Mapping Kenya's Cybersecurity Capacity-Building Needs

Policy Brief

KICTANet
The Power of Communities

www.kictanet.or.ke

GLOBAL PARTNERS DIGITAL

www.gp-digital.org

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

Authors:
Grace Githaiga
Victor Kapiyo

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

Year of publication:
Policy Brief No.16, July 2023

Photo (Title):
www.freepik.com

Table of Contents

1.0 Introduction **1**

1.1 Background and Context. 1

1.2 Methodology 2

2.0 Cybersecurity Capacity-building Needs in Kenya **5**

2.1 Law and Policy 5

2.2 Technical Level 5

2.3 Coordination. 5

2.4 Engagement 6

2.5 Awareness 6

2.6 Additional consideration 6

2.7 Current Good Practice 7

3.0 Challenges **8**

3.1 Financial 8

3.2 Legal and Policy 8

3.3 Social 8

3.4 Technical 9

3.5 Quotes From Participants 10

4.0 Recommendations **11**

4.1 Collaboration between State and Non-state actors 11

4.2 Government 13

4.3 Academia 14

4.4 Civil society 14

4.5 Justice Law & Order Sector 15

4.6 Public 15

4.7 Technical Community 15

4.8 Private Sector 15

4.9 Development Partners 16

1.0 Introduction

This policy brief is informed by the deliberations during the Round table meeting on "Cybersecurity Capacity-Building (CCB) Needs in Kenya" which took place on Friday, 9 December 2022. The meeting was hosted by the Kenya ICT Action Network (KICTANet) in partnership with Global Partners Digital (GPD) with the support of the government of the United Kingdom.

The Kenya ICT Action Network (KICTANet) is a non-profit organisation, which acts as a multi-stakeholder platform for individuals and institutions interested and involved in ICT policy and regulation.

The network aims to act as a catalyst for reform in the ICT sector in support of the national aim of ICT-enabled growth and development.

Global Partners Digital (GPD) is a social purpose company dedicated to fostering a digital environment underpinned by human rights and democratic values.

It works by making policy spaces and processes more open, inclusive, and transparent, and by facilitating strategic, informed, and coordinated engagement in these processes by public interest actors.

The overall objectives of the roundtable were to increase local stakeholder awareness of cybersecurity capacity-building needs and to identify common priorities for Kenya in 2023.

The roundtable was attended by local actors drawn from the government, including key agencies and departments, International Development partners, private sector companies and groups, the technical community, academia, civil society, and other non-governmental actors.

This brief outlines Kenya's cybersecurity capacity-building needs and identifies key recommendations to various stakeholders moving forward.

1.1 Background and Context

The COVID-19 pandemic induced a rapid adoption of ICTs and led to the covid assisted digital transformation (CaDIT) of several organisations in the country, across various sectors including e-commerce, e-health, e-learning, e-government, and entertainment.

The rushed adoption of digital systems while addressing major challenges presented by the pandemic, also presented new cybersecurity threats to users of digital devices.

According to statistics from the Communications Authority, cyber threats recorded in the country have been on the rise since 2020. As shown in the table below, the country recorded 139.9 million cyber threats in 2020, which increased by 242.2% by the end of 2021.

As of September 2022, 450 million cyber threats had been recorded by the Authority in the nine-month period since January 2022. This is almost double the total cyber threats recorded in 2020 and 2021.

More importantly, the significant increase of reported system vulnerabilities by 436% in the past year alone points to potential capacity gaps in securing information systems.

Cyber Threats	2020	2021	2022
Malware	124,168,113	181,888,153	163,880,687
DDOS/Botnet	4,060,899	92,108,268	82,742,427
Web Application Attacks	11,589,947	7,033,604	1,000,284
System Vulnerbilities	114,676	58,045,612	452,412,496
TOTAL	**139,933,634**	**339,075,637**	**700,035,893**

These statistics point to the need for all stakeholders, including the private sector companies and groups, the technical community, academia, civil society groups and other non-governmental actors to pay keen attention to cybersecurity capacity.

Responding to these growing threats means that there is a need for greater investment in cybersecurity capacity building (CCB), to ensure the implementation of rapid, proactive and strategic responses to prevent the rising incidents given the importance of digital systems to Kenya's overall information security, critical infrastructure, democracy, digital economy, and public safety.

Kenya has enacted several policies and laws including the 2020 National ICT Policy, the Kenya National Digital Master Plan 2022-2032, the National Cybersecurity Strategy 2022-2027, the Kenya Information and Communications Act, and the Computer Misuse and Cybercrimes Act, 2018.

The national policies highlight the country's deficiencies in skilled cybersecurity personnel and point to the need to enhance and upgrade institutional capacities, build cybersecurity skills and increase cyber hygiene awareness among the public.

1.2 Methodology

In 2019 KICTANet identified cybersecurity capacity building, awareness creation on cyber hygiene and the development of cybersecurity courses in learning institutions as key priorities, and again in 2022, called upon all stakeholders to develop strategies to address these gaps.

In July 2022, KICTANet participated in the 10th Edition of the Africa School of Internet Governance (AFRISIG) where together with other stakeholders, developed African cybersecurity capacity-building priorities. These priorities were shared with the Open-Ended Working Group on ICTs during the July Session.

Following this, KICTANet convened a stakeholders roundtable meeting on 9 December 2022, where stakeholders drawn from different sectors held discussions on local CCB priorities at the national level. This feedback has now been compiled, analysed and thus informs this brief.

Photo Gallery: Roundtable Meeting

2.0 Cybersecurity Capacity-building Needs in Kenya

Several capacity-building needs were identified straddling several thematic areas. The key ones noted are outlined below:

2.1 Law and Policy

a) The need to develop comprehensive cybersecurity strategies, policies, regulations and diplomacy that emphasize the security of individuals and communities, and that integrate applicable norms, confidence-building measures and international law.

b) Harmonizing legal frameworks and embracing the Malabo convention which Kenya has not yet ratified.

c) Implementation, and monitoring of agreed cyber norms and engaging with the applicability of international law and how to operationalize this in the Kenyan context.

d) Developing, implementing and enhancing data protection and privacy frameworks, in particular, to ensure organisations make the link between data protection and cybersecurity, and implement safeguards.

2.2 Technical Level

a) Protection of Critical Infrastructure (CI) and Critical Information Infrastructure (CII).

b) Preventing and responding to cyber incidents, including through information sharing, minimising risks and mitigating consequences and preparedness within Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) to be able to better predict and mitigate cybersecurity threats. This includes enhanced capacity for effective communication among response teams and between them and other concerned state and non-state actors.

c) Taking into account emerging technologies such as Artificial Intelligence (AI), 5th Generation Mobile Network (5G) and quantum computing, their challenges and capacity needs for the cybersecurity space.

d) Upskilling to cure some of these challenges through certification in data science. For practitioners, regular upskilling would be necessary, and not through an exam but in a forum that would allow them to exchange knowledge, with the immediate need being to get to know the skill gaps.

2.3 Coordination

a) Coordination and collaboration between state and non-state actors, especially in the global South.

b) Transparent feedback reporting mechanisms for all state representatives that attend sub-regional, regional and global engagements in order to institutionalise knowledge and information sharing.

c) Developing Confidence Building Measures (CBMs) in Kenya and African region.
Combating cybercrime including cross-border cooperation and evidence exchange.

e) Ensuring state and non-state actors can engage with one another in a manner that builds trust and confidence.

f) Carrying out substantive national consultations between state and non-state actors in the development and implementation of national cybersecurity positions and strategies.

2.4 Engagement

a) Understanding the opportunities that exist for engagement in multilateral policy processes and how to engage effectively.

b) Understanding the value of multistakeholder and expert-based delegations at the UN and other international cybersecurity and diplomacy processes.

c) Conducting comprehensive national cyber-needs assessments to determine gaps and needs of the different actors and stakeholder groups participating in cybersecurity processes.

2.5 Awareness

a) Increasing knowledge of applicable cybersecurity and human rights norms and standards as well as relevant international human rights instruments, including non-binding norms and standards initiated by industry and civil society.

b) Building capacity for the Police, Office of the Director of Public Prosecutions (ODPP), and Judiciaries, in investigation, prosecution, cross-border issues, digital evidence management, and adjudication of cyber crime cases.

c) Public awareness on appropriate measures for individuals to protect themselves, including cyber hygiene practices.

d) The cyber soldiers game by KE-CIRT is an example of how to enable children to learn the best cyber hygiene practices.

e) Cyber security awareness should be structured, in a way to address the different segments of society and their levels of awareness, in order to allow for targeting of the message for understanding and assimilation. The messaging must contextualise the cyber threats and not generalise.

2.6 Additional considerations

a) Mainstreaming gender responsiveness by increasing the representation of women, adopting gender-responsive policies, and gendered approaches to interventions.

b) Closing the digital divide, particularly for women, Persons living with Disabilities and other marginalised communities drawn from the unserved and underserved areas, rural communities and those living in informal settlements.

c) Developing and implementing reporting measures and mechanisms on cybersecurity incidents so as to enable transparency and access to information such as via publicly available information-sharing mechanisms and accountability.

d) Adequate financial resources to enhance the human resource capacity of institutions responsible for cybersecurity and to meet cybersecurity needs.

e) Kenya has identified cybersecurity as a national and economic security challenge. The NC4 is a coordinating committee which includes the Communications Authority and other actors, and serves as focal point of contact for cybersecurity matters in Kenya.

2.7 Current Good Practice

a) The NC4 is working with vendors such as Huawei, IBM, Microsoft, Cisco, and Juniper to develop an institution of excellence that will facilitate standard setting, inspection and type approval. It is also working with the National Counterfeit Agency to address supply chain issues and gaps.

b) The University of Nairobi developed a cyber security policy from an operational perspective, which gave rise to the development of the information security management system that oversees the whole spectrum of cybersecurity within the university. It also incorporates the Data Protection Act, to ensure that the Institution is operating within the law.

c) Moi University has built capacity on cybersecurity for students through training of students drawn from African countries such as Ethiopia, Ghana, Nigeria, and Togo.

d) Kenya could borrow a leaf from Israel, which inculcates cybersecurity awareness right from the basic level of education. Accordingly, children grow up knowing that they can create applications that could be used by their state. Also, the Israeli government invests in and supports local startups and local innovation.

e) The UK's National Cyber Security Centre (NCSC) set up the Cyber Information Sharing Partnership (CISP) which organises sectorial forums and enables banks and financial services institutions to share information on threats anonymously and seek advice from any other bank that has experienced a similar challenge.

f) The UK has a legal requirement for institutions such as banks to share information when hacked. The NCSC also talks directly to banks and this has created an information-sharing loop. Joining the forum is free even though people are vetted. This is an experience that NC4 can consider as a model among others, as it allows for collaboration instead of competition.

3.0 Challenges

Several challenges that limit and hamper the progress in ensuring cybersecurity in Kenya were identified as follows:

3.1 Financial

a) Cybersecurity is still under-resourced across government institutions and by non-state actors.

b) The government has not been able to match what the private sector is offering professionals.

c) Many students who have studied cybersecurity and graduated have no jobs and are not absorbed by the government given the budgetary constraints.

3.2 Legal and Policy

a) There is a deficit in the legal framework due to a limited understanding of evidence collection of cybercrime for investigators, prosecutors and judges.

b) There is a gap between cyber security and human rights with a limited understanding of how to ensure cybersecurity while also safeguarding human rights.

c) Cyber diplomacy has not yet been prioritised by many African governments, which have lean teams that are not engaging effectively, not working together to develop regional positions and with limited capacity to negotiate and engage on priority issues for the continent.

d) The country is yet to put in place a critical information infrastructure (CII) Bill. However, the NC4 has identified the critical infrastructure sectors through a gazette notice.

e) The regulation of the financial sector is fragmented and undertaken through the Central Bank (CBK), SACCO Societies Regulatory Authority (SASRA), Kenya Bankers Association (KBA) and Treasury.

f) These regulators do not collaborate, hence cybersecurity coordination is difficult.
Many law enforcement officers lack an understanding of cyber security issues, hence cannot deal with cybercrime cases when they are reported.

g) Cross-border transfers of personal data is an issue of concern.

h) There is a lack of a unified approach in the implementation of cybersecurity services that would improve governance and collaboration within the cybersecurity framework.

3.3 Social

a) There is a lot of suspicion among actors working in the cybersecurity sector.

b) Stakeholders have a trust deficit in information sharing, and yet this is critical for resilience.

c) Despite the mobile money penetration, women are scared of using digital wallets and mobile money payments, because of disinformation campaigns about cyberspace, e.g., trafficking and cyberbullying.

d) There is a deficiency in cybersecurity skills and capabilities.

e) Awareness of privacy rights is low, which leads to compromises in data handling.

f) Many children accessing their parent's devices at home have no training or awareness on cybersecurity, as their parents and teachers also lack an understanding.

g) The digital divide continues to grow as cyber hygiene messaging is not broken down to a level that members of the public can understand.

h) Cyberbullying and child pornography are on the rise.

i) Youths unless they are absorbed in the market are becoming the new cybercriminals.

3.4 Technical

a) It is difficult for the government to be vendor-neutral due to lack of coordination and effective guidance across ministries, departments and agencies.

b) There is a problem with some devices from China, from the grey market and electronic waste.

c) There is a gender divide when it comes to matters of science technology and mathematics (STEM).

d) The national CERT cannot handle all the cybersecurity issues.

e) There are trust issues as a result of operating on closed systems for a long time and the country should be gravitating towards a hybrid system.

f) In 2017 Moi University trained government agencies such as the Communications Authority, Telecom, Directorate of Criminal Investigations, and the Kenya Police Service but they have not rolled out other programmes.

g) There are a lot of digital literacy programs, internet connectivity and donations in terms of infrastructure e.g., computers being offered to the schools, yet the officials are not equipped to handle cyber security issues or deal with data breaches relating to children's data.

h) Kenya has local talent and homegrown solutions, which it is not being tapped into, as people often purchase solutions from outside Kenya. The country has local vendors who can supply cybersecurity services and solutions.

Quotes From Participants

"South-South cyber capacity building. We were in Ghana a few months ago, and Ghana is doing cybersecurity strategy and policy development in Sierra Leone, and I think Liberia. Kenya could think about trying to get involved with similar efforts in neighbouring countries."

One of the things you learn from looking at different cybersecurity strategies across Africa is that there is no one size fits all kind of model. Every country needs to kind of draft its strategy for its varying contexts.

"What I learned today, and would like to add is to ensure there is full inclusivity, including the people with disabilities. Another thing is more awareness and more advocacy in legislation, especially when evidence does not embrace nuances in cybersecurity. They should look into it in our legislation. Are they adequate? Thank you so much."

"Thank you for this particular workshop, it's our first time taking part in it. But we are truly happy that we have learned a lot of things. And it was great giving us a lot of insight into what we will also borrow from here. We look forward to these initiatives being expanded to a regional level so that we can also prepare for engagement together. Cybersecurity is a global issue. If Kenya itself, and your neighbours are not safe, that would be a weak link where you could have threats coming in. Learning from your experience, here, you are a bit ahead of us and the academia is also a bit well set up and we would benefit in terms of capacity building going forward in the future. Thank you."

Thank you very much. For me, it's two things. Awareness and collaboration cannot be over emphasised. And cyber literacy. For me, cyber literacy means that we need to cascade this kind of conversation down into counties and into villages where exactly we are looking to set up hot spots in 39,000, shopping centres. we also need to break down our language into a language that my grandmother can understand so that they're able to get the gist of this conversation."

"Now that we know what we know, now that we know where the gaps are, what are our next steps? And who are the people responsible for those next steps? We need to sell this awareness in different sectors, then what happens going forward?"

"What I learned today, and would like to add is to ensure there is full inclusivity, including the people with disabilities. Another thing is more awareness and more advocacy in legislation, especially when evidence does not embrace nuances in cybersecurity. They should look into it in our legislation. Are they adequate? Thank you so much."

"My take-home is research. We cannot overstate the importance of research because we can only move forward from our point of knowledge. That is something that we need, to seriously research cybersecurity."

"Now that we know what we know, now that we know where the gaps are, what are our next steps? And who are the people responsible for those next steps? We need to sell this awareness in different sectors,then what happens going forward?"

"We all understand that technology is changing pretty fast. I had a lot of capacity building, I think by the time we finish building this capacity, we will be moving on to something different. We need to move with speed to ensure that we don't play catch up, we can match the game. Mobile and cloud have changed the way work gets done. We no longer have the corporate perimeter that we used to have with firewalls. We now have a situation where we are perimeter-less. We have data flowing from devices, apps, and networks that we own,and those that we don't. This has increased the threat landscape and it's a huge task to be able to secure ourselves. It comes down to creating awareness so that people can be able to protect themselves, that will be a very good starting point. As we do the awareness, we also need to create this awareness that there are free safe tools that can secure you. Thank you so much."

"I hope we are on the internet mailing list. As you are seeing every body saying KICTANet should, KICTANet should…, meaning there is so much responsibility on the organisation. The mailing list is for everyone. If you see any issue, you post on the mailing list, and we discuss and build capacity."

"My take-home is research. We cannot over state the importance of research because we can only move forward from our point of knowledge. That is something that we need, to seriously research cybersecurity."

"Cyber security is everybody's responsibility. As long as you're operating online, you're using a digital gadget, you need to be in these conversations to bring in your voice. Thankyou."

"Thank you. Mine is to improve cybersecurity literacy among people and make sure people know that your data is yours,you don't have to give it out aimlessly."

"Despite having strategies and policies in place, unless your people are aware of the risks, the country is only as secure as your weakest link,which is the human factor."

4.0 Recommendations

This policy brief makes several recommendations for different stakeholders but notes that multi-stakeholder engagement is necessary in order to effectively secure cyberspace and to find the best ways to build cyber security capacity. There is therefore a need to develop both formal and informal mechanisms for sharing information within and across sectors. In addition, Kenya needs to position it self as a continental leader within the cybersecurity space.

The specific recommendations are as follows:

4.1 Collaboration between State and Non-state actors

a) Cooperation with the African Union Commissions Cyber Security Expert Group (AUCSEG), a multi-stake holdergroup of experts that advises the AU on cybersecurity issues and policies.

b) Internet governance capacity building at regional and national levels is provided through Schools of Internet Governance (SIGs) and by technical organisations.

c) Mobilising of financial resources to support capacity building from non-state actors, government agencies and development partners.

d) Development of knowledge products and training materials for community awareness and digital literacy by thetechnical community, civilsociety and business.

e) Supporting the alignment of cyber-related activities by nations and prioritisation by development partners, donor agencies, and other non-state actors in assisting countries to enhance cyber capacity building.

f) Facilitate and participate in the creation of multi-stakeholder spaces at national and continental levels that bring interested stakeholders together to come up with measures to support local and continental capacity-building efforts in cyber security expertise, information-sharing, and training. A good example is the engagement of EACO and AU where the discussions can be scaled to countries.

g) Engage stakeholders in developing strategies, policies and regulations that are relevant and comprehensive.

h) Develop a sustainable frame work for cyber capacity enhancement.

i) Establish peer-to-peer knowledge transfer at innovation hubs, centres of excellence and technoparkstoencouragehomegrown-expertiseinCyberandrelatedareas.

j) Promote awareness at national, regional and international levels of cybersecurity not only as technical security but as a form of societal security.

k) Develop national positions for global processes,such as the OEWG and the AdHoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information andCommunications Technologies for Criminal Purposes.

l) Develop and implement mechanisms for national, sub-regional, regional and continental collaboration between Cyber security Incidents Response Team (CSIRT) or Computer Emergency Response Team (CERT).

m) Spearhead the development of an engagement framework through which-state and non-state actors can exchange and share information, engage, share skills, build capacity and tackle threats.

n) Multistakeholder consultation on cybersecurity strategy and policy that actively influences and shapes not just the national dialogue, but also the regional dialogue.

4.2 Government

a) Review, develop and implement comprehensive national cybersecurity strategies, policies and regulations to enhance the security and stability of cyberspace. Cybersecurity strategies should include a threat assessment, a plan of action, roles and responsibilities assigned across the government, a dedicated funding and resource allocation mechanism, and a regular period for updating the strategy.

b) Prioritise cybersecurity in national budgets to ensure adequate resourcing for cybersecurity capacity development including through integrating cyber hygiene and digital safety and security into standard educational curricula at primary, secondary, and tertiary levels, and in vocational training programmes.

c) Establish sector CSIRTs and CERTs where they are not yet in place.

d) Develop cybersecurity-related standards that address and are accessible to Small Medium and Micro Enterprises (SMMEs). Enhance coordination and collaboration at national, region a land international levels between state and non-state actors , especially within the global South.

e) Enhance resilience of national Critical Infrastructure Protection (CIP) and Critical Information Infrastructure Protection (CIIP) by developing and operationalising national risk mitigation frameworks for identifying national critical assets and sectors.

f) Share resources and expertise nationally, sub-regionally and regionally.

g) Support research, local innovation, and the development of local cyber security skills, and specialised expertise to ensure in-country competitive, cost-effective and tailor-made solutions to fit localneeds ,in formed by sector threats.

h) Ensure KEBS has the capacity to set standards for the ICT supply chain to prevent malware, insecure and end-of-life devices , disposal of e-waste and prevent dumping of electronic waste from affecting people.

i) Encourage use of clean energy and energy efficient and smart devices e.g. lights.

j) Develop a Cybersecurity Information Sharing Act, and frameworks for e-waste management, virtualassets, cloud infrastructure, IoT and emerging technologies.

k) Review the Evidence Act to provide clarity on digital evidence collection and processing.

l) Implementation of the National Public Key Infrastructure.

m) Conduct regular threat assessment and transparency in threat analysis through the publication of statistics on the national cybersecurity threat landscape which are important in building trust.

n) Build the capacity of local innovators on appropriate cybersecurity skills relevant to the market needs, securing intellectual

property rights, ethical practices, entrepreneurship, and not just seeking jobs.

o) Cyber capacity building can help bridge the gap between effective strategy and implementation. This requires building trust between various actors responsible for cybersecurity.

4.3 Academia

a) Develop and share research methodologies for cybersecurity needs and readiness assessments at national, sub-regional and regional levels.

b) Local universities should enhance cybersecurity capacity building through affordable courses and accreditation.

c) Establish local professional certification standards and then accredit the universities and establish Cyber Security Centres of Excellence.

d) There is a need to have primary and secondary school networks in KENET. There needs to be a basic education curriculum on cybersecurity and awareness raising for the public.

e) Build the capacity of women and girls in cyber security.

f) Training and capacity building on cybersecurity should focus on prevention rather than response.

g) Check the quality of the IT systems in all learning institutions to ensure the protection and security of the personal information of students.

h) The support from KENET to both private and public universities should be expanded to colleges, secondary and primary schools to have a common way of monitoring.

i) There is a need to address the fundamentals i.e., human behaviour, ethics and culture in the cybersecurity curriculum.

j) There is a need for more research on the cybersecurity impact of new and emerging technologies and the development of good solutions and practices.

k) International cooperation is key. For example, IBM has collaborated with universities to provide certification for students on cyber security and on IBM QRadar tools.

4.4 Civil society

a) Raise awareness of African and international human rights standards that apply to cybersecurity law, policy, regulation crafting and implementation.

b) Work towards closing the digital divide and the gender digital divide through establishing and sustaining community networks and by building the capacity of women and girls to be engaged in cyber-related activities.

c) Combat gender-based violence online through awareness raising and building digital security skills provided by civil society groups.

d) Interact with the new cybersecurity strategy documents and give input to key processes.

e) Develop programmes to change local mindset that cybersecurity is an area for the security agencies, yet it needs a multi-stakeholder approach.

f) There is a need to include civil society in cybersecurity processes.

g) Continue having vital conversations on cybersecurity bringing stakeholders from

around the world, around the region, and from different sectors in order to adequately secure our cyberspace.

h) Conduct digital security training for journalists and human rights institutions and defenders.

i) Contribute to the development of laws, policies and regulations in the cyber and digital sphere.

4.5 Justice Law & Order Sector

a) Build the capacity of local law enforcement officers in the criminal justice sector across the country, especially on electronic evidence collection, investigation, prosecution, adjudication, seizure of digital assets, and new technologies e.g. crypto, and their impact on cyber crimes.

b) Develop specialised courts on ICT/cyber crimes.

c) There is a need to create an enabling framework and place systems in place to allow the development of sector CERTs.

d) Enhance the capacity and capability of law enforcement agencies through training and provision of adequate resources to enable the agencies tackle cybercrime and child online protection at national, regional and international levels.

4.6 Public

a) Promote cyber hygiene awareness across the board, from the mama mboga to the presidency. Awareness should target the older generation, children, the education sector, parents, and people with disabilities who are the most vulnerable as they are the weakest link.

b) Build awareness of the environmental impact of ICTs, the negative impacts on climate change, the management of e-waste, energy management of devices and the sustainable plans to address the environmental impact of ICTs on the climate crisis.

c) Measure the impact and effectiveness of the awareness messaging, especially downstream.

d) Create public awareness of privacy and data protection, emerging technologies like cryptocurrencies and blockchain and their potential uses and cybersecurity aspects.

e) Create awareness about the roles of the various cybersecurity stakeholders, what they are doing to make cyberspace safe, and how to report and seek remedies when faced with cyber threats.

4.7 Technical Community

a) Conduct and publish technical reports and white papers for example on cyber threat horizon reports on the national cyber status of the country.

b) Provide technical capacity building including digital safety and security training to cultivate cyber resilience.

c) Promote ethical cyber stars and champions through competition events e.g. ICT in girls' gender tech initiatives and mentorship and coaching in order to influence cybersecurity culture and resilience.

4.8 Private Sector

a) Strengthen information sharing within and across various sectors e.g., financial services, energy, manufacturing etc.

b) Encourage energy audits, especially for big corporate organisations.

c) Create awareness and enforce ICTA standards for IT solutions.

d) Collaborate with Universities in the development of training programmes and then absorb those trained.

e) Promote public-private partnerships among sector stakeholders.

4.9 Development Partners

a) Provide support for collaboration to non-state actors in the development of national positions and inputs at regional and global ICT security forums.

b) Enhance resource mobilisation and allocation for cybersecurity capacity building. Support cooperation in the development of cybersecurity strategy and policies.

KICTANet
The Power of Communities

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

KICTANet: Transformed communities through the power of ICTs