the clamour for multi-party politics grew, culminating in the removal of Article 2(a) of the Constitution that allowed for a return to multi-party politics in 1991.

The end of KANU's 39 years in power ushered in the Kibaki administration in 2003 and saw a change in the relationship between the state and civil society.[4] The period witnessed the development of a civil society-driven constitutional reform process, which followed the impetus provided by the 2007-8 post-election violence, culminating in a new robust constitution in 2010, which provided strong safeguards for civic space.

The period also saw widespread reforms in the governance, justice, law and order sectors targeting the judiciary, police and security services.

However, the relationship between the state, civil society and the political opposition deteriorated

1. *What is civic space?* https://www.ohchr.org/en/civic-space
2. *Kenya* https://www.icnl.org/resources/civic-freedom-monitor/kenya
3. *The Colonisation of Kenya* https://www.blackhistorymonth.org.uk/article/section/african-history/the-colonisation-of-kenya/; *Britain's brutal rule in Kenya on the docks* https://www.aljazeera.com/features/2012/10/6/britains-brutal-rule-in-kenya-on-the-docks
4. *Kenya* https://www.icnl.org/resources/civic-freedom-monitor/kenya

in the run-up to the contested 2013 elections.[5] The succeeding period has seen various restrictions on civic space. Civil society reports[6] during the period show that the government has routinely disrupted peaceful assemblies such as public demonstrations and protests often with excessive force leading to the extra-judicial killing of protestors with limited investigation or action taken against security agencies.

This contributes to a culture of impunity within the agencies. For example, in the run-up to the 2017 elections, crackdowns by security agencies in opposition strongholds led to the death of more than 100 protestors and the sexual assault of dozens of women and girls.[7]

Further, there have been reports of state directives that undermine press freedom including physical attacks, intimidation or harassment of journalists and bloggers, restrictions of media from covering opposition parties and orders to minimise negative coverage of the ruling party especially concerning subjects such as corruption and security.[8]

Notably, officers from security agencies are rarely held to account for their actions, despite the existence of an oversight body Independent Policing Oversight Authority (IPOA).

Efforts have been made to restrict funding for civil society and a disinformation campaign orchestrated targeting human rights defenders and civil society who were branded as the "evil society" for their work in promoting human rights, democracy, and good governance.[9]

Restrictive laws such as the Non-Governmental Organisations Coordination Act (1990), Prevention of Terrorism Act (2012), the Computer Misuse and Cybercrimes Act (2018), the Penal Code and the Public Order Act (1950) have routinely been abused by authorities targeting political opponents, bloggers, civil society and protesters.

At least 60 bloggers were arrested in 2016 and the government attempted to deregister various civil society organisations, including the Kenya Human Rights Commission (KHRC).[10] In addition, there has been growing concern over the limitations of digital rights and the unchecked communication surveillance of human rights defenders by the National Intelligence Service, which continues with limited or no oversight.

Indeed, the 2022 CIVICUS 'People Power Under Attack Report' rated civic space in Kenya as 'obstructed'.[11] Despite a new government taking office in September 2022 with a pledge to deliver a new policing paradigm and police reforms,[12] the human rights violations have continued in earnest with authorities intensifying efforts to clamp down on opposition activities in 2023, with the president and senior officials from the ruling party appearing to commend and defend brutal crackdowns while denying any culpability of security agencies.[13]

5. *Defending Civic Space: Successful Resistance Against NGO Laws in Kenya and Kyrgyzstan* https://onlinelibrary.wiley.com/doi/full/10.1111/1758-5899.12976
6. *Summary of Stakeholders' submissions on Kenya* https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/317/94/PDF/G1931794.pdf?OpenElement; *Concluding observations on the fourth periodic report of Kenya* https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/105/49/PDF/G2110549.pdf?OpenElement
7. *East Africa: Civic Space Shrinking* https://www.hrw.org/news/2019/01/17/east-africa-civic-space-shrinking
8. *Ibid*
9. *In Kenya, averting a move to strangle civil society with the financial noose* https://www.opendemocracy.net/en/openglobalrights-openpage/in-kenya-averting-move-to-strangle-civil-society-with-financial-noose/
10. *The Shrinking Civic Space in East Africa* https://cipesa.org/wp-content/files/publications/Civic-Space-in-East-Africa-2019.pdf
11. *Press Statement: Civil Society Statement on the State of Civic and Democratic Space in Kenya Ahead of the General Election* https://defenderscoalition.org/press-statement-civil-society-statement-on-the-state-of-civic-and-democratic-space-in-kenya-ahead-of-the-general-elections/
12. *Kenya* https://monitor.civicus.org/country/kenya/
13. *President Ruto: We Will deliver a new policing paradigm,* https://www.president.go.ke/president-ruto-we-will-deliver-a-new-policing-paradigm/; *Why President Ruto disbanded DCI's Special Service Unit* https://nation.africa/kenya/news/why-president-ruto-disbanded-dci-s-special-service-unit-3987662

The violations, which have been widely condemned locally and internationally, show a worrying resurgence in human rights violations[14] by state security agencies and a wavering commitment by the government to promote and protect human rights.[15]

It is important to consider the role of government and state security agencies and the impact of their actions on civic space in the context of terrorism.

1.2 Historical Background of Intelligence Collection and Surveillance in Kenya

As highlighted above, the impact of Kenya's intelligence collection and operations on civic space can be traced back to the colonial period.[16] Since then, intelligence methods and strategies have gone through a dramatic evolution in response to changing internal and external threats and to meet the needs of the government in power in successive administrations.

These include controlling civic space and civic space actors.

The current National Intelligence Service (NIS) was a branch of the Kenya Police Force and known as the Special Branch between 1895 and 1986.[17] During Kenya's struggle for independence, the Kenya Police Force Special Branch gathered intelligence about the Mau Mau uprising whose activities the colonial British government declared as "terrorism", which was a threat to British interests in the colony.

The Special Branch used tactics such as pseudo or counter-gangs to infiltrate the Mau Mau and killed or arrested and detained Mau Mau fighters in detention camps where they were subjected to torture and exposed to diseases.

The Special Branch also focused on criminal cases relating to illegal immigration, smuggling, and actions of forces on the Kenya-Ethiopia border at Moyale. Its operations included monitoring internal groups, foreign diplomats, journalists and foreign visitors through secret recordings and mail interception[18] among other tactics.

The period between 1986 and 1999 was a watershed moment in the history of intelligence operations in Kenya. The Special Branch was rebranded in 1986 as the Directorate of Security Intelligence (DSI), although many continued to refer to it as the Special Branch.[19]

Kenya's leadership had just transitioned following the death of former president Mzee Jomo Kenyatta in August 1978, with Daniel Toroitich Arap Moi ascending into the presidency. Unlike Kenyatta

14. *President wrong to celebrate killer police officers https://www.standardmedia.co.ke/entertainment/opinion/article/2001477878/president-wrong-to-celebrate https://www.standardmedia.co.ke/entertainment/opinion/article/2001477878/president-wrong-to-celebrate-killer-police-officers; Kimani Ichungwa Sends a Warning Message To Protesters, Directs Police Officers To Do This https://ke.opera.news/ke/en/justice/5485f0bbe74e95263e2bbe0541ed984b; Kindiki issues tough warning ahead of Azimio demos https://www.the-star.co.ke/news/2023-07-18-kindiki-issues-tough-warning-ahead-of-azimio-demos/; Kindiki dismisses claims of extrajudicial killings as malicious https://www.pd.co.ke/news/kindiki-dismisses-claims-of-extrajudicial-killings-192684/;* 15. *KNCHR: Torture, abductions and arbitrary arrests marred Azimio protests https://nation.africa/kenya/news/knchr-torture-abductions-azimio-protests-4316278; Kenya: OHCHR 'very concerned' over disproportionate use of force against protesters https://news.un.org/en/story/2023/07/1138742; Joint statement by Ambassadors and High Commissioners in Kenya on Demonstrations https://www.gov.uk/government/news/joint-statement-by-ambassadors-and-high-commissioners-in-kenya-on-demonstrations*

16. *The Origins of the Intelligence System of Kenya https://gsdrc.org/document-library/the-origins-of-the-intelligence-system-of-kenya/*

17. *Ryan Shaffer, Following in the Footsteps: The Transformation of Kenya's Intelligence Services Since the Colonial Era https://www.cia.gov/static/d8ab5052e50097c9349d13e8dfcb5168/Following-in-Footsteps.pdf*

18. *Ibid*

19. *Paradigm Shift in Kenya's Security Intelligence Service http://erepository.uonbi.ac.ke/bitstream/handle/11295/60052/Lebishoy_Paradigm%20shift%20in%20Kenyans%20security%20intelligence%20service.pdf?sequence=3&isAllowed=y*

who only received intelligence briefings from the Director, Moi supplemented his briefs with intelligence from provincial heads and a network of unofficial informers.

These tactics suppressed the opposition and repressed freedom of expression in the country, which was exacerbated by the attempted August 1982 coup. The period after the coup saw the entrenchment of an authoritarian regime whose grip on power was cemented by the DSI, who under the then section 14 of the Police Act had the power to detain suspects without trial.

The DSI quickly became a political instrument, doing little to combat crime. Consequently, it focused its reign of terror including the targeting of perceived members of the Mwakenya[20] Movement and implementing measures geared at silencing outspoken government critics including university students, professors, civil servants, and opposition politicians.

Many of them were arbitrarily arrested, detained incommunicado, charged with seditious activities in trials marred with procedural technicalities such as denial of access to legal representation, faced human rights abuses such as torture at the infamous Nyayo House torture chambers and Nyati House and convictions for lengthy periods without access to visitors.[21]

The DSI was also involved in geopolitical issues such as the Cold War and maintained foreign intelligence relationships with the British Secret Intelligence Service (MI6), Security Service (MI5), the CIA and West Germany's Federal Intelligence Service among others.[22] Notably, Kenya's cordial relationships with Western nations in counterterrorism also made the country a target for terrorists in the following years.

The August 1998 bombing of the US embassies in Kenya and Tanzania by al-Qaeda prompted a shift of attention and intelligence operations to emerging internal threats and transnational terrorism.[23]

Following the attack, the DSI worked together with the CIA and the US Federal Bureau of Investigations (FBI). However, it emerged that security loopholes and lapses in the build-up to the attack, including poor coordination between the DSI and police agencies, corruption and unguarded borders were exploited by Al Qaeda operatives.[24]

The attack brought out the capacity gaps of the intelligence service in tackling sophisticated criminal transnational organisations, which required specialised skills the agencies did not possess.

There were also challenges with the weak legal framework under the Penal Code, political interference in prosecutions at the Office of

20. These were a union of underground nationalists to liberate Kenya in the late 1980s accused of seeking to overthrow the existing government and economic system. See: Mwakenya Movement https://en.wikipedia.org/wiki/Mwakenya_Movement#:~:text=The%20Mwakenya%20Movement%20(Muungano%20wa,fight%20for%20multi%2Dparty%20democracy.

21. Ryan Shaffer, Following in the Footsteps: The Transformation of Kenya's Intelligence Services Since the Colonial Era https://www.cia.gov/static/d8ab5052e50097c9349d13e8dfcb5168/Following-in-Footsteps.pdf; Torture, compounded by the denial of medical care https://www.amnesty.org/en/wp-content/uploads/2021/06/afr320181995en.pdf

22. Ibid

23. Ryan Shaffer, Following in the Footsteps: The Transformation of Kenya's Intelligence Services Since the Colonial Era https://www.cia.gov/static/d8ab5052e50097c9349d13e8dfcb5168/Following-in-Footsteps.pdf

24. An Analysis of the role of the police service in counterterrorism operations in Kenya https://bit.ly/3LQmrEI

the Attorney General, lethargy in intelligence collection, rivalry between security agencies, and a disconnect with the Judiciary.[25] Notably, the country's communication surveillance capacities were "vague and opaque".[26]

The DSI was disbanded in 1998 and the National Security Intelligence Service (NSIS), was subsequently established by an Act of Parliament. The NSIS Act[27] marked a shift in the intelligence regime by moving the function from the police in a bid to entrench reforms, greater autonomy and professionalism in its work.

Its functions were limited to intelligence gathering, vetting, and making recommendations to the President. Further, a National Security Intelligence Council was established to advise the service on its policies, expenditure and administration.

In addition, to enhance accountability and oversight, a Complaints Commission was created under Part III of the Act to inquire into complaints against members of the service and report to the President and the Council, its findings and recommendations on complaints made to it.

The NSIS operated between 1999 and 2010. This period coincided with the end of Moi's regime and the transition to Mwai Kibaki's government in December 2002. The period was characterised by the commencement of the global war on terrorism following the September 2001 attack on the World Trade Centre, in New York, which led to the onslaught against terrorism spearheaded by the US.[28]

Moreover, a global coalition of 120 states (including Kenya) against terrorism was formed, marked by increased investment and commitment by states to track terrorism finances and to freeze and seize assets linked to terrorist groups.

Further, there were efforts to upgrade and strengthen intelligence collection, cyber security, surveillance, and national security; and the implementation of airline security standards. It would also lead to the start of a military campaign against Al Qaeda in Afghanistan, and widespread adoption of anti-terrorism legislation.

Additionally, governments and law enforcement agencies set up coordinated operations to identify, arrest and detain suspected terrorists including offering substantial rewards. They introduced "Most Wanted Terrorist" lists, and initiated grants to support counter-terrorism efforts.[29]

In 2003, the government established the Anti-Terrorism Police Unit (ATPU)[30] following the Kikambala terror attack at Paradise Hotel in 2002,[31] as a response to prevent, disrupt, and investigate terrorist activities, share intelligence with other agencies, and create a terrorist database.

The Directorate of Military Intelligence of the Kenya Defence Forces was also actively involved in the counter-terrorism efforts. Other units such as the Recce Squad, Rapid Deployment Unit, and Rapid Response Teams were incorporated into counter-terrorism efforts.

The agencies worked closely with the NSIS in conducting signal intelligence by eavesdropping and intercepting phone calls of suspected persons

27. *National Security Intelligence Service Act* http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/NationalSecurityIntelligenceServiceActCap205.pdf
28. *The Global War on Terrorism: The First 100 Days* https://2001-2009.state.gov/s/ct/rls/wh/6947.htm
29. *Ibid, The Global War on Terrorism: The First 100 Days* https://2001-2009.state.gov/s/ct/rls/wh/6947.htm
30. *Anti-Terrorism Police Unit* https://www.cid.go.ke/index.php/sections/formations/atpu.html
31. *At least 12 killed in Kenya hotel blast* https://www.theguardian.com/world/2002/nov/28/israel.kenya

using IMSI catchers, using forensic cellular analysis technology to track down locations of individuals and analysing device content, sharing intelligence with security agencies such as Israel's Mossad, UK's MI6, and the CIA, who were given leeway to conduct covert operations in Kenya's coast and North Eastern regions.[32] The West also provided technical assistance to build the capacity of the Kenyan units on tactical operations, combat and signal intelligence under various security partnerships.

During the period, several security lapses exposed gaps in the investigation and coordination of security agencies in counter-terrorism efforts.[33] Further, the crackdown on the proscribed Mungiki sect members in 2007, led to massive human rights violations including extra-judicial killings and enforced disappearances.

In addition, operations of security agencies such as the ATPU and the tactics used to capture, detain and rendition terrorism suspects were clouded in secrecy and linked to human rights violations,[34] while corruption at border entry points remained the Achilles heel in preventing infiltration of foreign extremists.

Moreover, the lack of anti-terrorism laws limited the ability of law enforcement agencies to hold suspects accountable, and inadequate resource allocation to the police made it difficult for the service to purchase updated equipment, upgrade its facilities or train officers on modern policing practices. [35]

At the same time, a culture of impunity saw the agencies continue to use extra-legal means to deter terrorism. In the decade that followed, wanton abuse of surveillance and communication interception powers in the absence of adequate judicial oversight was reported.[36]

These failures culminated in the 2007-8 post-election violence, which caught security agencies flat-footed. The violence was exacerbated by the spread of ethnic hate, driven by unresolved historical tensions among various communities in the aftermath of the disputed presidential election, leading to over 1,000 deaths and 600,000 displaced internally.[37]

Arising from the shocking violence and threat to statehood, several fundamental reforms were undertaken including the adoption of a new Constitution in 2010, which introduced changes in the security sector.

The Constitution transformed NSIS into the National Intelligence Service (NIS), the Armed Forces was renamed as Kenya Defence Forces (KDF), and the Kenya Police Force became the National Police Service (NPS), and designated them as constitutional bodies comprising the national security organs. In 2012, the government enacted several security-related laws including the National Intelligence Service Act, the Prevention of Terrorism Act, and the National Security Council Act.

---

32. Ibid, An Analysis of the role of the police service in counterterrorism operations in Kenya https://bit.ly/3LQmrEl

33. Refworld, Kenya: The Mungiki sect, including organizational structure, leadership, membership, recruitment and activities; the relationship between the government and sects, including protection offered to victims of devil worshippers and sects, such as the Mungiki (2010-October 2013), 15 November 2013, KEN104594.E, https://www.refworld.org/docid/52a72f7e4.html

34. Kenya: Killings, Disappearances by Anti-Terror Police https://www.hrw.org/news/2014/08/18/kenya-killings-disappearances-anti-terror-police

35. Ibid, An analysis of the role of the police service in counterterrorism operations in Kenya https://bit.ly/3LQmrEl

36. Privacy International, Track, Capture, Kill: Inside Communications Surveillance and Counterterrorism in Kenya https://privacyinternational.org/sites/default/files/2017-10/track_capture_final.pdf

37. Ryan Shaffer, Following in the Footsteps: The Transformation of Kenya's Intelligence Services Since the Colonial Era https://www.cia.gov/static/d8ab5052e50097c9349d13e8dfcb5168/Following-in-Footsteps.pdf

In 2014, the hastily enacted Security Laws (Amendment) Act 2014 introduced a raft of amendments to other laws including the establishment of the multi-agency National Counter-Terrorism Centre (NCTC)[38] and a Joint Terrorism Task Force (JTTF).

Other measures were also taken to regulate speech and enhance communication surveillance on grounds of national security. These measures were widely opposed for their unconstitutionality by civil society,[39] legislators[40] and the opposition who filed a suit at the High Court.[41]

As a response to criticism, the government in 2014 unsuccessfully attempted to use the anti-terrorism law to silence prominent human rights organisations such as MUHURI and Kenya Human Rights Commission, and 500 others, ostensibly for registration irregularities and fraud.

Despite these efforts, counter-terrorism efforts continued to suffer setbacks due to a strained and stretched security workforce, widespread corruption and impunity, poor investigative capacity due to professional shortcomings, and lack of accountability.

This was coupled with coordination gaps resulting from weak relations, mistrust, supremacy battles and internal power struggles among security agencies. Lingering lapses provided a fertile ground for the execution of the 2013 Westgate Mall attack,[42] the 2015 Garissa University attack[43] and the 2019 DusitD2[44] Hotel attack, all of which could have been averted.

In response to the 2013 attacks, the government in April 2014 launched a brutal counter-terrorism offensive dubbed Operation Usalama Watch in Nairobi's Eastleigh area and Mombasa where security forces sought to identify illegal immigrants and criminals.[45]

As part of the operation at least 4,000 people largely from the Somali community suspected of engaging in terrorist activities were arrested, ill-treated and detained, while at least 1,000 were forcibly relocated to refugee camps in northern Kenya and 359 were expelled from Kenya.[46]

The operation despite its good intentions showed little regard for human rights standards and as a result, alienated and sowed resentment among the Muslim and Somali communities, highlighting the biased and discriminatory counter-terrorism efforts that profile and target Muslims and Somalis, the institutional weaknesses and political divisions in counter-terrorism efforts.[47] In 2017, the NIS declared that terrorism threatened Kenya's national security and development.[48]

In recent years there have been efforts to strengthen Kenya's counter-terrorism posture, including by

38. *Security Laws (Amendment) Act, 2014* https://www.refworld.org/pdfid/4df202da2.pdf
39. *Kenya: Concerns with Security Laws (Amendment) Bill* https://www.article19.org/resources/kenya-concerns-security-laws-amendment-bill/; *Kenya: Security Bill Tramples Basic Rights* https://www.hrw.org/news/2014/12/13/kenya-security-bill-tramples-basic-rights
40. *Senators recalled to discuss terror laws* https://nation.africa/kenya/news/politics/Senators-recalled-to-discuss-terror-laws/1064-2570012-9up33x/index.html
41. *Kenya anti-terror law in court hearing* https://www.dw.com/en/kenya-opposition-to-clock-up-political-mileage-over-anti-terror-law/a-18155675
42. *Terror in Nairobi: the full story behind al-Shabaab's mall attack* https://www.theguardian.com/world/2013/oct/04/westgate-mall-attacks-kenya
43. *Al-Shabaab Attack on Garissa University in Kenya*
44. https://www.start.umd.edu/publication/al-shabaab-attack-garissa-university-kenya
45. *Nairobi DusitD2 hotel attacked by suspected militants* https://www.bbc.com/news/world-africa-46880375
46. *Kenya should go back to the drawing board to find a realistic solution to the threat of terrorism, radicalization and religious extremism* https://issafrica.org/iss-today/kenyas-current-probe-on-terror-why-operation-usulama-watch-wont-cut-it
47. *Kenya: Somalis scapegoated in counter-terror crackdown* https://www.amnesty.org/en/latest/press-release/2014/05/kenya-somalis-scapegoated-counter-terror-crackdown/
48. *Update Briefing - Kenya: Al-Shabaab – Closer to Home* https://www.files.ethz.ch/isn/184018/Kenya-Al-Shabaab.pdf

addressing the key challenges in coordination. Some of this has seen the establishment of the National Counter Terrorism Centre (NCTC) established in 2014.[49]

In 2022, the Director of Public Prosecutions issued the Inter-Agency Guidelines on Cooperation & Collaboration in the Investigation and Prosecution of Terrorism and Terrorism Financing, these are expected to promote effective coordination, collaboration and cooperation in the investigation and prosecution of terrorism and terrorism financing.[50]

Kenya's counter-terrorism programmes are largely financed by the state. The national budgetary allocation for the Ministry of Defence, Ministry of Interior, National Police Service and National Intelligence Services has been on the increase in the past three years standing at KES 143 billion, KES 26 billion, KES 1.2 billion and KES 43.8 billion respectively in the 2023/24 financial year. [51]

This reflects the country's focus on addressing security challenges, including terrorism. It is also worth noting that the specific budgetary allocations for certain counter-terrorism activities such as by the military, are largely classified and there is limited public information on its extent and nature.

Special projects such as the National Integrated Identity Management System (NIIMS), National Forensic Laboratory and National Communication and Surveillance System were funded to the tune of KES 1 billion, KES 335 million and KES 1 billion in the 2022/23 financial year.[52]

Kenya has also received financial and technical support in the form of training and equipment for Kenya's security forces, as well as intelligence sharing and cooperation in counter-terrorism operations.

Kenya is a key partner to the United States and a member of the Global Coalition to Defeat ISIS.[53] Between 2012 and 2015, Kenya received USD 147 million (KES 23.9 billion) from the United States[54] towards AMISOM operations, military and police training on cyber security, conducting operations and data sharing.

Support from the United Kingdom included grants totalling GBP 3.68 million (KES 760 million) between 2018 and 2021 to support law enforcement and criminal justice work.[55]

Similarly, Kenya has received support from other countries such as China (USD 100M (KES 8.5B)) for the installation of CCTV cameras in major cities in 2012; Germany (EUR 550 million (KES 96.8 million)

---

49. Kenya: Terror Groups Pose Biggest Threat to Kenya's Security - NIS, http://allafrica.com/stories/201709200081.html

50. National Counter Terrorism Centre (NCTC) https://counterterrorism.go.ke/

51. National Counter Terrorism Centre, Newsletter, November-December 2022, VOL 1 https://counterterrorism.go.ke/wp-content/uploads/2023/02/National-Counter-Terrorism-Centre-Newsletter-Vol-1-10-min.pdf

52. The National Treasury and Economic Planning, The National Treasury https://www.google.com/url?q=https://www.treasury.go.ke/budget-books-1/%231649848244709-4dedb564-8b63&sa=D&source=docs&ust=1683617084670365&usg=AOvVaw2UJLGDX8ebVZdsavodkujN; Budget Statement: FY 2020/2021 https://www.treasury.go.ke/wp-content/uploads/2021/03/Budget-Speech-2020-2021.pdf; Budget Statement: FY 2021/2022 https://www.treasury.go.ke/wp-content/uploads/2021/06/FY-2021-22-Budget-Statement.pdf; Budget Statement: FY 2022/2023 https://www.treasury.go.ke/wp-content/uploads/2021/06/Budget-Statement-for-the-FY-2022-23_F.pdf

53. Ibid 48

54. Kenya joins global coalition against Islamic State https://nation.africa/kenya/news/Kenya-joins-coalition-against-Isis/1056-4971788-mmlsmsz/index.html

55. Kenya: Killings, Disappearances by Anti-Terror Police https://www.hrw.org/news/2014/08/18/kenya-killings-disappearances-anti-terror-police; US Counterterrorism Aid to Kenya: Focusing on a Military with Motivation and Corruption Problems https://securityassistance.org/publications/u-s-counterterrorism-aid-to-kenya/

in 2016;[56] Canada (USD 6 million (975 million);[57] and the European Union (KES 75 million).[58] Kenya has also received technical support and training from France,[59] Israel[60] and the European Union.[61]

A timeline of key terrorist attacks in the past three decades is highlighted below.

Timeline of Key Terrorist Attacks in Kenya

Year	Incident
1980s-1990s	Northern Frontier District (NFD) insurgencies affecting Somali communities; Norfolk Hotel attack resulting in the death of 20 people and injury of 100 others.[62]
1998	US Embassy bombing on August 7, 1998, where 224 people were killed and 4,500 wounded after an attack by terrorists linked to al-Qaeda [63]
2002	Kikambala Hotel bombing on 28 November 2002, where 15 people were killed and 80 injured by suicide bombers linked to al-Qaeda. [64]
2011	Various grenade attacks across several towns and establishments in October and November resulted in the death of seven people, 15 injured and one kidnapping by terrorists linked to al-Shabaab. [65]

56. United Kingdom Government, "East Africa Crime and Justice Programme" https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/758132/AFRA_East_Africa_Crime_and_Justice_Programme_Summary_FY_18_19.odt; United Kingdom Government "East Africa Crime and Justice Programme Summary 2020" https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1003192/East_Africa_Crime_and_Justice_programme_summary_2020_to_2021.odt

56. The Federal Government "Federal Government Strategy to Prevent Extremism and Promote Democracy" https://www.bmfsfj.de/resource/blob/115448/cc142d640b37b7dd76e48b8fd9178cc5/strategie-%20der-bundesregierung-zur-extremismuspraevention-%20und-demokratiefoerderung-englisch-data.pdf

57. Global Affairs Canada, Canada Kenya Relations https://www.international.gc.ca/country-pays/kenya/relations.aspx?lang=eng

58.

59. France in Kenya and Somalia, French Embassy in Nairobi https://ke.ambafrance.org/The-Defense-Mission; Kenya Defence Forces, Defence PS Hosts French Delegation in Bid to Cement Cooperation https://mod.go.ke/news/defence-ps-hosts-french-delegation-in-bid-to-cement-cooperation/

60. Kenya, Israel's Forward Base in Africa https://www.haaretz.com/2013-09-23/ty-article/.premium/kenya-israels-forward-base-in-africa/0000017f-e3b6-d75c-a7ff-ffbf90a00000

61. The European Union Official Website, The European Union and Kenya, https://www.eeas.europa.eu/kenya/european-union-and-kenya_en?s=352; 2023/2024 Estimates of Development expenditure of the Government of Kenya for the year ending 30th June 2024, Volume I, April 2023 https://www.treasury.go.ke/wp-content/uploads/2023/05/FY-2023-24-Development-Budget-Book-1011-1083.pdf

62. Report on the Negative Effects of Terrorism https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/AdvisoryCom/Terrorism/Kenya.pdf

63. East African Embassy Bombings
https://www.fbi.gov/history/famous-cases/east-african-embassy-bombings

64. 2002: Terrorists hit Paradise Hotel after elaborate planning https://nation.africa/kenya/life-and-style/dn2/2002-terrorists-hit-paradise-hotel-after-elaborate-planning-913752

65. Report on the Negative Effects of Terrorism https://www.ohchr.org/sites/default/files/Documents/HRBodies/HRCouncil/AdvisoryCom/Terrorism/Kenya.pdf

Year	Incident
2012	Various grenade and gun attacks on churches, businesses, markets and estates by terrorists linked to al-Shabaab resulted in the death of several people including police officers and injuries to several others.[66]
2013	Westgate Mall attack on Sept. 21 2013, 67 people were killed and 175 injured, by terrorists linked to al-Shabaab.[67]
2014	Attacks on a Mandera bus by terrorists linked to al-Shabaab killing at least 28 people and injuring several others.[68] Attack on a bus on Thika road left 62 wounded and three killed.[69]
2015	Various grenade attacks across several towns and establishments in October and November resulted in the death of seven people, 15 injured and one kidnapping by terrorists linked to al-Shabaab.[70]
2019	DusitD2 Hotel attack on 15 January 2019, where 21 people were killed and several injured[71] and 33 other attacks also by terrorists linked to al-Shabaab resulting in 62 fatalities, including 42 security officials.[72]
2020	Manda Bay attack on 15 January 2020 on a military base resulted in the death of five people and 40 injured by terrorists linked to al-Shabaab.[73] Attacks on communications masts were also reported.
2021	Mandera attack where two police officers were killed and 12 others injured by terrorists linked to al-Shabaab.[74]
2021	Mandera attack where two police officers were killed and 12 others injured by terrorists linked to al-Shabaab.[75]
2023	At least 19 violent acts including explosions, battles and attacks by Al-Shabaab led to several injuries and the death of at least 26 civilians, military personnel and police officers in Garissa, Lamu and Wajir counties.[76]

66. *2011–2014 terrorist attacks in Kenya* https://en.wikipedia.org/wiki/2011%E2%80%932014_terrorist_attacks_in_Kenya
67. *Terror in Nairobi: the full story behind al-Shabaab's mall attack* https://www.theguardian.com/world/2013/oct/04/westgate-mall-attacks-kenya
68. *Kenya bus attack survivor tells how gunmen selected their victims* https://www.theguardian.com/world/2014/nov/23/kenya-bus-attack-survivor-tells-how-gunmen-selected-their-victims
69. *Bus bombing in Nairobi leaves at least three dead* https://www.theguardian.com/world/2014/may/04/kenya-bus-bombing-nairobi-thika-highway
70. *Garissa University College attack in Kenya: What happened?* https://www.bbc.com/news/world-africa-48621924
71. *Kenya attack: 21 confirmed dead in DusitD2 hotel siege* https://www.bbc.com/news/world-africa-46888682
72. *Trends of Violent Extremist Attacks and Arrests in Kenya, January 2019 - December 2019* https://cve-kenya.org/media/documents/Trends_of_Violent_Extremist_Attacks_and_Arrests_in_Kenya_2019.pdf
73. *Extremists attack Kenya military base, 3 Americans killed* https://apnews.com/article/somalia-us-news-ap-top-news-international-news-east-africa-65926ee82091f779d28d6a9644fb739f
74. *One militant killed after the killing of 2 cops in Mandera* https://www.the-star.co.ke/news/2021-12-05-special-teams-kill-one-militant-after-killing-of-2-cops-in-mandera/
75. *3 Kenyan police officers wounded in roadside blast in border region* https://english.news.cn/africa/20220606/a9329a8657644eca91c09c452c37793e/c.html; *13 People Killed by Roadside Bomb in Northeastern Kenya, Terror Group Al-Shabaab Suspected* https://www2.cbn.com/news/world/13-people-killed-roadside-bomb-northeastern-kenya-terror-group-al-shabaab-suspected; *Six Christians Killed in Kenya Terrorist Attack* https://www.persecution.org/2022/01/03/six-christians-killed-kenya-terrorist-attack/
76. *Kenya: Al-Shabaab Attacks Surge Ahead of Somalia-Kenya Border Reopening* https://acleddata.com/2023/07/07/kenya-situation-update-july-2023-al-shabaab-attacks-surge-ahead-of-somalia-kenya-border-reopening/

From the statistics, it is evident that attacks increased in intensity at some point, and therefore the role of the law and surveillance technologies have become essential to gather intelligence to support the fight against terror.

The challenge for states such as Kenya, is how to achieve results while respecting human rights and freedoms, ensuring compliance with the rule of law, and promoting greater transparency and accountability of state security agencies involved in countering terrorism.

1.3 Objectives

The objectives of this study are to:

1. Document the use and misuse of digital laws, technologies and infrastructure to surveil civic actors, silence dissent, and restrict online civic space;

2. Establish the role of private telecoms, content moderation platforms, and global and local media organisations, including suppliers of sophisticated hacking and surveillance tools and platforms used to arbitrarily surveil and intercept communications;

3. Understand the potential use of digitised government services and the use of biometric data by the government to restrict civic space;

4. Assess the impact of COVID-19 in entrenching surveillance and restrictions that impact civic space; and

5. Identify the opportunities that exist to disrupt, reform, and over the long term, transform the influence of security on civic space.

1.4 Methodology

In conducting this research, the KICTANet team reviewed the various policies, laws, regulations, strategies and technologies that have an impact on Kenya's counter-terrorism efforts.

The information in the report builds on previous reports and analyses on privacy, access to information, freedom of expression, and surveillance by KICTANet. The report is based on information in the public domain including official government reports, media articles, civil society reports and analyses.

We note that there were limitations to the study that impacted our ability to cover the topic with more depth and complexity. These include limited information and documentation by state and private actors, limited data and lack of reliable information on certain aspects of the topic, and limited time.

The role of the law and surveillance technologies have become essential to gather intelligence to support the fight against terror.

The challenge for states such as Kenya, is how to achieve results while respecting human rights and freedoms, ensuring compliance with the rule of law, and promoting greater transparency and accountability of state security agencies involved in countering terrorism.

2.0 Applicable Laws and Standards

2.1 International and Regional Framework

Kenya is a signatory to various international human rights instruments that are essential for the protection of civic space and the right to privacy. Key among them include the Universal Declaration of Human Rights (UDHR)[77] and the International Covenant on Civil and Political Rights (ICCPR).[78]

The country is also a signatory to the African Charter on Human and People's Rights (ACHPR) whose articles 5 and 24 emphasise the importance of individual and group dignity in pursuing their development.

Kenya also adopted the East African Community (EAC) Framework for Cyber Laws which aims to establish a standardised cyber environment, requiring each country to enact legislation on data protection and cyber security.[79]

However it's to ratify or sign the African Union (AU) Convention on Cyber Security and Personal Data Protection.

Concerning privacy, the United Nations Human Rights Committee has stated that any interference with anyone's privacy must be under the law, necessary and proportionate to achieve a legitimate aim.

> ***The United Nations Human Rights Committee has stated that any interference with anyone's privacy must be under the law, necessary and proportionate to achieve a legitimate***

The laws must be,

(a) Publicly accessible;

(b) contain provisions that ensure that collection of, access to and use of communications data is tailored to specific legitimate aims;

(c) Are sufficiently precise, specifying in detail the precise circumstances in which any such interference may be permitted, the procedures for authorising, the categories of persons who may be placed under surveillance, the limits on

77. *Universal Declaration of Human Right, Article 12*
78. *International Covenant on Civil and Political Rights, Article 17 https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights*
79. *Grace Mutung'u, Surveillance Law in Africa: A Review of Six Countries Kenya Country Report*

the duration of surveillance, and procedures for the use and storage of the data collected; and

d) Provide for effective safeguards against abuse."[80]

Similarly, Principle 41 of the ACHPR Declaration of Principles on Freedom of Expression 2019[81] outlines how states should conduct communication surveillance.

It provides that states "shall not engage in or condone acts of indiscriminate and untargeted collection, storage, analysis or sharing of a person's communications.
It requires that such surveillance be authorised by law that conforms with international human rights law and standards, and that is premised on specific and reasonable suspicion that a serious crime has been or is being carried out or for any other legitimate aim.

Further, laws authorising targeted communication surveillance provide adequate safeguards for the right to privacy. Principle 42 calls upon states to adopt laws for the protection of the personal information of individuals following international human rights laws and standards.

It also urges the creation of effective remedies to privacy violations and the establishment of independent oversight entities to protect privacy.

2.2 Constitution of Kenya, 2010

The Constitution provides that general rules of international law and treaties ratified by Kenya shall form part of the law of Kenya.

These include international human rights instruments highlighted above, which are essential for the protection of civic space and whose standards are elaborated in the Bill of Rights.
Under Article 24(1), these rights may only be limited by law to the extent that the limitation is "reasonable and justifiable in an open and democratic society based on human dignity, equality and freedom."

Article 238(1) defines national security as: "the protection against internal and external threats to Kenya's territorial integrity and sovereignty, its people, their rights, freedoms, property, peace, stability and prosperity, and other national interests."

The constitution further outlines the principles to be promoted to achieve national security including recognition of the supremacy of the Constitution, compliance with the law with the utmost respect for the rule of law, democracy, human rights and fundamental freedoms among other principles.

Moreover, Article 10 sets the values and principles of governance which include, the rule of law, democracy, human dignity, protection of the marginalised, good governance, integrity, transparency, and accountability among other values.

Whereas state organs and officers mandated to promote national security are bound by these principles and values the threat-based definition of national security is in practice often interpreted narrowly to focus on security sector interventions and not human rights considerations or the principles under the constitution.

Further, the National Security Council is required under Article 240(7) of the Constitution and Section 16 of the National Security Council Act, 2012 Act[82] to report to Parliament annually on the state of security.[83]

80. U.N. High Commissioner for Human Rights, The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner
81. Declaration of Principles on Freedom of Expression 2019 https://achpr.au.int/index.php/en/special-mechanisms-reports/declaration-principles-freedom-expression-2019#:~:text=The%20Declaration%20establishes%20or%20affirms,to%20express%20and%20disseminate%20information.
82. The National Security Council Act, 2012 https://www.nis.go.ke/downloads/THE%20NATIONAL%20SECURITY%20COUNCIL%20ACT,%202012.pdf
83. Parliament of Kenya, Annual Report to Parliament on the State of National Security, http://www.parliament.go.ke/sites/default/files/2020-11/SP%207284-2020%20ANNUAL%20REPORT%20FINAL%20JAN%202020%20_0.pdf

2.3 Statutes Facilitating Communication Interception & Surveillance

The National Intelligence Service Act 2012, Prevention of Terrorism Act (POTA) 2012, Mutual Legal Assistance Act 2011, Computer Misuse and Cybercrimes Act 2018 and the Kenya Information and Communication Act 2011, are some of the laws which permit surveillance and the interception of communications.
These laws and policies restrict the right to privacy and grant state intelligence and law enforcement agencies broad powers to surveil and intercept communications of targeted persons in the course of criminal investigations, including terrorism.

Section 34 of the Prevention of Terrorism Act empowers police officers to seek ex parte warrants before a magistrate's court to gather information where there is suspicion of the commission of a terrorism-related offence.

Notably, section 35 permits the limitation of the right to privacy, by enabling the search of a person's home or property, seizure of such property, and investigation, interception, or interference with their communication.

Whereas section 36 of the Act requires applications for warrants for interception of communication to be approved in writing by the Inspector-General of Police or the Director of Public Prosecutions, it is not apparent whether this is always the case.

Further, while the Cabinet Secretary is required to make regulations under section 36A to regulate the interception of communication by the National Security Organs, these regulations are yet to be put in place. Therefore, such interception potentially continues without adequate oversight and accountability.

Section 36 of the National Intelligence Service Act[84] limits the right to privacy of any person under investigation.

Further, section 42 of the Act empowers the Director-General of NIS to authorise the conduct of "special operations" which include covert measures to neutralise threats against national security subject to guidelines issued by the National Intelligence Service Council.

These include the power to authorise members of NIS to enter any place, access anything, search, monitor communication, install any devices, or take any necessary action to obtain any information or document to preserve national security.

The authorisation is required to be specific, accompanied by a warrant from the High Court and valid for a renewable period of 180 days.

Part IV of the Computer Misuse and Cybercrimes Act 2018 grants police officers power during criminal investigations to among others: search and seize computer data, record and access seized data, seek production of computer data, require expedited preservation and disclosure of traffic data, collect traffic data in real-time, and intercept content data.[85]

Police officers are required to seek warrants from courts to authorise the afore-mentioned actions, save for where expedited preservation and partial access are required where the police are only required to issue a notice.

Service providers may be compelled under sections 52 and 53 to collect information on behalf of the police, or allow police to collect information directly through the application of technical means.

Part V of the law provides elaborate provisions for the facilitation of mutual legal assistance in

84. National Intelligence Service Act http://kenyalaw.org:8181/exist/kenyalex/actview.xql?actid=No.%2028%20of%202012
85. "Content data" is defined as the actual substance of the communication

criminal investigations seeking access to computer systems, electronic communications, traffic data and computer data.

Courts may require service providers to keep the content of warrants and orders confidential. However, while the Cabinet Secretary is required to make regulations to guide the conduct of search, seizure and collection of electronic evidence, these regulations are yet to be put in place.

As such, these practices are potentially carried out without a clear standard operating procedure. The Mutual Legal Assistance Act also provides a framework through which foreign states can request real-time traffic data and content data.

To obtain an interception request, the requesting state must disclose information about the criminal activity being investigated, the identification of the individual in question, including their electronic or telecommunication address for monitoring purposes, the intended duration of the interception, and the authority making the request.

Furthermore, a warrant or lawful interception order from the requesting nation must be confirmed by the Central Authority (Office of the Attorney General).

Section 89 of the Kenya Information and Communication Act requires the Communications Authority to seek search and seizure warrants to enter into any premises and examine any telecommunication system or apparatus in the company of police officers where there is a reasonable belief that an offence under the Act is being or is likely to be committed.

The Kenya Information and Communications (Registration of SIM-cards) Regulations, 2015[86] under regulation 5, requires telecommunications operators or agents to register subscribers by collecting their personal information.[87]

Regulation 11 grants the Authority power to enter into any telecommunications operator's offices and inspect and access its systems, premises, facilities, files, records and other data to ensure compliance with the regulations.

Currently, there is no requirement under these laws to notify a person who is the subject of such interception warrants, and as such, subjects of such orders will most likely be unaware of the same and hence find it difficult to challenge them.

As such, there is limited transparency surrounding such warrants as most of the time, are issued to compel third parties, mostly the network operators to facilitate interception without a stipulation to serve the subject of the interception with the warrant.

Hence, subjects cannot know that they are the subject of an investigation, thus limiting their ability to challenge such orders.
Notably, section 51 of the Data Protection Act exempts the processing of personal data where

86. The Kenya Information and Communications (Registration of SIM-cards) Regulations, 2015 https://www.ca.go.ke/wp-content/uploads/2018/02/Registration-of-SIM-%E2%80%93Cards-Regulations-2015-1.pdf

87. These include names, originals and copies of official identification (identity card, service card, passport, alien card or birth certificates), copies of registration certificates, date of birth, gender, physical and postal addresses, and other numbers associated with them

necessary for national security or public interest. The blanket exemption creates room for abuse by security and intelligence agencies when conducting surveillance.

It also shields them from the oversight and compliance regime despite the volume, sensitivity and nature of the personal data they collect and the impact of their functions on the enjoyment of the right to privacy.

The draft National Closed-circuit Television (CCTV) Policy 2019 guides the installation, operation, and management of CCTV systems in public and private premises to promote their use as a mechanism to ensure a safe and secure nation.

The policy, which is yet to come into force, requires persons who install CCTV systems to register them with the relevant authorities, maintain documentation of the system components, provide reasonable access to security agencies, and disclose CCTV footage/images for investigations.[88]

Kenya has also adopted several other policies and strategies that are crucial. The National Information, Communications and Technology (ICT) Policy 2019[89] highlights cybercrime and cybersecurity vulnerabilities as key challenges and commits to implementing computer and cybercrime legislation.

The National Strategy to Counter Violent Extremism, 2016[90] complements security-focused counterterrorism laws with a framework for CVE, which includes the provision of employment options, business opportunities and life skills among other interventions aimed at reducing youth vulnerability to violent extremism.

The National Cybersecurity Strategy 2022[91] identifies cyber terrorism, cyber subversion/activism and cyber espionage as key threats and notes the use of ICTs for recruitment, radicalization, incitement, financing, training, planning and execution of terrorist attacks.

2.4 Safeguards in Laws to Protect Privacy

Several laws provide safeguards for the protection of the right to privacy. The Data Protection Act gives effect to Article 31 of the Constitution 2010.

It establishes the Office of the Data Protection Commissioner and prescribes the principles that must be adhered to when processing personal data,[92] the rights of data subjects[93] and technical and organisational measures to be put in place by entities to ensure the protection of personal data during its processing.

Under section 36 of the Prevention of Terrorism Act, the interception of communication other than as provided by this law is an offence punishable by imprisonment for a term not exceeding ten years or a fine not exceeding five million or both.[94]

To intercept communications, a police officer must obtain the written consent of the Inspector-General of Police or the Director of Public Prosecutions before making an ex parte application before a Chief Magistrate or the High Court.

88. *National CCTV Policy https://www.interior.go.ke/wp-content/uploads/2019/07/CCTV-POLICY-DRAFT-TWO-14-02-2019.pdf*
89. *National Information, Communications and Technology (ICT) Policy https://www.ict.go.ke/wp-content/uploads/2019/12/NATIONAL-ICT-POLICY-2019.pdf*
90. *Mikewa Ogada, A Policy Content Evaluation of Kenya's National Strategy to Counter Violent Extremism https://www.chrips.or.ke/download/a-policy-content-evaluation-of-kenyas-national-strategy-to-counter-violent-extremism/*
91. *Ministry of ICT, National Cybersecurity Strategy, https://ict.go.ke/wp-content/uploads/2022/10/KENYA-CYBERSECURITY-STRATEGY-2022.pdf*
92. *Data Protection Act, 2019, Section 25*
93. *Ibid 31, Section 26*
94. *Prevention of Terrorism Act, 2012, Section 36(6)*

Further, the court can only grant an interception order if the information relates to the offence or the whereabouts of the suspect. However, it is not clear whether these procedures are always complied with.

Section 55 of the Computer Misuse and Cybercrimes Act provides for an appeal mechanism whereby a person aggrieved by an order of the court may appeal the decision within 30 days of the order.

However, the fact that the orders could be confidential means the mechanism is of no use to third parties such as telephone subscribers whose information is sought under the orders.

This is also complicated by the fact that whereas there is no legal obligation on service providers to disclose or publish transparency reports of statistics of information requests received from law enforcement agencies, they also do not do so voluntarily as has become global best practice in the technology sector.

Section 31 of the Kenya Information and Communication Act (KICA) prohibits a licensed telecommunications provider from intercepting or disclosing the contents of the information intercepted or sent through a licensed communication system other than in the course of its business.

It imposes a fine of up to KES 300,000 or imprisonment for up to three years. Regulation 16 of the Kenya Information and Communications (Registration of SIM-cards) Regulations, 2015 requires telecommunications operators to take reasonable steps to ensure the security and confidentiality of their subscriber's registration particulars.

Whereas this is the case, there have been incidents where the personal data of subscribers have been mishandled leading to data breaches.

For example, in 2022, it was reported that Safaricom staff in 2019 stole the personal data of 11.5 million subscribers and sold the same to Pevans East Africa, a sports betting company.[95]

Also, in February 2023, Safaricom was sued in a class action suit following its requirement for subscribers to submit biometric information as part of its SIM-card registration process.[96]

These examples demonstrate that compliance with privacy laws and cybersecurity requirements is still a challenge, even for Kenya's largest telco.

The Kenya Information and Communications (Consumer Protection) Regulations, 2010[97] under regulation 3 guarantees the right to personal privacy and protection of subscribers against unauthorised use of their personal information.

Regulation 4 mandates service providers to "take appropriate technical and organisational measures to safeguard the security of its services" and to inform the subscribers of any risk of breach of the security, the remedies and the costs involved.

Similarly, regulation 15 requires licensees not to monitor, disclose or allow the monitoring or disclosure of information transmitted through their systems, whether through listening, tapping, storage, or any means of interception or surveillance of communications and data.

95. How Safaricom mishandled subscriber data leak https://nairobilawmonthly.com/how-safaricom-mishandled-subscriber-data-leak/

96. Court allows subscribers to join Safaricom suit over 'data leak' clause https://nairobilawmonthly.com/court-allows-subscribers-to-join-safaricom-suit-over-data-leak-clause/

97. Kenya Information and Communications (Consumer Protection) Regulations, 2010 https://www.ca.go.ke/wp-content/uploads/2018/02/Consumer-Protection-Regulations-2010-1.pdf

In addition, regulation 7 requires licensees to put in place a complaint-handling procedure, handle complaints within a reasonable time and allow subscribers to escalate complaints to the Communications Authority.

2.5 Challenges and Gaps in Laws

Broad and Vague Laws

Generally, states (including Kenya) are known to exploit national security, terrorism and public order rationales as justification for intrusive surveillance technology and techniques, with little regard for human rights standards.

Further, laws developed to address threats to national security have been criticised for being too broad, vague, and lacking adequate safeguards against abuse, leading to violations of the right to privacy and freedom of expression.

Moreover, there are concerns that the laws are used to target terror suspects, political dissenters, journalists, and human rights defenders, besides being used to gain a competitive advantage in business.

For example, the surveillance powers under section 42 of the NIS Act are framed in broad terms, which creates room for abuse as it permits the deployment of surveillance against a wide array of targets.

The laws are neither limited to investigations of the most serious crimes, nor do they stipulate the use and exhaustion of other less intrusive means to achieve the same goals.

For example, section 36 of the National Intelligence Service Act does not specify the offences for which surveillance and interference with communication may be undertaken, thus leaving it open for broad interpretation and could be abused to target civic actors.

Moreover, section 36 of POTA authorises the conduct of surveillance and interception of communication in broad terms meaning interception orders can relate to several persons, which goes against the principle of proportionality.

Abuse of laws

Notably, even when laws are explicit on what ought to be done, like when to seek warrants, law enforcement agencies disregard and rarely comply with the stipulations, often with little or no consequences due to the weak oversight and redress mechanisms.

A 2017 report by Privacy International[98] revealed that communication surveillance was often carried out by the NIS outside legal procedures, without oversight and the information obtained was used to commit further human rights violations.

The report documented gaps in the provisions of POTA and the NIS Act, and their actual implementation in practice.
Sections 22 (false publications) and 23 (publication of false information) of the Computer Misuse and Cybercrimes Act have been criticised for being broad, ambiguous and with the potential of profound and chilling effect on the work of civic actors.

These two provisions have been used to target bloggers. In 2020, blogger Cyprian Nyakundi was arrested and charged under section 23 for posting information on his Twitter account.[99]

In 2021, another blogger, Edgar Obare, was arrested and charged under the same law for an expose on his social media accounts.[100]

98. *Privacy International, Track, Capture, Kill* https://privacyinternational.org/sites/default/files/2017-10/track_capture_final.pdf
99. *Cyprian Nyakundi Officially Charged For Alleged Publication Of False Information* https://ifree.co.ke/2020/04/cyprian-nyakundi-officially-charged-for-alleged-publication-of-false-information/
100. *Kenya police turn to Twitter PR as the arrest of a blogger goes against public opinion* https://advox.globalvoices.org/2021/03/19/kenya-police-turn-to-twitter-pr-as-the-arrest-of-a-blogger-goes-against-public-opinion/

During the COVID-19 pandemic, several bloggers and social media users were arrested under the same law, for allegedly spreading false information online, including misinformation about the pandemic.[101]

The High Court has pointed out[102] that ambiguity in law may result in a varied understanding of the legislation. Thus, provisions seeking to limit rights ought to be sufficiently precise to enable subjects to regulate their conduct accordingly.[103]

> ***The High Court has pointed out that ambiguity in law may result in a varied understanding of the legislation. Thus, provisions seeking to limit rights ought to be sufficiently precise to enable subjects to regulate their conduct accordingly.***

Facilitation of Surveillance by Intermediaries

While the laws require security agencies to obtain warrants before intercepting communications, NIS had direct access to communication networks through which they intercepted both communication content and call data records without warrants or the knowledge of network operators.

Subsequently, NIS often shared this intelligence with the police, who then sought court warrants to re-surveil based on such tips to comply with legal requirements.

In addition, research has found that the telcos frequently provided customer data to security agencies without demanding warrants, possibly due to direct or implied threats to their licences, further aided by the presence of plainclothes NIS officers on the premises of the operators.[104]

These malpractices continue despite the various restrictions in laws such as the Computer Misuse and Cybercrimes Act, National Intelligence Service Act, Prevention of Terrorism Act, Kenya Information and Communications Act and the Kenya Information and Communications (Consumer Protection) Regulations.

Targeting of Human Rights Defenders

Section 3 of Prevention of Terrorism Act 2012, establishes the procedure for declaring entities as "specified entities".

It requires the Inspector General, where there are reasonable grounds to believe that an individual or entity has committed, attempted, or facilitated a terrorist act, or acted on behalf of, at the direction of, or in association with a terrorist, to recommend to the Cabinet Secretary to declare such an entity as a specified entity by publishing an order in the Gazette.

The provision where abused or arbitrarily applied can have a significant impact on the work of human rights defenders, as it lacks adequate oversight or accountability mechanism.

101. Freedom of the Net 2020 https://freedomhouse.org/country/kenya/freedom-net/2020

102. Geoffrey Andare v Attorney General & 2 others (2016), eKLR in this matter the court declared section 29 of the Kenya Information and Communication Act unconstitutional on grounds of the use of ambiguous terms such as "grossly offensive"

103. Abdulmalik Sugow, The Right to be Wrong: Examining the (Im) possibilities of Regulating Fake News while Preserving the Freedom of Expression in Kenya, https://press.strathmore.edu/uploads/journals/strathmore-law-review/SLR4/The%20Right%20to%20be%20Wrong.pdf

104. Privacy International, Track, Capture, Kill https://privacyinternational.org/sites/default/files/2017-10/track_capture_final.pdf

This provision has previously been abused to target human rights organisations Haki Africa and Muslim for Human Rights (MUHURI). In April 2015, the two organisations filed a case[105] challenging their inclusion by the Inspector General of Police in a list of entities to be designated as specified entities under the Act.

This gazette notice was issued without allowing the entities the opportunity to demonstrate that they should not be declared as specified entities contrary to section 3(2) of the Act.

The court, while recognizing the importance of national security, and the history of terrorist attacks in Kenya, agreed with the petitioners' arguments that the respondents had infringed on their right to fair administrative action under Article 47 of the Constitution when they failed to follow procedures set out in the Act.

The court held that the fight against terrorism needed to be conducted in strict adherence to the letter and spirit of the Constitution and the law.

Violation of constitutional standards

The Security Laws (Amendment) Act, 2014 (SLAA) is an omnibus law which was hastily debated and adopted in response to the Westgate attack and introduced numerous problematic amendments with far-reaching implications to the POTA, the Penal Code, and the NIS Act.

Section 12 amended the Penal Code by introducing a new section 66A which prohibited the publishing of any "insulting, threatening, or inciting material or images of dead or injured persons" which were likely to cause fear and alarm to the general public or disturb public peace.

Section 16 introduced a new section 42A of the Criminal Procedure Code to allow the prosecution to withhold evidence "immediately" before the hearing of a case under select statutes.[106]

Sections 20 of SLAA amended section 364 of the Code by introducing an automatic 14-day stay of bail where the Director of Public Prosecutions indicated an intention to apply for a review of the bail order issued by a subordinate court.

Sections 26 of SLAA introduced 20A of the Evidence Act which permitted the admissibility of statements made to an accused person even where the person remained silent.

Section 95 introduced a new section 95(a) to the NPS Act creating a National Police Service Disciplinary Board. Section 64 of the Act prohibited the broadcasting of information which undermined investigations or security operations relating to terrorism without authorisation from the police. Several stakeholders objected to the bill, citing its unconstitutionality.

The High Court in response to a case filed by the opposition Coalition for Reform and Democracy (CORD), found these sections together with sections 12, 16, 20, 26, 34, 48, 64 and 95 of the Act unconstitutional for violating various provisions of the constitution and protected rights such as freedom of expression, freedom of media, and the rights of accused persons.[107]

It is worth noting that in recent years, courts

105. Muslims for Human Rights (MUHURI) & another v Inspector-General of Police & 5 others [2015] eKLR http://kenyalaw.org/caselaw/cases/view/116382/

106. Prevention of Terrorism Act, Narcotic Drugs and Psychotropic Substances (Control) Act, the Prevention of Organized Crime and Anti-Money Laundering Act and the Counter-Trafficking in Persons Act

107. Petition No. 628 of 2014 https://www.klrc.go.ke/images/images/downloads/SLAA-ruling.pdf

appear to be amenable to granting extended pre-detention periods upon application by the Director of Public Prosecutions.

For example, Paul Mackenzie a suspected cult leader who was arrested together with 94 others over the deaths of more than 400 people in what has been dubbed the "Shakahola forest massacre", has been in pre-trial detention since their arrest in April 2023.[108]

Prosecutors announced in January 2024 that the group would be charged with various offences including murder and terrorism, and their detention would continue pending mental health evaluations.[109]

2.6 Weak Oversight of State Surveillance Practices

Kenya has established various oversight bodies with various mandates including monitoring, investigating and reporting on the observance of human rights in the republic, including observance by the national security organs.

However, these bodies face numerous challenges that effectively limit their ability and effectiveness to discharge their oversight roles.

Instructively, key institutions such as the Kenya National Commission on Human Rights, the Independent Police Oversight Authority, the Internal Affairs Unit of the National Police Service, the Office of the Data Protection Commissioner and the Judiciary are plagued by a constant lack of adequate financial, human resources and technical resources necessary to enable them effectively discharge their mandates and hold state security agencies accountable for human rights abuses and violations.

The National Intelligence Service Act establishes under Part VII oversight mechanisms such as the National Intelligence Service Council, Parliamentary Oversight and the Intelligence Service Complaints Board.

Notably, the Board which is required to investigate and receive complaints against officers is yet to be established a decade after the law came into force.

In 2018, Katiba Institute sued the government[110] for its failure, neglect or refusal to establish and operationalize the Intelligence Service Complaints Board.

The High Court declared the failure unconstitutional and ordered the establishment and operationalization of the Intelligence Service Complaints Board within 180 days from the date of the judgment.

Despite the court order, the Board is yet to be established, signalling the lack of political will to ensure oversight of intelligence operations.

In addition, there is limited transparency and accountability in the actions of state security agencies on the nature and extent of their surveillance activities, including in the context of counter-terrorism operations.

For example, whereas the Kenya Defence Forces have been taking an active role in the fight against terrorism, their surveillance activities remain largely opaque and shielded from the scrutiny of oversight bodies.

108. Kenya cult leader Paul Mackenzie faces terror charges over mass deaths https://www.bbc.com/news/world-africa-67992038;
109. Kenya cult leader charged with 'terrorism' over starvation deaths https://www.aljazeera.com/news/2024/1/18/kenya-cult-leader-charged-with-terrorism-over-starvation-deaths; Kenya to charge Shakahola cult leader, members with murder, terrorism https://www.theeastafrican.co.ke/tea/news/east-africa/kenya-to-charge-shakahola-cult-leader-murder-terrorism-4493616
110. Katiba Institute v Attorney General & 3 others; Kenya National Commission on Human Rights (Interested Party) [2019] eKLR http://kenyalaw.org/caselaw/cases/view/186822/

As a result, and in the absence of a reporting requirement, as is required of NIS to Parliament, it is difficult for the other oversight bodies to effectively monitor, or access critical information to discharge their functions. Likewise, reports made to Parliamentary Committees are not always made public.

Moreover, gaps in the legal framework that exempt security agencies from accountability and give oversight mechanisms limited authority over the agencies make it difficult to hold agencies accountable for any human rights violations.

In addition, these oversight institutions lack financial, decisional and administrative independence and are often subject to political interference. Also, the lack of public awareness of privacy rights means that few are aware of their rights, and do not report privacy breaches or challenge communication interception and surveillance orders.

Lastly, there are also few civil society organisations working on counter-terrorism. Some do notable work, but they cannot effectively challenge the use of surveillance laws, technologies and techniques that are used to curtail civil liberties, given threats in the civic space, financial limitations and technical capacity gaps.

Moreover, the government's repressive actions against Haki Africa and MUHURI could likely have had a chill effect on individuals and organisations seeking accountability in terrorism operations. Thus, as some have observed, this led to a reluctance to engage in political topics.[111]

Further, civil society has been weakened by the unfavourable environment and the lack of access to independent funding. Notably, some of the funders supporting civil society work have in recent years tended to support efforts directed at countering violent extremism rather than actions targeting human rights accountability in terrorism operations.

some of the funders supporting civil society work have in recent years tended to support efforts directed at countering violent extremism rather than actions targeting human rights accountability in terrorism operations

111. Civil Society and the War on Terror in East Africa https://www.kas.de/c/document_library/get_file?uuid=4cc019d1-cb67-0732-2e84-296604121c9d&groupId=280229

3.0 Case Studies: Enablers of Digital Surveillance

3.1 Communication and Interception Programmes

While it is publicly known that Kenyan state security agencies, including the military, conduct communication interception and surveillance, the details, nature, extent and capacity are not publicly reported on or disclosed.

However, there is evidence that they have in their possession, a variety of invasive technologies and techniques to monitor, intercept and store communications and surveil the activities of individuals and groups suspected of terrorism and other criminal activities.

The monitoring covers telephone calls, short message services (SMS), and internet activities, including the use of spyware to monitor computers and mobile devices.

A 2013 research conducted by the Citizen Lab of the University of Toronto discovered the installation of 61 Blue Coat ProxySG devices and 316 PacketShaper appliances on public and government networks in several countries including Kenya.[112]

ProxySG devices can categorise web pages to permit filtering of unwanted content, while PacketShaper can establish visibility of over 600 web applications and control undesirable traffic. Collectively, they can provide real-time network intelligence service by filtering application traffic by content categories.

The research raised concerns that the technologies could be used to permit filters, surveillance and censorship.

In 2014, The Intercept[113] reported that a classified programme of the US National Security Agency (NSA) called SOMALGET, which is part of a broader programme called MYSTIC was used to secretly monitor, intercept, collect and record metadata and content of phone conversations from multiple countries including Kenya, as part of its counterterrorism operations.

Information about the system was revealed following leaked documents released by whistle-blower, Edward Snowden.

According to the report, MYSTIC is capable of scraping mobile networks for "metadata" of calls while SOMALGET enables the collection and storage of the actual audio content of every conversation in an entire country.

The data gathered through it has been used to generate intelligence reports.

112. Citizen Lab, Planet Blue Coat Mapping Global Censorship and Surveillance Tools, 15 January 2013 https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/

113. The NSA is recording every cell phone call in Bahamas https://theintercept.com/2014/05/19/data-pirates-caribbean-nsa-recording-every-cell-phone-call-bahamas/

The report states that "the operation in Kenya is 'sponsored' by the CIA, and collects 'GSM metadata with the potential for content at a later date'." [114]

The internal documents describe MYSTIC as a "program for embedded collection systems overtly installed on target networks, predominantly for the collection and processing of wireless/mobile communications networks."

According to the Washington Post, the MYSTIC, which was developed in 2009, could record and store an entire nation's phone traffic for 30 days and was approved to gather intelligence related to terrorism-related information under President Obama.[115]

Foreign surveillance in the US is conducted under Executive Order 12333[116] and is according to experts, not entirely regulated under the Foreign Intelligence Surveillance Act.

Moreover, it is unclear what - if any - role the government of Kenya, as well as telecommunication and communication providers, played in the deployment of and continued operation of MYSTIC in counterterrorism operations.

In 2015, a Citizen Lab study revealed that Kenya and 32 other governments were likely users of the FinFisher, based on the presence of a FinFisher master at an Internet-Protocol (IP) address (46.23.73.xxx and 197.254.122.xxx) registered to a Kenyan user named "National Security Intelligence."[117]

FinFisher is a complex spyware suite comprising FinSpy Master and FinSpy Relays sold exclusively to governments for intelligence and lawful interception purposes.

FinSpy Master is a command-and-control server installed in an agency's premises, while the FinSpy Relays are anonymising proxies located in other countries used to obscure the location of the Master.

Hence, an infected device communicates with the proxy via a Virtual Private Network to the Master, while facilitating access to agents who have back-end access to information from the Master.

In March 2022, the German surveillance software vendor FinFisher GmBH shut down operations and filed for insolvency after years of civil society advocacy against its operations.[118]

Likewise, in 2018, the Citizen Lab found suspected NSO Pegasus infections in Kenya and 45 other countries, where operators of NSO Group's Pegasus spyware may have been conducting operations.[119]

The study found five operators focusing on Africa, with infections in Kenya potentially used for political targeting. Pegasus is a mobile phone spyware suite that is used to monitor a target who is sent a specially crafted exploit link, which when clicked, delivers an avalanche of zero-day exploits that penetrate a phone's security features to install the software without the knowledge or permission of the user.

To avoid detection, the links impersonate typical domain names and show the user decoy landing pages of popular online services, banks, or government services that are linked to cloud-based virtual private servers which redirect the traffic and data to the Pegasus servers.

114. SSO Dictionary Excerpt https://theintercept.com/document/2014/05/19/sso-dictionary-excerpt/

115. NSA surveillance program reaches 'into the past' to retrieve, replay phone calls http://www.washingtonpost.com/world/national-security/nsa-surveillance-program-reaches-into-the-past-to-retrieve-replay-phone-calls/2014/03/18/226d2646-ade9-11e3-a49e-76adc9210f19_story.html

116. Executive Order 12333 https://www.archives.gov/federal-register/codification/executive-order/12333.html

117. Pay No Attention to the Server Behind the Proxy https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/

118. Victory! FinFisher shuts down https://www.accessnow.org/press-release/finfisher-shuts-down/

119. Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

Once installed, the software contacts its command-and-control server and can take instructions from an operator and collect and send back data from the target's phone.

The software grants unrestricted access to a target's device including to its device settings, passwords, stored files, location, phone contacts, calendar events, browser history, emails, text messages, live voice calls, microphone, camera, and photos and screenshots.[120] In 2021, the US blacklisted the NSO Group.

In 2017, the NIS, Directorate of Military Intelligence (DMI) and DDCI were reported to have devices and systems with the capacity to conduct phone call interception, triangulate users' locations and jam network signals.

Both NIS and DMI used International Mobile Subscriber Identity (IMSI) catchers or Stingrays, which are surveillance devices used to intercept and track mobile communications by mimicking or impersonating legitimate cell towers, intercepting communications through the connected devices, tracking and identifying connected devices and thereby tracking the location and movements of targeted individuals.

Further, the NIS technical team also operates Base Transmission Stations (BTS) in Nairobi and North Eastern areas to facilitate the interception of calls and geo-location using GPS or satellite technologies.[121]

Some of the reported technologies in use include Blackbird, a signal search, collection, geolocation, and analysis system developed by SPX, an American spectrum monitoring company.

It is a powerful tool that can be used to identify and track a wide variety of signals, such as radio, radar, and satellite signals. Blackbird can also be used to geolocate signals to track the movement of people or objects.

Another is Verint's Engage GI2, a portable, tactical cellular monitoring and management system that enables law enforcement agencies and military forces to identify, intercept, track, manipulate, and locate targets' mobile phones during everyday operations.[122]

The Engage GI2 system acts as a GSM or UMTS (3G) base station, allowing users to remotely block and control target cellular communications, intercept outgoing and incoming calls and SMS, including A5/1 encrypted networks, and locate cellular phones on GSM and UMTS (3G) networks.

The system is also flexible enough to be deployed in a variety of settings, including vehicles, fixed sites, and aircraft.

In October 2022, it emerged that the National Security Advisory Committee (NSAC) had in 2019 blocked the planned merger of Telkom Kenya and Airtel Networks on the grounds that it created a risk to national security.[123]

In October 2022, it emerged that the National Security Advisory Committee (NSAC) had in 2019 blocked the planned merger of Telkom Kenya and Airtel Networks on the grounds that it created a risk to national security

120. Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229

121. Privacy International, Track, Capture, Kill: Inside Communications Surveillance and Counterterrorism in Kenya https://privacyinternational.org/sites/default/files/2017-10/track_capture_final.pdf

122. Tactical Off-Air Intelligence Solutions https://www.documentcloud.org/documents/885760-1278-verint-product-list-engage-gi2-engage-pi2

123. Revealed: How NIS stopped planned merger of Telkom Kenya and Airtel https://nation.africa/kenya/business/revealed-how-nis-stopped-planned-merger-of-telkom-kenya-and-airtel-3979420

According to the report, the merger would have rendered government communication vulnerable to interception as the current communication architecture did not exclusively demarcate government security communication infrastructure from the rest of the network.

In 2023, the National Treasury acquired a 60% stake in Telkom Kenya to prevent spying on KDF and NIS communications through exclusive access to phone and data networks.[124]

The report revealed that the two organs were building new telecommunications infrastructure thus the acquisition was justified on grounds of national security. These reports confirm access by security agencies to the country's telecommunications network.

Investigations using OONI Probe by the Centre for Intellectual Property and Information Technology Law (CIPIT) in 2017 revealed that Safaricom Plc, Kenya's largest telecommunications provider had a middlebox, a software tool which enables deep packet inspection of origin, destination and content of data packets, installed on its cellular network.[125]

Recent data on OONI Explorer[126] also show anomalies in the access to some websites, Signal Messenger, and circumvention tools such as Tor and Tor Snowflake Test which indicates potential restrictions to accessing some sites, albeit quite minor. These indicate potential censorship of certain content and websites online.

A report by Citizen Lab in 2020 also revealed that Kenya and 24 other countries were likely customers of Circles, a surveillance firm affiliated with the Israeli-based NSO Group, which developed the Pegasus spyware.[127]

It found that Kenya had a single system geo-located at an IP address (41.72.215.226 – 228) belonging to Telco Kali Rainbow. According to the Citizen Lab, the Circles system exploits Signalling System 7 (SS7)[128] vulnerabilities and weaknesses in the global phone system to snoop on phone calls and text messages and track the location of phones around the world.

Customers, who are exclusively states, can purchase a system, which they connect to local telecommunications companies' infrastructure or "Circles Cloud" which interconnects with telcos across the world.

The DCI operates a Digital Forensic Laboratory[129] whose overall function is to identify, seize, acquire and analyse all electronic devices related to all cyber-enabled offences reported and collect digital evidence for use in court for prosecution purposes.

The laboratory carries out malware analysis and computer and mobile device forensics. Thus, it can retrieve data from devices including messages, call logs, browser history, and any deleted data from the device storage and removable drives.

The DCI operates a Digital Forensic Laboratory whose overall function is to identify, seize, acquire and analyse all electronic devices related to all cyber-enabled offences reported and collect digital evidence for use in court for prosecution purposes.

124. Treasury bought Telkom to avoid spying on NIS, military https://www.businessdailyafrica.com/bd/economy/treasury-bought-telkom-to-avoid-spying-on-nis-military--4186552
125. Centre for Intellectual Property and Information Technology Law, Safaricom and Internet Traffic Tampering, March 2017, https://blog.cipit.org/wp-content/uploads/2017/03/Final-March-Brief-pages.pdf
126. Kenya https://explorer.ooni.org/country/KE?since=2023-04-15&until=2023-05-15
127. Running in Circles: Uncovering the Clients of Cyberespionage Firm Circles https://citizenlab.ca/2020/12/running-in-circles-uncovering-the-clients-of-cyberespionage-firm-circles/
128. A protocol suite developed for exchanging information and routing phone calls between different wireline telecommunications companies, and is used to handle roaming services.
129. Digital Forensic Laboratory https://www.cid.go.ke/index.php/sections/forensic-sections/cyber-crime.html

The Computer Incident Response Team carries out network forensics, investigates email and social media, tracks email and messages, SIM-card analysis, and conducts e-discovery and recovery of data from server and network database systems.

The global commercial spyware industry is growing, and the acquisition and use by state agencies of spyware and related surveillance technologies and tools, if not checked, can be used to target civil society, opposition, journalists and human rights defenders.[130] Indeed, a 2021 report by the Defenders Coalition in Kenya highlighted concerns by 56 human rights defenders about the real and perceived threat of their mobile phones being tapped and their communication intercepted.[131]

Such experiences have a chilling effect on the exercise of their rights and freedoms by leading to self-censorship and behaviour changes that ultimately undermine their ability to carry out their work.

Further, the UN Special Rapporteur on the Promotion and Protection of Human Rights and Fundamental Freedoms while Countering Terrorism, while recognizing the need to counter terrorism stated that bulk access to communication and content data without prior consent, amounts to a systematic interference with the right to privacy of communications and requires a corresponding compelling justification.[132]

3.2 Mass Data Collection Programmes

This section highlights some of the ongoing mass data collection programmes currently being implemented in Kenya.

3.2.1 Maisha Namba (NIIMS)

The Kenyan government introduced the National Integrated Identity Management System (NIIMS) through the Statute Law (Miscellaneous Amendment) Act No. 18 of 2018 in January 2019.

The amendments to the Registration of Persons Act established NIIMS as a database containing the personal information of all Kenyan citizens and foreigners residing in Kenya. The system assigns a unique national identification number, previously known as Huduma Namba (Service Number), to every registered person.

The government required Kenyan citizens and foreign nationals to provide sensitive personal information through a nationwide mass biometric registration exercise that started in March 2019 to create the NIIMS database.

In late 2022, the government tabled before the National Assembly its budget statement proposing a reduction of 84 per cent from the KES 680 million allocated for the controversial digital ID system that sought to consolidate all the primary data on Kenyans into a single database.[133]

Initially, registration for Huduma Namba was compulsory and accompanied by threats of denial of access to government services after 12 December 2021.

However, in late 2019, three petitions were filed in the Kenyan High Court challenging various aspects of NIIMS, with one of the main arguments being that the unregulated collection and processing of personal and biometric data in the absence of a national data protection law posed a threat to fundamental rights.

130. *Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses* https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229

131. *Defenders Coalition: Impact of Communication Surveillance on HRDs in Kenya* https://privacyinternational.org/report/4469/defenders-coalition-impact-communication-surveillance-hrds-kenya

132. *Martin Sheinin, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, U.N. Doc. No. A/HRC/13/37, 28 Dec. 2009, p. 13, para. 33,* https://www2.ohchr.org/english/bodies/hrcouncil/docs/13session/a-hrc-13-37.pdf.

133. *Huduma Namba drive suffers setback with 84pc budget cut* https://www.businessdailyafrica.com/bd/economy/ruto-signals-end-of-huduma-namba-with-84pc-budget-cut--4132352

The court agreed with the petitioners and ruled in January 2020 that the collection of DNA and GPS coordinates was intrusive and unnecessary and lacked justification, given the government's inability to process the data for the entire population.

The Nubian Rights Forum had filed an appeal but before it was determined; the Cabinet Secretary for Interior and Coordination of National Government announced the launch of the Huduma card on 18 November 2019.

The Katiba Institute applied to halt the rollout of the card because it was being launched without a data impact assessment, which was required under section 31 of the Data Protection Act.

The High Court, in a 14 October 2021 verdict, ruled that the Data Protection Act applied retrospectively, meaning that the requirement to conduct a data protection impact assessment applied even though the data collection exercise had taken place before the Act came into force.

The Court found that the Data Protection Act was enacted to protect the right to privacy as guaranteed by Article 31 of the Kenyan Constitution. The High Court squashed the government's directive to introduce Huduma Namba cards.

Additionally, it instructed the government to perform a Data Protection Impact Assessment on the effects of data protection under section 31 of the Data Protection Act before processing data or launching the Huduma Namba cards again.[134] A 2021 report revealed that some human rights defenders were apprehensive that data collected under NIIMS could be misused.[135]

In 2022, the government reintroduced the Maisha Namba (Life Number) which includes various components similar to the Huduma Namba system, including a Maisha Namba (Universal Personal Identifier (UPI), Maisha Card, Digital ID and a National Population Master Register.[136]

In February 2023, the UPI concept was cemented as the government planned to launch digital birth and death certificates and require UPI to attend school and to serve as a national ID number.

The Maisha Namba card is expected to replace the current 2nd generation national identity card and the Maisha Namba shall be issued to all new-borns following the nationwide pilot launch in November 2023.[137]

Whereas the government has hopes that the centralised system shall resolve challenges with existing registration processes, including enhancing accuracy and eliminating duplicate records, civil society have raised concerns.[138]

134. *Data Protection Impact Assessments and ID systems: the 2021 Kenyan ruling on Huduma Namba https://privacyinternational.org/news-analysis/4778/data-protection-impact-assessments-and-id-systems-2021-kenyan-ruling-huduma*

135. *Defenders Coalition: Impact of Communication Surveillance on HRDs in Kenya https://privacyinternational.org/report/4469/defenders-coalition-impact-communication-surveillance-hrds-kenya*

136. *What you need to know about Maisha Namba: FAQs https://vellum.co.ke/what-you-need-to-know-about-maisha-namba-faqs/*

137. *Understanding Maisha Namba: Kenya's New Digital Identity System https://www.kictanet.or.ke/understanding-maisha-namba-kenyas-new-digital-identity-system/; Govt Begins Pilot Phase Of Maisha Namba Roll Out https://www.capitalfm.co.ke/news/2023/11/govt-begins-pilot-phase-of-maisha-namba-roll-out/*

138. *Kenya Huduma Namba funding almost entirely cut as UPI, digital birth registration begins https://www.biometricupdate.com/202303/kenya-huduma-namba-funding-almost-entirely-cut-as-upi-digital-birth-registration-begins*

The main concerns raised by civil society in a case filed by Haki Sheria in December 2023 include the lack of public participation in the development of legislation,[139] concerns over privacy and security of the personal data collected under Huduma Namba and the Maisha Namba, potential exclusion and discrimination of marginalised communities who already face barriers in registration.

The High Court in December 2023 temporarily halted the process of introduction of the Maisha Namba following a case by the Katiba Institute which cited the government's lack of a legal basis for the rollout.[140]

The Maisha Namba system has also been introduced in the backdrop of the expansion of government services on eCitizen, the national e-government services online portal, which also consolidates the personal data of all Kenyans.[141]

There are concerns that the triangulation of the information on these systems, coupled with other surveillance apparatus could be abused to facilitate the targeting and surveillance of human rights defenders.

3.2.2 Integrated Public Safety Communication and Surveillance System (IPSCSS)

In May 2012, the government received a grant of USD 100 million (KES 15.8 billion) from the Chinese government for the installation of CCTV cameras in major cities around the country including Nairobi, Mombasa, and Kisumu. [142]

The then Prime Minister Raila Odinga stated in parliament that the CCTV cameras would assist the government to stop terrorism and improve security.

In 2013, the government proposed the use of CCTV cameras in fighting crime and in 2014 contracted Safaricom Plc – the leading telecom service provider in Kenya – to build the Integrated Public Safety Communication and Surveillance System (IPSCSS).[143]

Under the IPSCSS, 1,800 CCTV cameras with face and motor vehicle registration number recognition capabilities were installed in strategic locations in Mombasa and Nairobi.

Also, a command-and-control centre where real-time footage from the CCTV cameras and handheld devices would be relayed; a video conferencing system; the connection of 195 police stations with high-speed internet; the development of a 4G LTE 18 network for the police with 80 base stations; supply of the police with 7,600 radio communication devices with SIM cards and photo and video capability; and linkage of 600 police vehicles to the command-and-control centre.

The project's use of unregulated facial recognition technology without adequate safeguards or independent oversight was highlighted by KICTANet as a breach of the constitutional right to privacy, despite the government's justification that it was important in the fight against terrorism.[144]

139. Registration of Persons (Amendment) Regulations 2023 and the Births and Deaths (Amendment) Regulations 2023

140. High Court puts the brakes on Kindiki's plan to introduce Maisha Namba https://nation.africa/kenya/news/high-court-puts-the-brakes-on-kindiki-s-plan-to-introduce-maisha-namba-4454474

141. eCitizen www.ecitizen.go.ke

142. Chinese Government provides $100 million grant for CCTV Installation Project https://china.aiddata.org/projects/30364/

143. Is surveillance a panacea to Kenya's security threats? https://giswatch.org/sites/default/files/is_surveillance_a_panacea_to_kenyas_security_threats.pdf

144. Ibid, Is surveillance a panacea to Kenya's security threats?

The project's initial cost was KES 14.9 billion (USD 169.6 million), which was expected to rise to KES 18.8 billion (USD 214 million). A further KES 440 million (USD 5 million) would be applied for maintenance and support. In 2014, Huawei, along with Safaricom, installed 1,800 CCTV cameras across downtown Nairobi as part of its 'Safe City' program.

There is little information accessible to the public on how the USD 100 million grant by the Chinese government was used to finance the project carried out by Safaricom.[145]

In August 2021, members of the Nairobi County Assembly(MCAs) proposed a motion that would make it mandatory for all commercial and residential buildings in the city to install CCTVs to help reduce crime in the capital.

The MCAs wanted City Hall and the then Nairobi Metropolitan Services (NMS) to enforce the requirement.[146] The legislators expressed concerns that most CCTV cameras were located inside buildings and only a few are placed in strategic areas for crime detection and prevention.

They also noted that the CCTV cameras outside are primarily used for monitoring traffic, leaving the streets without proper surveillance. They argued that the lack of street cameras had made it easier for criminals to take advantage of unsupervised areas to terrorise members of the public.[147]

The proposed CCTV policy was criticised by Amnesty International for being intrusive and harmful to individuals' privacy rights due to the lack of a data protection mechanism to prevent misuse.

The organisation termed the policy as just part of a larger government plan to establish a police state-like environment that monitors and subjects citizens to government interference.

According to Amnesty International, this plan began with amendments to the registration of birth and death laws, continued with the mandatory Huduma Namba program, and is now being amplified with the ongoing cyber security bill and the newly proposed CCTV policy.[148]

In the aftermath of popular protests instigated by the leader of the opposition leader Raila Odinga in March 2023, the DCI, through its official Twitter account, released photos of alleged protestors.

The protestors were purportedly captured on camera destroying property, attacking innocent citizens, and hurling projectiles at the police.[149] The DCI stated that the persons depicted in the photos would be traced and arrested.

However, independent fact-checkers were able to establish that the photos circulated were fake and in fact, some were from protests in other countries. Following this revelation DCI issued an apology for the "mix-up".

The move by the DCI had two effects; to put protestors on notice of the DCI's ability to surveil protests and to intimidate them from exercising their right to assemble, demonstrate, and picket under Article 37 of the Constitution.

---

145. Chinese Government provides $100 million grant for CCTV Installation Project https://china.aiddata.org/projects/30364/

146. A Policy For Installation Of Closed-circuit Televisions On Commercial And Residential Buildings In The County https://nairobiassembly.go.ke/motion/a-policy-for-installation-of-closed-circuit-televisions-on-commercial-and-residential-buildings-in-the-county/

147. Nairobi MCAs propose CCTV cameras on all buildings https://nairobinews.nation.africa/nairobi-mcas-propose-cctv-cameras-on-all-buildings/

148. How state plots to watch your every move https://www.the-star.co.ke/news/2019-08-16-how-state-plots-to-watch-your-every-move/

149. DCI's Fake Photos of Azimio Protests Exposed by Fact-Checkers https://www.capitalfm.co.ke/news/2023/03/dcis-fake-photos-of-azimio-protests-exposed-by-fact-checkers/

This extensive use of CCTV camera networks raises concerns about mass surveillance and potential profiling of individuals including human rights defenders.

The lack of clear regulation as the draft CCTV policy is yet to be adopted is problematic. These gaps can heighten fear of surveillance and have a chilling effect on the work of human rights defenders.

3.2.3 Mandatory SIM-Card Registration

Kenya has had mandatory SIM-card registration requirements since 2014,[150] which requires telecommunications companies to register subscribers of SIM cards.

Due to gaps in compliance, the Communications Authority (CA) of Kenya ordered mobile phone users to register their SIM cards with their service providers, failing which unregistered cards would be blocked.

The Authority said the exercise was also meant to curb incidences of sim-boxing, financial fraud, kidnapping, and terrorism.[151]

The original deadline for updating the personal details of subscribers was set for April 15, 2022, but the CA extended the deadline to October 15, 2022, after discovering that the mobile operators still had a long way to go to achieve full compliance.

By April 2022, Safaricom, Airtel, and Telkom Kenya had compliance levels of 67%, 55%, and 33%, respectively. The CA was to conduct a detailed compliance audit on each of the operators on the new deadline and impose immediate penalties as stipulated by law for any non-compliance by either the operators or subscribers.[152]

During the exercise, Safaricom was accused of seeking to collect more data than was required under the regulations.[153] In October 2022, a class action suit was filed against the company over the data it sought from subscribers during the SIM card registration process.[154]

In a study conducted by Comparitech[155] on the collection and use of biometric data by countries, Kenya scored poorly. This was largely attributed to concerns about surveillance and disregard for the privacy of sensitive biometric data collected.

155 countries currently implement mandatory SIM card registration across the world. While these efforts are considered an attempt to stop criminals from hiding their identities, there are concerns regarding the abuse of SIM card registration data.

There are concerns that authorities can access call data records and location data to facilitate the targeted surveillance of human rights defenders' movements and communications which could have a chilling effect on their ability to mobilise, speak freely and conduct their work without fear of censorship, intimidation, harassment or violence.

In the absence of strong data protection laws, robust independent oversight, transparency and accountability, SIM card data in centralised government databases could provide a treasure trove of data that can be breached or otherwise misused to target human rights defenders.

---

150. Kenya Information and Communications (Registration of Subscribers of Telecommunications Services) Regulations, 2014 http://kenyalaw.org/kl/fileadmin/pdfdownloads/LegalNotices/2014/LN10_2014.pdf; Kenya Information and Communications (Registration of Telecommunications Services Subscribers) Regulations, 2022 https://ict.go.ke/wp-content/uploads/2022/05/Draft-Kenya-Information-and-Communication-Registration-of-telecommunications-service-subscribers-Regulations-2022.pdf

151. There Is No Crisis, Extend SIM Card Registration To December, DP Ruto Urges Communications Authority https://www.capitalfm.co.ke/news/2022/04/there-is-no-crisis-extend-sim-card-registration-to-december-dp-ruto-urges-communications-authority/

152. Kenya extends SIM registration deadline https://www.commsupdate.com/articles/2022/04/20/kenya-extends-sim-registration-deadline/

153. Safaricom, CA face second class action suit over SIM listing https://www.businessdailyafrica.com/bd/corporate/companies/safaricom-ca-face-second-class-action-suit-over-sim-listing-4016004

154. Safaricom, CA face second class action suit over SIM listing https://www.businessdailyafrica.com/bd/corporate/companies/safaricom-ca-face-second-class-action-suit-over-sim-listing-4016004

155. Biometric data: 100 countries ranked by how they're collecting it and what they're doing with it https://www.comparitech.com/blog/vpn-privacy/biometric-data-study/

3.2.4 Device Management System (DMS)

The Communication Authority published on its website in 2016, a tender document for the supply, installation and maintenance of a Device Management System (DMS).

The DMS, according to the tender document was to be used to: identify all active devices on the public telecommunications networks and isolate illegal communication devices; create and maintain a whitelist of legitimate communication devices; and, ensure that only devices on the white list have access to public telecommunications networks.

This DMS was noted to have significant surveillance capabilities which risk infringing the right to privacy of people in Kenya.

Its implementation was subsequently challenged at the High Court, which initially held that the use of the DMS was inconsistent with the constitutional provisions and that it posed a threat to the right to privacy of the individuals.

It applied the 'analysis' test provided under Article 24 of the Constitution to determine the legality of the DMS. It held that a person's right to privacy entailed control over their personal information and the ability to conduct their personal affairs relatively free from unwanted intrusions.[156]

During the hearing, Safaricom Limited raised privacy concerns, pointing to the fact that their concerns had been raised in meetings with the CA in 2016 and 2017, yet the Authority went ahead to implement them before concerns by stakeholders could be addressed. Counsel also raised concerns surrounding the accessibility of the information by KRA, KEBS and NPS.[157]

The matter was appealed at both the Court of Appeal and the Supreme Court with the Law Society of Kenya (LSK) arguing that the DMS would allow the CA to manage and monitor mobile phone users' devices such as smartphones, tablets, and laptops.

The Supreme Court dismissed the appeal and rendered its judgement in April 2023.[158]

The decision of the Supreme Court paved the way forward for the CA to implement the project, in partnership with the Anti-Counterfeit Agency (ACA), the Kenya Bureau of Standards (KeBS), the Kenya Revenue Authority (KRA), Kenya Industrial Property Institute (KIPI), and the National Police Service (NPS) in the eradication of counterfeit communication devices by analysing IMEI data and use the information to blacklist IMEI of lost, stolen or imported counterfeit devices.[159]

This technology can enable authorities to access all relevant activity logs pertaining to devices and potentially facilitate surveillance and threaten the realisation of civic rights. Currently, there are no clear or published rules relating to how the DMS system will be managed and the data therein be used, which heightens concerns regarding abuse, transparency and safeguards implemented in the system.

---

156. Okiya Omtatah Okoiti v Communication Authority of Kenya & 8 others [2018] eKLR http://kenyalaw.org/caselaw/cases/view/151117/

157. Unpacking the Device Management System (DMS) Judgement https://cipit.strathmore.edu/unpacking-the-device-management-system-dms-judgement-2/

158. Supreme Court Delivers Ruling on Govt's Tech to Track Mobile Phones https://www.kenyans.co.ke/news/88420-supreme-court-delivers-ruling-govts-tech-track-mobile-phones

159. Tender for the Design, Supply, Delivery, Installation, Testing, Commissioning and Maintenance of a Device Management System (DMS) https://www.ca.go.ke/wp-content/uploads/2018/01/Tender-Document-for-Device-Management-System.pdf

3.2.5 COVID-19 Surveillance

Kenya's first case of COVID-19 was confirmed on March 12, 2020, and with it came a new buzzword: contact tracing. For decades, contact tracing has been a cornerstone of public health efforts to combat infectious diseases.

It entails identifying people who could have had contact with an infected individual and systematically gathering further information about these interactions.

According to World Health Organisation (WHO), a person who had direct or person-to-person contact with a confirmed or probable case, often within one metre for a minimum of fifteen minutes with or without the use of personal protective equipment, was described as having had contact in the context of COVID-19.[160]

Immediately after the government declared the presence of COVID in the county, it implemented various public health measures, including asking organisations and businesses to permit their employees to work from home, travel restrictions, closing schools, suspending public gatherings, and a night curfew in a bid to slow the spread of the disease while the nation increased investment in its healthcare systems.

The government developed the Public Health (COVID-19 Restriction of Movement of Persons and Related Measures) Rules 2020,[161] which gave the Cabinet Secretary for Health extensive powers to impose restrictions on people's freedoms and rights, including the right to privacy and the freedoms of assembly and movement, among many others, which were enforced through subsidiary legislation and presidential decrees.

The government also deployed electronic monitoring to keep tabs on individuals on self-quarantine after travelling from outside Kenya. The purpose of the surveillance was to make sure they did not leave their quarantine areas.

Those in self-quarantine were required to specify where they would do so and were forbidden from turning off their electronic devices. People who violated the restrictions on movement were apprehended by law enforcement and medical staff and taken to government-run quarantine facilities.

According to a story in The Standard newspaper, a woman who had travelled from the UK and had vowed to self-quarantine for 14 days and instead went to work[162] was tracked down by security agencies to her office and taken to a government medical facility.

Other people who escaped forced quarantine in designated facilities were also tracked down using their mobile phones.

A 2021 study found that human rights defenders were concerned that data collected by the government and the private sector during the COVID-19 pandemic was not safeguarded.[163]

Another study by ARTICLE 19 Eastern Africa, KICTANet and Pollicy found that legal frameworks and practices adopted during the pandemic enabled an extraordinary surveillance environment.[164]

---

160. Adebisi, Y. A., Rabe, A., & Lucero-Prisno Iii, D. E. (2021). COVID-19 surveillance systems in African countries. Health promotion perspectives, 11(4), 382–392. https://doi.org/10.34172/hpp.2021.49 161. Public Health (Restriction of Movement of Persons and Related Measures) Rules 2020 https://www.icnl.org/covid19tracker/covid19uploads/Kenya%20-%20Public%20Health%20(COVID-19%20Restriction%20of%20Movement%20of%20Persons%20and%20Related%20measures)%20Rules,%202020.pdf

162. Ombati, C. (2020, 24 March). State taps phones of isolated cases. The Standard. https://www.standardmedia.co.ke/nairobi/article/2001365401/state-taps-phones-of-isolated-cases

163. Defenders Coalition: Impact of Communication Surveillance on HRDs in Kenya https://privacyinternational.org/report/4469/defenders-coalition-impact-communication-surveillance-hrds-kenya

164. Unseen Eyes, Unheard Stories Surveillance, data protection, and freedom of expression in Kenya and Uganda during COVID-19 https://www.kictanet.or.ke/?mdocs-file=43606

The report documented various gaps including poor oversight over COVID-19 data collection, lack of independent data protection authorities, disclosure of personal data without consent, use of telecommunication data to track and trace individuals, use of CCTV and biometric technologies to surveil public spaces, broad search and detention powers to medical and public health officers, lack of transparency and accountability of state and non-state actors.

In addition, it highlighted gaps in contact tracing applications including their non-compliance with privacy standards, lack of adequate privacy policies and limited transparency in the relationships between governments and the private sector.

While the pandemic is over, it provided insights into the extent of existing surveillance capabilities, which can also be used to target human rights defenders.

The real-time monitoring of people's movements through their mobile phones is only legally permissible where a warrant has been issued by a court.[165]

However, during the COVID-19 pandemic, this targeted surveillance was normalised.

What is also clear, is that these actions were a perfect testament to the capabilities of the existing surveillance capacity and offer a practical glimpse of how they can be used in counter-terrorism surveillance, including against human rights defenders.

3.3 Social Media Surveillance and Enforcement

The section below highlights some of the ongoing initiatives on social media surveillance programmes being implemented by various government agencies.

Kenya was one of the first countries to officially endorse the Christchurch Call, which is a commitment by governments and tech companies to address the spread of terrorist and extremist content online, initiated by New Zealand following the Christchurch Mosque terrorist attack in New Zealand in March 2019 which was live streamed online. [166]

The Call which has been endorsed by over 130 governments provides a useful mechanism to promote greater transparency and accountability by social media platforms.

However, it presents concerns regarding the vague definition of terms such as "terrorism", "violent extremism" and "harmful content", which could lead to subjective interpretation and inconsistent enforcement through overzealous content moderation by social media platforms thus restricting freedom of speech online. [167]

The call has also been criticised for enabling government overreach and focusing on the removal of content without measures to address the root causes of extremist content online.

165. *Section 52, Computer Misuse and Cybercrimes Act.*
166. *Christchurch Call story* https://www.christchurchcall.com/about/the-christchurch-call-story
167. *The Christchurch Call: The Good, the Not-So-Good, and the Ugly* https://www.eff.org/deeplinks/2019/05/christchurch-call-good-not-so-good-and-ugly

Either way, it is still not clear the overall impact of the call as there is still limited evidence of its effectiveness.

The call aligns with Kenya's implementation of its National Strategy to Counter Violent Extremism 2016 which has a pillar dedicated to media and online. [168]

Specifically, the measures under the pillar include deploying counter-narratives online, sensitising media not to be unwitting transmitters of images or narratives that further the cause of terrorists, engaging the private sector in communications technologies and encouraging citizens to identify and resist extremist speech online.

Kenya has also expressed commitment to the implementation of the UN Global Counterterrorism Strategy and the Plan of Action on Preventing Violent Extremism. In 2019, the country also hosted the UN High-Level Conference on Counter-Terrorism and affirmed its commitment to international cooperation.[169]

The nature of social media surveillance by National Security Organs in the criminal justice sector is not publicly well documented, though it continues. The Kenyan government is reported to have written severally to technology companies such as Meta, Twitter (X) and Google requesting user information for civil, administrative, criminal, and national security purposes.

Accordingly, Google received a total of 48 requests for user information from the government between January 2013 and July 2023.[170] Between January and June 2023, the company provided data in two of three requests made.

Meta received a total of 116 requests for personal data between July 2014 and July 2023.[171] In 2021, the platform received 25 requests relating to 114 user accounts, the highest in the period, of which it provided data in response to 42.5% of the requests.

Further, Twitter (X) received five requests between July and December 2019 but they have never complied with any.[172] Notably, there is limited data of such requests from the X platform from January 2022, following changes on the platform ownership.

---

168. National Strategy to Counter Violent Extremism https://counterterrorism.go.ke/wp-content/uploads/2023/07/National-Strategy-to-Counter-Violent-Extremism-NSCVE-1.pdf

169. Statement by the Kenyan Mission to the UN https://www.un.org/en/ga/sixth/74/pdfs/statements/int_terrorism/kenya.pdf

170. Global requests for user information https://transparencyreport.google.com/user-data/overview?hl=en&user_requests_report_period=series:requests,accounts;authority:KE;time:&lu=user_requests_report_period

171. Government Requests for User Data https://transparency.fb.com/data/government-data-requests/

172. Information Requests https://transparency.twitter.com/en/reports/information-requests.html#2019-jul-dec

In March 2022, Twitter suspended 22 accounts of human rights defenders who were participating in an online campaign dubbed #NjaaRevolution without good reason, an act termed as censorship.[173]

Other government agencies have also undertaken social media surveillance. These include the Kenya Revenue Authority (KRA) which announced it was monitoring social media posts in a bid to enhance tax compliance and nab tax cheats in November 2021.[174]

Similarly, in previous elections, the National Cohesion and Integration Commission (NCIC) partnered with the then Communications Commission of Kenya (CCK)[175] and the Media Council of Kenya to monitor online communications and SMS[176] and filter hate speech and inflammatory content.[177]

Further, the Kenya Film Classification Board (KFCB) also conducts social media monitoring to ensure compliance with its standards for audio-visual content viewed by Kenyan audiences.[178]

A 2022 study by ARTICLE 19 also found that content moderation systems on major social media platforms operating in Kenya were flawed for various reasons.

Some included lack of country-level data, the presence of algorithms amplifying polarising content, the lack of consideration of local context, and the inconsistent application and enforcement of content rules.

This state of affairs makes it difficult to ascertain the nature and extent of harmful or illegal content posted by users from specific countries.

Twitter (X), Meta and Google did not share details on the requests they received. Hence, it is difficult to determine which requests were on information for terrorism investigations and surveillance.

Local intermediaries including internet service providers and telecommunications companies do not publish any transparency reports about the requests for information they receive from government agencies. This lack of transparency and accountability continues despite wide acknowledgement of such requests being made and personal information relating to subscribers provided to investigative and intelligence agencies such as the police and NIS.

173. Country Brief: Overview of recent restrictions to civic freedoms ahead of 2022 elections https://www.civicus.org/documents/KenyaCountryBrief.August2022.pdf

174. Kenyans react after KRA says it's coming for online wealth flaunters https://www.standardmedia.co.ke/national/article/2001428680/kenyans-react-after-kra-says-its-coming-for-online-wealth-flaunters; KRA's strategy on social media surveillance explained https://vellum.co.ke/kras-strategy-on-social-media-surveillance-explained/

175. The Communications Commission of Kenya (CCK) was renamed the Communications Authority of Kenya (CA) in 2014

176. "Four years on, the battle to build a cohesive nation continues", National Cohesion and Integration Commission, 2012, https://cohesion.or.ke/index.php/media-center/press-releases-speeches/115-four-years-on-the-battle-to-build-a-cohesive-nation-continues

177. "CCK issues new rules to curb hate speech in campaigns," The Nation, 24 October 2012, https://nation.africa/kenya/news/politics/CCK-sets-new-rules-to-curb-hate-speech-in-campaigns/1064-1594004-8r0fmm/index.html; "Phone firms block 300,000 hate texts daily, says Ndemo," The Nation, 21 March 2013 https://nation.africa/kenya/news/Phone-firms-block-300-000-hate-texts-daily-says-Ndemo-/1056-1726172-bysv8uz/index.html; Kenya to monitor social media during elections https://www.theeastafrican.co.ke/tea/news/east-africa/kenya-to-monitor-social-media-during-elections-1360384; and Kenya to monitor social media during elections https://www.standardmedia.co.ke/national/article/2001422093/ncic-rolls-out-plan-to-monitor-social-media-ahead-of-2022-polls

178. KFCB Digital Media Monitoring Solution Tender https://kfcb.go.ke/sites/default/files/tenders/2023-01/DIGITAL%20MEDIA%20MONITORING%20SOLUTION%20-%20TERMS%20OF%20REFERENCE_0.pdf

4.0 Conclusion and Recommendations

4.1 Conclusion

In the past two decades, Kenya has witnessed a transformative journey in its efforts to combat terrorism and violent extremism.

The continued terror attacks have led the government through its intelligence and law enforcement agencies to invest in and implement various counter-terrorism strategies ostensibly to safeguard the public and thwart potential terror threats.

However, some of the measures such as communication surveillance and its enabling legislation, pose a grave threat to the work of human rights defenders and civic space, which the measures seek to protect.

This study highlights the historical challenges in the surveillance measures implemented by the government and its intelligence apparatus to combat domestic terrorism and the impact of the measures on human rights defenders.

It also points out the gaps and challenges in the legal and institutional frameworks, including the weak oversight of surveillance operations that facilitate the continuation of human rights abuses, as key concerns.

Moreover, the study shows that the government has in place various infrastructure and mechanisms at its disposal to facilitate surveillance at the national level, including of human rights defenders.

These include various investments in enhancing the communication interception and surveillance capacity of key national security organs, mass data collection programmes and social media surveillance.

The study further observes that these security-oriented measures can and have been used to target human rights defenders and consequently hamper their ability to discharge their mandates.

Extensive surveillance operations aided by vague and repressive laws can create a chilling effect on freedom of expression, information, media, assembly and association and lead to self-censorship as dissent or criticism of government actions could be misconstrued as a sign of radicalization, leading to targeted harassment, intimidation, arbitrary arrests, detention or prosecution.

Further, surveillance operations can be discriminatory and biased to target individuals and groups based on their ethnicity, religion and political beliefs, leading to stigma and silencing of key voices and opinions.

In addition, the conduct of surveillance operations in the absence of robust personal data protection safeguards, limited transparency and accountability, exemptions to national security organs and weak oversight of security and intelligence agencies enables overreach and impunity in the violation of the right to privacy, fuels apprehensions regarding the abuse of the data, and undermines the public trust between citizens and government.

Collectively, the measures profoundly affect civic space as they create an environment of mistrust and fear of retribution, hamper public discourse, civil society activism and democratic participation, and effectively weaken social cohesion and democratic values, which the measures seek to protect.

While ensuring national security, preventing terrorism and countering violent extremism are in the public interest, the response measures adopted should not come at the expense of fundamental rights and freedoms.

Measures such as communication interception and surveillance to combat terrorism should be carefully calibrated to avoid undermining the values they seek to protect.

They should also be targeted, transparent, accountable, and implemented judiciously in line with constitutional edicts and international human rights standards.

Security sector actors must appreciate that civil rights are paramount and essential for the enjoyment of national security and thus, the latter should not be used as a pretext to claw back on human rights or restrict civic space.

In addition, there is a need for open dialogue among all relevant stakeholders to promote the application of human rights standards in counter-terrorism operations.

This will be an essential imperative to build the much-needed public trust and ensure that human rights defenders can flourish while finding appropriate solutions to counter violent extremism that do not compromise our voices, values, liberties and fundamental freedoms.

4.2 Recommendations

The study proposes several recommendations targeted at civil society, government, the private sector, academia and media as outlined below.

Civil society

a) To monitor, document and report on human rights violations by developing reports and research on the abuse of laws and incidents such as arbitrary arrests, detentions, torture and extra-judicial killings of human rights defenders arising from the application of surveillance laws and technologies in counter-terrorism operations.

b) Advocate and demand that the private sector tech companies comply with human rights standards, and expose the companies that are complicit in aiding and abetting unwarranted surveillance by selling equipment and services to government bodies.

c) Conduct public interest litigation to challenge the abuse of and legality of communication surveillance in counter-terrorism operations, seek access to information, and redress on behalf of victims of abuses by security agencies.

d) Lobby legislators and policy-makers to review and amend surveillance policies, laws and practices used in terrorism operations to ensure they incorporate human rights principles.

e) Review and hold the government and non-state actors such as tech security companies accountable for their roles in facilitating human rights abuses during surveillance and counter-terrorism operations.

f) Create public awareness and build the capacity of other non-state actors such as., media and civil society on the impact of communication surveillance including in counter-terrorism operations, by sharing knowledge, experiences and best practices to mitigate emerging risks,

promote privacy rights and defend civic space.

h) Build the capacity of communities and human rights defenders to understand their rights; adopt strategies to defend and protect themselves from abuses by security agencies; identify potential vulnerabilities and threats, risks, technologies and tools used for surveillance; and invest in secure communication tools and practices.

i) Use regional and international human rights accountability mechanisms and platforms such as the African Commission on Human and Peoples' Rights, the Universal Periodic Review (UPR) Process, the UN Human Rights Council and bilateral engagements to highlight the situation in Kenya and put pressure on the government to respect human rights in surveillance and counter-terrorism operations.

j) Build coalitions across sectors at the local, regionally and globally to push back and counter the human rights threats related to communication surveillance, counter-terrorism operations and other unlawful practices geared towards shrinking the civic space.

Government

a) The government should put in place concerted and coordinated efforts to deal with the root causes of radicalisation and terrorism in the country through intentional, integrated and human rights-respecting government policies that also target and address poverty, inequality and discrimination in access to resources and opportunities.

b) Parliament should review and reform Kenya's legal and institutional framework for surveillance including laws such as the Computer Misuse and Cybercrimes Act, Evidence Act, Mutual Legal Assistance Act, Prevention of Terrorism Act, and National Intelligence Service Act to ensure they are consistent with and implemented in line with constitutional and international human rights standards and that they embed principles of transparency and accountability, ensure adequate and independent oversight mechanisms, provide redress mechanisms to victims, and are limited and proportional to control the state surveillance practices.

c) Parliament should amend the Data Protection Act to eliminate the blanket national security exemptions and restrict the use and deployment of biometric mass surveillance. These should also include mandatory due diligence obligations on tech companies facilitating surveillance and putting in place effective and robust enforcement mechanisms with tough sanctions against violators for breaches of such obligations.

d) Parliament should amend the Prevention of Terrorism Act to among others, provide more precise definitions of the terms 'terrorist' and 'terrorism'; revise the procedure the procedure for declaring entities as "specified entities under the to include judicial oversight and an accountability mechanism; and provide for robust oversight, transparency, accountability, remedies and safeguards to prevent its abuse against human rights defenders.

e) Parliament should allocate adequate resources and guarantee in law, the full independence of oversight and regulatory bodies such as the Kenya National Commission on Human Rights, the Independent Police Oversight Authority, the Internal Affairs Unit of the National Police Service, the Office of the Data Protection Commissioner, Intelligence Service Complaints Board and the Judiciary. These should also facilitate capacity building and awareness on privacy standards for relevant officers.

f) Oversight and regulatory bodies should conduct regular privacy audits and assessments to hold accountable operators of national telecommunication networks, mandate carriers,

social media platforms and vendors of surveillance equipment to National Security Organs to ensure they conduct due diligence to identify, disclose, and address their human rights impact, including within their supply chains.

g) Oversight and regulatory bodies should enhance their monitoring, documentation and reporting on privacy rights abuses associated with communication surveillance and emerging violations arising from the use and deployment of digital technologies in the country.

h) The Kenya National Commission on Human Rights, the Independent Police Oversight Authority, and the Internal Affairs Unit of the National Police Service should investigate reported cases of unlawful surveillance of human rights defenders and ensure the culpable persons are held responsible.

i) The Executive should comply with court orders to operationalise the Intelligence Service Complaints Board to enable it to execute its functions.

j) The Cabinet Secretary should develop in a participatory manner the proposed regulations under s. 36A of the Prevention of Terrorism Act, s.70 of the Computer Misuse and Cybercrimes Act, and s. 67 and 80 of the National Intelligence Service Act.

k) The Executive should review the definition of terrorism and national security and outline a policy and guidelines for the implementation of national security considerations and tackling the root causes of terrorism in Kenya and the region.

l) The Executive should collaborate with other stakeholders to facilitate public discourse and awareness on counter-terrorism measures, privacy and surveillance and their impact on civic space.

Private Sector

a) Operators of national telecommunication networks, mandate carriers, social media platforms and vendors of surveillance equipment to National Security Organs should comply with international human rights standards, including the United Nations Guiding Principles on Business and Human Rights and conduct due diligence to identify, disclose, and address their human rights impact, including within their businesses and supply chains.

b) Promote transparency and accountability of state activities by publishing regular transparency reports, supporting public awareness and providing information to oversight bodies and civil society organisations.

c) Develop and implement ethical guidelines and internal policies to ensure their products and services are rights-respecting by design and default. Suppliers of communication devices including manufacturers and telcos should ensure products and services have security features that include end-to-end encryption, firewalls, virtual private networks, two-factor authentication.

d) Provide financial support, technical expertise and other resources to civil society organisations that promote human rights, transparency and accountability around state surveillance activities.

e) Develop and implement privacy policies, safeguards, and remedy mechanisms across their products and services.

f) Demand court orders before sharing customer data, and challenge any arbitrary or illegal information requests from state security agencies that do not comply with the law.

Academia

a) Conduct research communication interception and surveillance and its impact on civic space and counter-terrorism.

b) Highlight gaps in existing surveillance and counter-terrorism laws and practices by security agencies and the extent to which they incorporate human rights principles and their impact on civic space and make recommendations for policy reform.

c) Develop courses targeting law enforcement ~~officials and the public that cover~~ the various human rights standards applicable in communication surveillance and counter-terrorism operations.

e) Share knowledge, experiences, and best practices for promoting privacy rights and defending civic space in Kenya in the context of rising surveillance and counter-terrorism operations.

f) Participate and share expertise in coalitions that advocate for reform, to push back and counter the threats to civic space arising from surveillance practices and counter-terrorism operations.

Media

a) Highlight and raise public awareness among the public by conducting investigative reports, writing articles and opinion pieces that cover human rights abuses by security agencies and private sector actors relating to communication interception and surveillance in counter-terrorism.

b) Highlight gaps in government justifications for communication interception and surveillance by holding government officials to account, exposing inconsistencies in policies, and highlighting abuses.

c) Implement measures to safeguard the security of journalists working on sensitive cases, their sources of information and other whistleblowers.

d) Support local coalitions that seek to push back and counter the threats and practices on communication surveillance and shrinking the civic space.

e) Build the capacity of journalists to understand their rights; adopt strategies to defend and protect themselves from abuses by security agencies; identify potential vulnerabilities and threats, risks, technologies and tools used for surveillance; and invest in secure communication tools and practices; and use the access to information laws to access information held by state agencies.

KICTANet

The Power of Communities

KICTANet.or.ke | Twitter | LinkedIn | Facebook | Instagram | YouTube

KICTANet: Transformed communities through the power of ICTs