POLICY REVIEW

TOWARDS CITIZEN CYBER-HYGIENE IN KENYA

Dr. Katherine W. Getao

May 20, 2022

KICTANet
The Power of Communities
www.kictanet.or.ke

UKaid
from the British people

Imprint

Published by:
Kenya ICT Action Network (KICTANet)
Email: info@kictanet.orke
Web: www.kictanet.or.ke
Twitter: @kictanet

Programme:
United Kingdom - Foreign, Commonwealth and Development Office (FCDO) Digital Access Programme.

Project title:
Enhanced digital inclusion, cybersecurity and Cyber hygiene awareness
through key multiple stakeholder engagement and knowledge exchange in Kenya.

Sponsor:
United Kingdom's Digital Access Program

Authors:
Dr. Katherine W. Getao

Editor:
John Walubengo

Design & Layout:
Stanley K. Murage (stanmuus@gmail.com, Cell:+254 720316292)

Photo (Title):
Photo 1: The-5-Latest-Cyber-Security-Technologies-for-Your-Business./ www.freepik.com
Photo2:Hand-protective-gloves-typing-laptop-keyboard-cyber-crime-protection-data-information-concept_77190-4582.jpgt Photo / www.freepik.com

Location:
Nairobi 2022

Year of publication:
Policy Brief No.11, May 2022

Table of Contents

INTRODUCTION

In recent years, as more business, government and civil applications are accessed through the Internet and private networks, the issue of Cyber-security has become a major concern. Every year financial losses, as well as reputational and social embarrassment, are experienced as a result of antisocial and criminal activity in cyberspace.

Therefore, it has become necessary for both corporates and governments to invest in securing infrastructure, networks, systems and users, as well as creating policies and laws to mitigate the risks posed by the use of technology.

There is sometimes an assumption that if all the technical risks are mitigated, users are safe from risk. However, social engineering and other types of attacks that directly target users of computer systems, mean that users must be sensitized to manage their devices, applications and online activities in order to minimize risks. These practices can broadly be defined using the term Cyber-hygiene.

The focus in the literature has largely been on the use of cyber-hygiene in formal environments such as corporates; however, the widespread use of technology by ordinary users in informal environments means that cyber-hygiene must become the concern of all. Moreover, the environment, applications and the user differ greatly in these informal environments and therefore the practice of cyber-hygiene must be tailored for diverse groups within this broader audience.

In addition, Cyberspace is creating a new domain where cultural norms are not well-defined. Citizens are involved in participating in dialogues and developing media for this new domain, sometimes without appreciating the audience. An example is when Kenyans recently robustly engaged online users in other countries including Nigeria, Uganda and South Africa, after being offended by posts which originated in these respective countries. They described themselves as a "cyber-army" and robustly engaged the users.

The question arises about the protocols that should be adopted in such engagements and the risks involved in such undiplomatic citizen to citizen interactions. Additional issues are the use of these media for anti-social or even terrorist grooming, illegal activities, and improper uses of data which are in contravention of the law. Many users are not aware of legal provisions in cyberspace.

In this policy review paper, we will consider the issue of cyber-hygiene for ordinary users (with special consideration for vulnerable and disadvantaged users) in Kenya, risks and remedies and policy issues that must be addressed to both protect users and better assist them to protect themselves.

2 DEFINITIONS FOR THIS REVIEW

The United States Cybersecurity and Infrastructure Security Agency (CISA) defines Cybersecurity as

> "Cybersecurity is the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information."

Noting that many modern humans rely on some type of technology for work, entertainment, payment and other financial transactions, transportation, health and a variety of other everyday activities.

In Kenya, more than 90% of adults have a mobile device with more than half of these being smartphones. This means that at least half the adult population is vulnerable to cyber-insecurity.

The Government of Kenya, the private sector in Kenya and the Civil Society take formal measures to protect vulnerable citizens, however, it is the premise of this study that citizens have a role in protecting themselves through effective cyber-hygiene.

The global computer security firm, Kaspersky, provides a simple definition of cyber-hygiene as:

> *"Cyber hygiene refers to the steps that users of computers and other devices can take to improve their online security and maintain system health. Cyber hygiene means adopting a security-centric mindset and habits that help individuals and organizations mitigate potential online breaches. A fundamental principle of cyber hygiene is that it becomes part of everyday routine."*

However, given the social and economic importance of ICT to Kenyans, to the extent that they are devoting an increasing proportion of their capital and daily operational expenditures to ICT-related issues, we have adopted a broader definition of cyber-hygiene which encompasses the practices necessary to keep citizen's devices and the applications which they use on those devices useful, available and workable.

This model of Cyber-hygiene is explained in the policy models set out in chapter 4 of this report.

Since this document focuses on policy issues it is also important to define policy for the purposes of this review.

The US Centre for Disease Control and Prevention explains that policy, in the context of Government is:

> *"Policy is a law, regulation, procedure, administrative action, incentive, or voluntary practice of governments and other institutions."*

Anke Hassel defines public policy as:

> *"Public policy is a set of decisions by governments and other political actors to influence, change, or frame a problem or issue that has been recognized as in the political realm by policy makers and/or the wider public."*

This paper will draw on elements of both these definitions, attempting to frame the issue of cyber-hygiene as well as make recommendations for formal adoption by the Government in the form of laws, policies, procedures, incentives and administrative actions.

The last definition that is important for understanding the methodology of this review is the issue of disadvantaged groups.

The European Union thesaurus defines disadvantaged groups as:

> *Groups of persons that experience a higher risk of poverty, social exclusion, discrimination and violence than the general population, including, but not limited to, ethnic minorities, migrants, people with disabilities, isolated elderly people and children."*

Drawing on this definition one could argue that the coherent issues for cyber-hygiene would be digital exclusion (through lack of awareness, skills, devices, bandwidth, appropriate applications, as well as any deliberate administrative actions to exclude certain groups from digital access), digital discrimination and cyber-insecurity!

Chapter 4 of the Constitution of Kenya 2010 sets out the fundamental rights of Kenyan citizens including labour relations, economic and social rights, language and culture, family rights, consumer rights, rights to fair administrative action, access to justice, fair treatment at a time of arrest, a fair hearing, rights when detained, held in custody or imprisoned.

In addition, the rights of certain vulnerable groups are clearly set out and these include children, persons with disabilities, youth, minorities and marginalized groups and older members of society. We could thus argue that these vulnerable groups as well as any person or group of persons who are not enjoying the rights set out in the bill of rights is disadvantaged.

3 Current State of Cyber-Hygiene In Kenya

3.1 The Evolution Of Cyber-Hygiene In Kenya

In the last 40 years the environment in which users of ICT in Kenya operate has changed drastically. In the early 1980s, most people encountered digital devices in the workplace. They belonged to the employer, were operated and managed by specialized staff, and were often standalone in their operation; where there was a network, it also tended to be a private network operated by the employer to connect branches of the same business.

The rare end user who had a device at that time had a "desktop" device used exclusively in the office environment, was largely confined to applications selected by his or her employer and was not responsible for the management or maintenance of any part of the digital environment.

15 years later the Internet was beginning to aggressively enter the advanced corporate and educational environments and the idea of using the Internet infrastructure as a way of publishing corporate systems was already permeating the workplace.

This would empower end-users by making centralized corporate systems more widely available without the need to develop a huge private infrastructure. The "portal" was becoming a major resource for end-users, but it was still formally managed by the institutional owner.

During the following ten years, devices were becoming affordable and mobile in nature. End-users increasingly owned personal digital devices which they used for personal and home-based applications. This introduced a "bring-your-own-device" (BYOD) culture in the workplace because users preferred using their familiar devices rather than turning to legacy devices within the workplace. However, the networks to which they connected these devices were still owned and managed by the institution.

Many institutions made security arrangements that protected the network from the impact of the BYOD devices. Some also developed policies and trained and obliged their end-users to conform to these policies.

Finally, the COVID-19 pandemic moved employees, students and business people from the formal workplace to the home environment. Now a large number of users had to set up their own home networks connected to service providers whom they had individually selected.

With minimal security arrangements provided by the internet service provider (ISP), it was the responsibility of each home to manage its own security. Most corporates procured systems that enabled them to protect their sensitive applications (which were now being regularly accessed from homes and public spaces) by setting up virtual private networks (VPN.) However, there is no doubt that these uncontrolled environments posed new risks to businesses.

It can be noted from this summarized history that:

- The 40-year culture placed the responsibility to take care of information security squarely on institutions, with the few user expectations contained in a brief policy.
- There has been an evolution from institutional computing to end-user computing – in the absence of a similar evolution in the orientation of users.

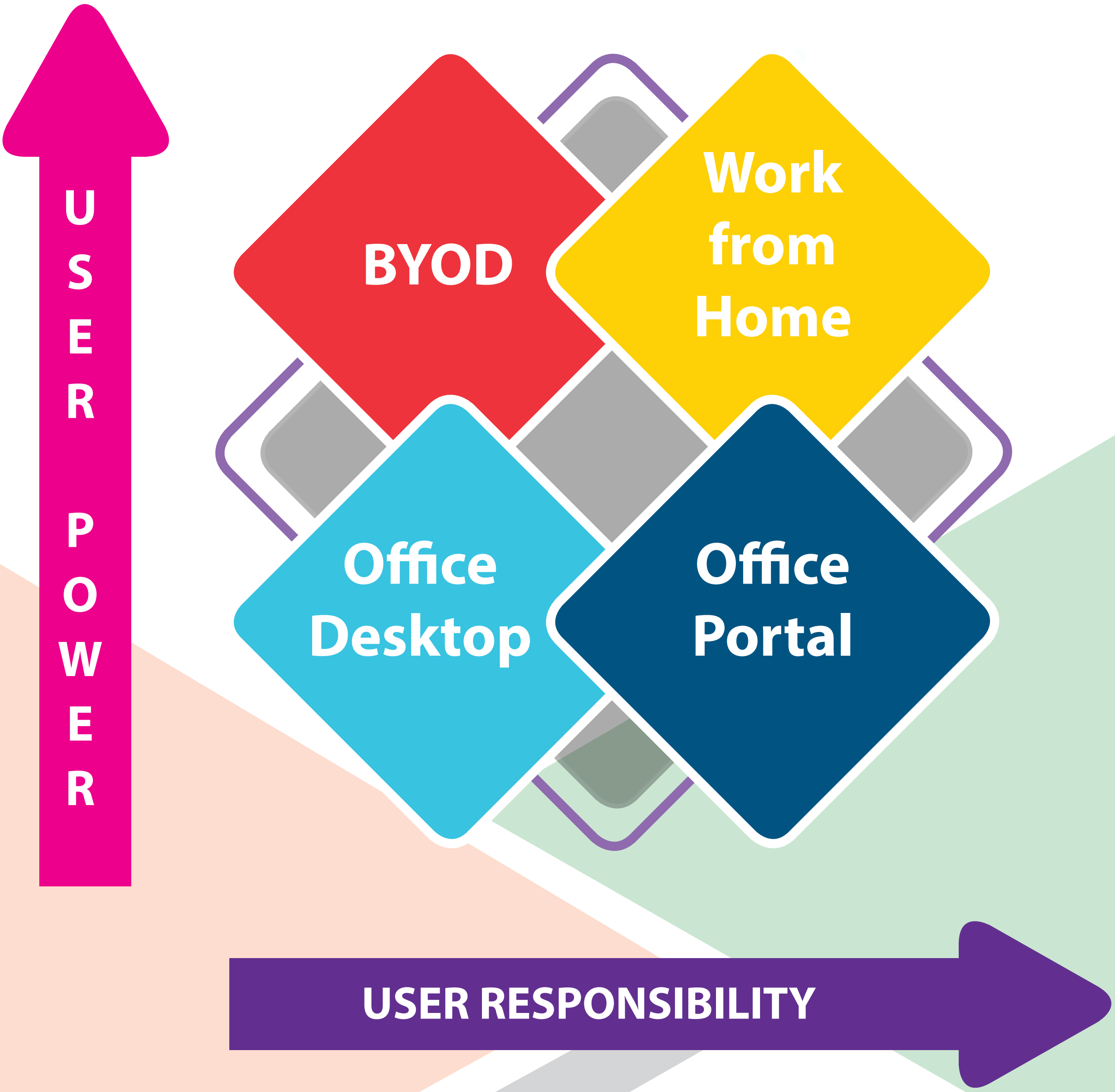

Figure 1: The evolution of the digital environment

So while the end user has never been more empowered in terms of access to technology and the ability to use it in diverse locations, the prevailing culture has not prepared the user to take the level of responsibility required to create a safe and secure computing environment. The empowerment of the user has also created digital divides where disadvantaged and vulnerable users do not have equitable access to technology and skills.

The cyber-hygiene model presented in this paper attempts to define and address this shortfall, especially on effective models of creating a cybersecurity culture among end-users. It is acknowledged that the picture is likely to become far more complex when the use of technology moves from deterministic applications used in home, office and leisure environments to the deployment of intelligent and autonomous mobile technology in society by ordinary users.

3.2 Legal and Policy Environment

3.2.1 Policies and Laws

While computers have been in use in Kenya since the early 1970s, it was not until 1998 when the Kenya Information and Communication Act (KICA), a law largely designed to regulate the telecommunications and related sectors, was passed to deal with some of the issues that were arising as a result of digital technology in society.

The law has undergone a number of revisions the most significant taking place in 2009 and 2015. KICA created the Communications Commission of Kenya (CCK), which later was renamed the Communications Authority (CA) as well as created Kenya's main cybersecurity response team KE-CIRT/CC.

The Act deals with the provision of communication services and has several sections which are of relevance to cyber-hygiene issues such as the registration of SIM Cards and improper uses of telecommunications services. The Act also deals with the issue of electronic transactions. Since the KICA was the first law in this space it has the advantage of covering a broad range of issues such as broadcasting, multimedia, telecommunications, postal services and multimedia.

This could prove to be a boon since there is increasing technology convergence encompassing these domains.

Subsequent to KICA a number of important policies have been developed and laws passed to deal with emerging issues.

Laws covering cyberspace are very important in regulating the use of technology, protecting users, and ensuring that Kenya conforms to international best practices. Existing and emerging laws in this area in Kenya which are relevant to citizen cyber-hygiene include

- Computer Misuse and Cybercrimes Bill 2018
- Data Protection and Privacy Act 2020***
- The Critical Infrastructure Protection Bill
- The Kenya Information and Communication Act
- National Payment System Act (and its regulations and guidelines)
- Health Information Act

Laws take a long time to develop and ratify, so the policy is very important in guiding the use of technology and creating a stable environment for business planning and operations.

Cyber-hygiene could, as a first step, be addressed by updating and developing relevant policies and strategies. Existing policies and strategies include

- The Kenya National ICT Masterplan 2014-2017
- National Cybersecurity Strategy 2014 (currently being updated under the aegis of the National Cybersecurity Command Centre)
- Digital Economy Blueprint 2018

- ICT Policy 2019
- The Draft Kenya National ICT Infrastructure Masterplan 2019-2029 (drafted by the ICT Authority, currently under review)
- The National Broadband Strategy 2018-2023

While these laws and policies provide a good starting point for citizen cyber-hygiene they have a number of weaknesses for example

- Mandate overlap and lack of coherent governance (which hopefully will be mitigated when the National Cybersecurity Coordination Committee becomes fully operational)
- No clear responsibility for the research and advisory element of emerging technology policy
- The broad nature of cyber-hygiene means that some very pertinent issues that affect ordinary citizens fall through the cracks (e.g. the rapid obsolescence of technology that is marketed to low-income groups, the legality of SIM card sharing etc.)
- While the Communications Authority has made good efforts to communicate emerging issues to citizens, many citizens do not know where to take their cybersecurity and cyber-hygiene-related issues
- Some legal requirements that put a substantial burden on organizations and persons to comply with directives which they have little capacity to fulfil. For example, the Data Protection Act obliges data processors to report data breaches or unauthorized access where there is a risk of harm to data subjects within 72 hours. This not only poses a definitional challenge (i.e. “harm”) but the literature reports that the average time taken to discover a breach is over 270 days!
- Issues such as insurance are going to become very important for the mitigation of cybersecurity issues yet the Insurance Act does not deal with the issue of Cybersecurity insurance
- The Mwongozo policy for parastatal boards as well as other public governance instruments for control and training should also urgently deal with these issues if the investments of citizens are to be adequately protected.
- Ordinary citizens may be unaware of the laws and policies so may not adhere to the provisions.
- The process of developing policy and law is slow, and technology adoption and innovation is fast. There is no clear timetable for the monitoring and evaluation of policies and laws being adopted, or for the response timetable for emerging technology. Citizens are thus often exposed to policy and technology that has not been field-tested.
- There needs to be much more robust adoption of stakeholder engagement policies and standards (such as those developed by the Kenya Law Reform Commission) to ensure that the views and issues of citizens, especially disadvantaged and vulnerable groups, are regularly obtained and considered for issues such as Cyber-hygiene.
- It is very important that laws which are in process are appropriately ratified and that regulations, which make it possible to operationalize the laws, are quickly developed and / or updated.

3.2.2 Institutions

Institutions are extremely important for the adoption of policy and the implementation of relevant programmes and activities.

Mandating an institution is important for the success of any policy, however, it must be ensured that the institution is strategically, technically and financially capacitated for success.

The main institutions that have a relevant mandate and/or are directly involved in cybersecurity (and to a lesser extent cyber-hygiene) activities in Kenya

- Ministry of Interior and National Coordination (MINC)
- National Computer and Cybercrimes Coordination Committee
- National Cybersecurity Command Centre (NC3)
- Cyber Crime Unit, Directorate of Criminal Investigation
- Ministry of Information, Communication Technology and Youth Affairs (MoICTYA)
- Communications Authority (CA)
- Kenya National Computer Security Incident Response Team and Coordination Centre (KE-CIRT/CC)
- Information and Technology Authority (ICTA)

3.2.3 Processes

It is clear that cyberspace crosses borders and therefore cyber-hygiene can never be completely successful if its conventions are confined within our national borders.

It is therefore important for Kenya to participate in bilateral, regional and international processes to influence the adoption of appropriate conventions for good cyber-security across the board. For many years Kenya has been integrally involved in important cybersecurity and digital technology activities that are relevant to citizen cyber-hygiene. These include

- The United Nations Group of Governmental Experts on Developments in the Field of Information and Communication in the Context of International Security
- The United Nations Open-ended Working Group Developments in the Field of Information and Communication in the Context of International Security
- Global Forum on Cyber Expertise, Member
- United States of America – Kenya Cyber and Digital Economy Dialogue
- Joint Working Group on Security, India-Kenya
- Cybersecurity Alliance for Mutual Progress – CAMP Initiative, Member
- Kenya – Israel Cooperation
- Memorandum of Understanding, Cyber Security Framework for Cooperation and Collaboration between the Northern Corridor Infrastructure Projects Partner States
- The United Kingdom Digital Access Programme

3.3 Statistics, Citizen Attitudes and Experiences

3.3.1 Case Studies

Cyber-hygiene Case Study 1

The Person: W is a 69-year old retired teacher whose husband is a businessman. She has the latest expensive smartphone with dual SIM and biometric access security functions.

She was recently the victim of a social-engineering attack, during which she lost over Kenya Shillings 120,000/= from scammers who pretended to be agents of her main telecommunications provider checking her SIM registration (there had been a legitimate message from the provider regarding SIM re-registration.)

The scammers later devised a complex theft involving money transfer reversal, registration on money-lending apps followed by maximum borrowing, and finally a SIM swap followed by emptying of her mobile money account. They subsequently accessed and emptied her conventional bank account.

She had not disclosed her PIN therefore there was a suspicion that the scammers tricked her into repeating a phrase used for voice recognition access, which they may have recorded. The victim was able to report the losses to the

telecommunications provider as well as the police and received limited assistance.
She was left traumatized and had lost confidence in technology which she is now hesitant to use.

The Challenge: W was ill-equipped to resist the scammers, discover the scam and report it. The security features on her phone were impotent against the type of scam that she faced.

The Provision: There is a unit at her local police station which is competent to receive cybercrime reports. The telecommunication provider was also able to receive the report and take some action (which later proved to be inadequate since a quarter of the money was lost after the report.)

A month after the attack the bank refunded the money lost and the telco informed her that she was not expected to repay the mobile loans. Both providers informed her that they had assessed her case genuinely because she has a high-risk profile.

The Need: Since social-engineering attacks are common, subscribers need information as well as protective apps.

The providers need to increase security at times when they are carrying out campaigns that can easily be exploited by criminals as well as devise robust responses which immediately stop the scam once it has been reported.

They may also monitor subscriber accounts for suspicious activity. Fintech apps need stronger protection and legislation and consumer protection with limited liability provisions.

Cyber-hygiene Case Study 2

The Person: X is a 30-year-old single man. He graduated from university with an IT degree five years ago and subsequently obtained a good position with a bank, which he lost during the COVID-19 Pandemic.

He has been surviving on his savings and a few system development consultancies. He has hired some premises in a small university town and is preparing to open a cybercafe business. Recently he won a consultancy in a government department.

On New Years he called a senior government official who became suspicious about how the young man had obtained his contact details.

He came to the attention of security officers, and while they were investigating him they associated him with a foreign national who had been arrested for cybercrime. He was subsequently arrested and all his electronic devices confiscated.

He is unable to work without his devices and his business contacts are unable to contact him. He has hired an inexperienced lawyer who is able to give him minimal support and information.

The Challenge: Although X has an IT degree he has very little knowledge or understanding of Cyberlaw including his rights and obligations.

There are few lawyers with sufficient experience to support people charged with cybercrimes. The issue of confiscation of devices upon which people rely for their livelihood has not been thought through.

The Provision: There is a Computer and Cybercrimes Law. There is a unit in the Criminal Investigation Department that investigates such crimes.

The Need: Persons working in IT need a clearer understanding of the laws that govern their sector. Legal professionals also need to be equipped to support clients and processes during such proceedings.

Cyber-hygiene Case Study 3

The Person: Y is a 58-year-old civil servant. She is preparing for her retirement. About 10 years ago she saved up and purchased a high-end desktop computer to use at home.

She also purchased legal copies of a number of software packages to use on the desktop. She made limited use of this equipment over the years because her employer provided her with a laptop and software.

She is now trying to revive her home equipment and has experienced a rude shock. The operating system has become obsolete and was expensive to update since the manufacturer no longer supports the desktop model.

Most browsers will not work with the operating system because of insecurity concerns since it is no longer supported by the manufacturer. The licensed software became impossible to re-install after upgrading the operating system.

The equipment is still in good condition but is almost unusable due to a lack of security and software upgrades for the model. She is realizing that she may have to invest in new equipment and software at a time of life when resources are scarce.

Information Technology is moving from capital expenditure business models and operating expenditure models.

The Challange: This is challenging for people in developing countries who do not have a generous and regular income. Due to competition and technology “innovation”, the support cycle for “outdated” technology is extremely short.

The Provision: Processes such as ISOC exist where these kinds of issues can be raised.

The Need: Since nearly all IT is designed for developed countries it is necessary for developing countries to come together and negotiate more amenable business and support models for their citizens.

Cyber-hygiene Case Study 4

The Person: Z is a 24-year-old school leaver. He did not complete secondary school due to challenges in paying fees and survives through casual, unskilled work.

His cheap, feature phone is a lifeline for contacting potential employers and receiving wages through mobile money. Recently his phone malfunctioned and now he survives by persuading friends and neighbours to temporarily allow him to fit his SIM card in their devices. With his current income level he cannot afford a new phone.

The Challenge: The new arrangement is inconvenient and insecure. The kind of phones that Z can afford are not durable so his TCO may actually be quite high.

The Provision: Although there are mobile loans Z’s options for acquiring a quality handset are limited.

The Need: Low-income persons need secure and durable devices.

Cyber-hygiene Case Study 5

The Person: A is a 28-year-old unemployed and visually-impaired youth. Through a non-governmental organization, he has acquired a laptop with software that enables him to read websites and use open-source applications for visually-impaired people.

A aspires to be a journalist and he has a blog and actively participates in popular social media platforms. However, his greatest aspiration is to write high-quality, well-researched articles that will be considered for publication by conventional newspapers and magazines.

The Challenge: Apart from the cost of bandwidth which puts a strain on his tight budget, A is frustrated that some public sector websites are not implementing disability-friendly standards for their online resources.

This makes it awkward for his programmes to access all the information that he needs from these websites. He is also afraid that, since the cost of disability-friendly hardware is very high, he will not be able to afford a new device if his current one gets lost or becomes outdated.

The Provision: He would like standards to be enforced for all public sector online media, and also thinks that there should be locally-manufactured, affordable, disability-friendly hardware.

The Need: Disabled persons need equal access to all online resources and to affordable equipment.

Cyber-hygiene Case Study 6

The Person: Q is a 40-year old young woman who runs a small but successful non-governmental organization. Although her expertise is in social work she is quite tech-savvy and frequently uses online and mobile resources including GPS navigators.

The Challenge: Recently Q needed to drive to a rural location in Kenya and she was confident that she would be able to easily find the location given that the person she was visiting had provided her with a location pin. She had confidence in a widely-available navigation app, which she uses frequently and successfully in her urban home ground, so she started her journey a little late in the evening.

However, the app led her to outdated roads, some of them which led her through private land. Although she finally arrived at her destination, it was late in the evening and on several occasions, she had felt extremely vulnerable and unsafe. It was clear that the app was not optimised for the local conditions in remote areas.

The Provision: Internationally-developed apps inspire confidence in local users, however, often their language, maps and functionality are not optimised for local conditions.

The Need: Policy and standards for internationally-available applications should ensure that either they frequently update and optimise for the local conditions, or they provide contextual disclaimers to ensure that users are aware of their reduced capabilities in certain conditions.

3.3.2 Statistics

With the rapid global growth in smart user devices which are connected to the Internet, malware infection in devices is growing exponentially with just 12.4 million recorded incidents in 2009 growing to more than a billion in 2020.

By 2018 about 92% of malware was delivered through email but as the number of smart mobile devices increased the number of mobile malware payloads being discovered is doubling every two years.

Since Android operating system devices are the most cost-effective for ordinary users, and development tools for Android devices are readily available (in order to encourage the development of user-friendly applications), it is not surprising that 98% of mobile malware targets Android devices.

Another interesting development is the rapid increase of malware targeting Apple platforms, and conversely a slow decrease in the number of new malware programs targeting Windows platforms.

Ransomware attacks are also increasing exponentially with a 350% increase in 2018 alone. Ransomware attacks are estimated to cost about 6 trillion dollars annually (by 2021) to businesses, with 40% of businesses having paid the demanded ransom.

While malware causes damage to systems and data, and ransomware extorts resources from businesses, other malicious applications such as cryptojacking use system resources without the knowledge of users.

Cryptojacking involves the deposit of a crypto mining algorithm on a user device which then uses the device's memory and processing power to perform calculations necessary to mine crypto coins before passing its results back to the perpetrator of the intrusion.

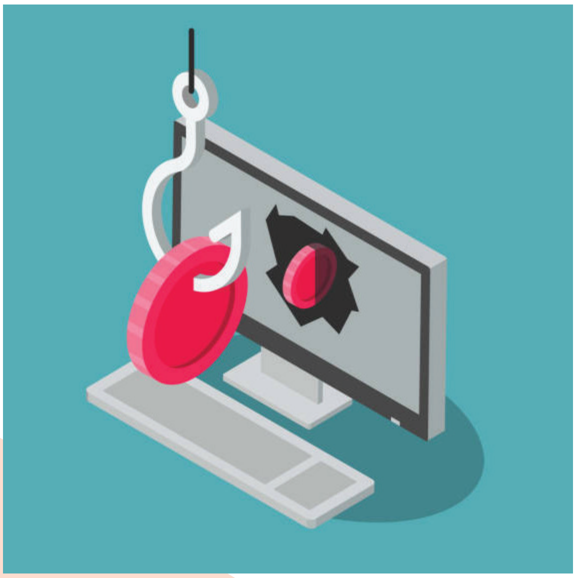

Photo: istockphoto-1141906522-612x612.jpg

While this is an ingenious method of capturing the large amounts of computing power necessary to carry out such calculations, it causes considerable slowing down of the user's machine and applications and also uses bandwidth which many users can ill afford!

As more and more users turn to the convenience of digital currency which relies on cryptography for its implementation it is likely that these types of intrusion to user devices will also be on the rise.

While there are other threats, we will just focus on one more: social engineering schemes. A social engineering scheme uses psychological manipulation to target both naïve and sophisticated users and trick them into performing actions, such as the disclosure of confidential information, that facilitate a variety of malicious cyber activities, for example, unauthorized access to protected data and systems using the credentials of an authorized user. It should be noted that the ability of big data systems to mine demographic and transactional user data to build accurate user profiles is likely to increase the chances that a social engineering attempt will succeed in manipulating a specific user.

A disturbing statistic is that 98% of cyber attacks rely on social engineering for success! In 2021 **43%** of IT professionals contacted reported that they had been the subject of social engineering schemes. Naïve users such as new employees of a firm are thought to be most susceptible to social engineering schemes.

In developed countries, the most common breach facilitated by social engineering schemes is identity theft **(65%)** followed by account access **(17%)** and financial access **(13%)** and general harassment **(4%.)** It is likely that the picture is different in Kenya with the most common motive likely to be financial access (e.g. mobile money theft) however, I have been unable to identify a definitive study.

In 2018, the number of records breached was about **56%** of social media records **(56%)** and 1.2 billion Government records **(27%.)** Such breaches were much less common in the retail, technology and other industries sectors (averaging about **(5%.)** Given the level of vulnerabilities in web-based applications and their supporting databases, it is likely that hackers find it much easier to access such information through Internet-based portals.

Phishing, where users are tricked into following a fraudulent link is common with **30%** of users falling for the ruse, while only **3%** reported the successful attack to authorities (for example, an employer.)

Another issue of concern is cyber-grooming, including cyber-radicalization where an anonymous person or group is able to contact and manipulate a user with the aim of influencing them to adopt antisocial ideas and engage in illegal activities.

Photo: Cyber-Security-Technologies-for-Your-Business./ www.freepik.com

Children and young people are particularly vulnerable to these types of communications which sometimes have disastrous results. The unsuspecting user may fall victim to anything from child pornography rings, antisocial persons who are able to arrange a physical meeting during which they harm the victim, and recruitment to terrorist organisations such as ISIS and Al Shabaab.

It is clear that user naivety juxtaposed with criminal deviousness is creating a dangerous situation where criminal cyber activity succeeds, results in serious losses and embarrassment for companies, government and users and often goes unreported. This is a situation which must obviously be seriously addressed. Cyber-hygiene attempts to mitigate risk by orienting users to practices that facilitate cyber-security.

One elephant in the room is that, as many cybercrimes succeed and few are discovered and prosecuted, an increase in the number of disadvantaged and unemployed youth who have good cybersecurity skills will tempt many of them to turn to cyber-crime as a viable means of making a living.

It is thus necessary to combine training in digital skills with sound, social values as well as make continuous efforts to provide positive opportunities for youth employment in the digital realm.

In the meantime, ordinary citizens have woven technology into the texture of their everyday lives.

3.3.3 Issues and Experiences

Leonard D.K.,1970, countries where local conditions such as livelihoods, culture, income and lifestyles vary greatly need a decentralised approach to the design of incentives and interventions.

This was one of the motivations for devolution in Kenya and there may also be evidence that one-size-fits-all digital cyber-hygiene policy interventions may not be ideal, and some regional or demographic variations may have to be considered.

This view is strengthened by the contention of Jackson R, 1970 that resource-scarce, less-developed environments political and economic concerns are likely to be the main drivers of policy, planning and decision-making processes.

Social inequalities of various types may disadvantage some groups and make them much less likely to benefit fully from digital opportunities, many of which depend on a certain degree of literacy and modern skills and abilities. For example, Nderitu A.M., 2018 notes that by 2010 there were significant differences in literacy rates between ethnic groups in Kenya, with the highest literacy rate enjoyed by the Kisii at 83.4% and the lowest by the Somali at 20%.

Apart from the Kisii, it appears that low literacy is correlated with small populations, who have a high likelihood of being defined as disadvantaged or marginalized groups.

Kibua T. N 2020 draws a convincing contrast between the lives of the small minority of the richest Kenyans with the daily experiences of the low-income minority that demonstrate it is near impossible for the two groups to understand each other.

He also points out the impact of the use of financial handouts to influence the choices of low-income groups during electoral processes and this may help explain why minority groups enjoy much less leverage during such processes leading to marginalization, including digital exclusion.

Burbridge D., 2015. makes the important point that infrastructure is often developed in remote areas without the participation or understanding of the local people.

Communication about such projects tends to appear in formal channels, in English, and with an orientation towards reporting corruption, inefficiency and failure, rather than an opportunity. Marginalized and disadvantaged communities are therefore likely to be much less aware of digital opportunities as well as risks.

Negroponte N, 1996 foresaw the impact that the digital revolution would transform society by providing an efficient, effective and personal way of delivering information to individuals as well as groups. One group that has been profoundly affected by the advent of digital technology in a variety of ways are the youth.

As early as 2010 changes in the behaviour of this group were already being noted. Watson R., 2010, coined the term “screenagers” because of the large amount of time that 12 to 19-year-olds spend using digital devices. Research has shown that this affects their attention span, persistence, concentration, desire for instant gratification and traits in consuming and responding to information.

Some youth develop a “persona” a virtual identity with desired characteristics which the owner does not possess (such as wealth, age, popularity) in order to gain “followers.” While the Internet and digital devices provide many positive opportunities for young people they also pose substantial risks to both the activities and character development of youth which must be counteracted at home and through the education system.

In Kenya the impact of digital technology on citizens who use financial applications is one significant issue.

Beck T. et al, 2010 reported that, by 2009, although mobile money had only been in common use for a few years, citizens were already rating it as “the least risky and fastest channel” to send remittances to family and friends. (It was rated second after family and friends in terms of the least expensive and easiest to obtain channel.)

The study also revealed that ownership of a mobile phone made an individual more likely to use financial services and less likely to experience financial exclusion regardless of other factors normally associated with exclusion such as age, gender, or living in a rural area.

Kusimba S.; 2021 has written a book that provides a very informative account of the ways in which ordinary Kenyans in rural and peri-urban areas manage their mobile money transactions. The respondents of the study were encouraged to visually represent the network of people and applications they access through mobile devices.

The drawings were not only surprisingly complex, but they also illustrated how mobile devices have permeated the social and cultural as well as the financial activities of ordinary Kenyans. The networks encompassed family, business, social and religious relationships, involving remittances and receipts of money as well as social exchanges and negotiations.

There was sharing of devices and even SIM cards creating obligations and risks. The main financial transactions identified included community coordination and planning (for example during fundraising for social events such as funerals and weddings), informal transportation arrangements/ ride-hailing, informal savings, formal fundraising (for example by cooperative groups), and gift-giving.

There has been an increase in applications that facilitate borrowing, and the challenge of mobile debt is growing rapidly. Payment of remote workers, payment of bills, remote shopping and e-commerce are other growing applications. Regarding security, the awareness of its importance is tellingly portrayed by a user who represented her mobile loan account as a box with three locks.

While the impact of existing technology on ordinary citizens may also be causing concern it is clear that emerging technology is likely to have an even greater impact in the near future.

Photo: Cyber crime./ www.freepik.com

Susskind D., 2020 analyzes the potential of existing and emerging technology to make many current jobs and tasks performed by humans redundant.

He points out that human decision-makers will have to choose whether they will use technology to complement, supplement or replace humans in the performance of tasks, while human workers will have to reconsider their skill and performance base in order to remain relevant.

He points out a number of strategies that humans can use to manage this emerging reality, and the role of the State and the education sector in designing viable responses.

Moore, G. A, 1991. focuses on the task of technology companies in marketing their emerging technology products to traditional businesses. Of course, the landscape has changed drastically in the last 31 years since the book was published and the corporate sector has accepted that innovation is an important survival strategy.

However, the book brings out the tension between visionaries and technology enthusiasts on the one hand and conservatives and pragmatists on the other. When policymakers fall into these camps it can be difficult to predict how technology is going to penetrate the market, making it more challenging to plan for the future.

Baeza-Yates R et al, 1999 writing twenty years before the widespread use of big data mining and user modelling algorithms, researchers in the field of Information Retrieval (IR) were already predicting that would pose the risk of information exploitation for users while Tranberg H. et al, 2004 note that medical records are among the most sensitive information held about a user.

While they are supposed to be highly confidential and responsibly used by a small group of medical professionals, it is also clear that this information is valuable for others such as employers, relatives, insurance companies, researchers, pharmaceutical companies and others, so the challenge of keeping the information private, especially when it is held in digital formats, can be substantial.

In addition, when the information is shared between service providers, a mistaken entry or omission can have disastrous effects on a patient. Humble medical practices may not have the technology or skills necessary to handle this information responsibly.

In developed countries, there are specialized training programmes relating to health information and laws (an example being the Health Information Protection Act (HIPA) in the United States of America.

The situation is less clear in developing countries where there may be no legislation, or, as in Kenya, may rely on data protection legislation which defines medical information as “sensitive personal information.” Data protection legislation may place administrative burdens on busy medical practices by requiring them to register, continuously report, give individuals access to their personal records on-demand, pay annual licensing fees and submit to periodic inspections, for example.

A study of events, emerging technology and policy issues demonstrates that the issue of cyber-hygiene in a developing country which is rapidly adopting, adapting and innovating digital technology is a complex one. Therefore the next section will pose the kind of issues that cyber-hygiene should encompass if it is to effectively serve citizens.

4. A POLICY MODEL FOR CYBER-HYGIENE IN KENYA

The most authoritative method currently available for Cyber-hygiene is currently the Cybersecurity Capacity Maturity Model (CMMI) developed by the Oxford Martin School in the U.K.

It has 5 elements which both organize and enable the measurement of cybersecurity maturity. These are:

D1: Cybersecurity Policy and Strategy

D2: Cyber-culture and society

D3: Cybersecurity education, training and skills

D4: Legal and regulatory frameworks

D5: Standards, organisation and technologies.

Countries, organizations and businesses can use the maturity model to self assess, or an assessment can be formally guided by consultants. The assessment is intended to be a starting point for an effective strategy toward cybersecurity maturity.

It is D2: Cyber-culture and society is the most pertinent element when it comes to citizen cyber-hygiene. It has five components: Cybersecurity mindset in Government and the Private Sector and users; Trust and confidence in the use of the Internet for eGovernment and eCommerce applications, User understanding of personal information protection online, a progress reporting mechanism, and the important use of digital technology by media, including social media.

While this is excellent we argue in this paper that the growth in digital technologies and digital applications for users, and the unique dominance of financial technology among ordinary people in Kenya, require that this model must be enhanced and extended to provide a robust methodology for protecting users in Kenya, including vulnerable and disadvantaged people.

We thus use this section to develop additional components in this section.

This extension has two major components: a stakeholder model and an issue model. Figure 2 below sets out the stakeholder model.

The purpose of clearly setting out the stakeholders is twofold: to ensure that all stakeholder groups are represented, by policy, in any process; and to ensure that initiatives are properly designed to address the needs and demands of each stakeholder group.

The Government, as the developer of law and policy as well as the provider of infrastructure, is an important stakeholder.

This stakeholder must be followed to ensure that citizen-cyberhygiene becomes a significant consideration in the development of the digital economy, in essence, to develop an architecture of cyber-hygiene.

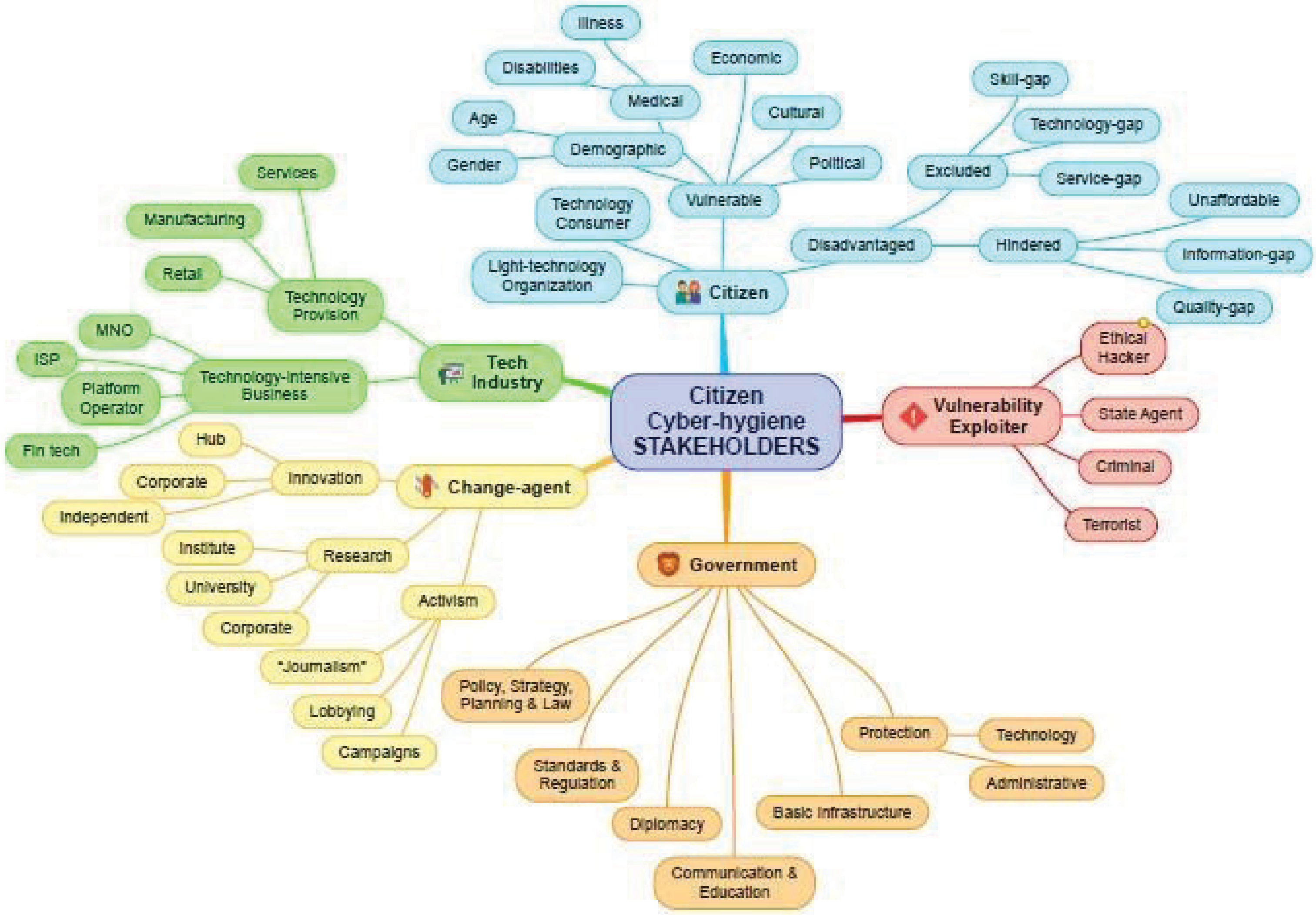

Figure 2: Citizen Cyber-hygiene stakeholders

Photo: 60-The-5-Latest-Cyber-Security-Technologies-for-Your-Business. www.freepik.com

Due to technology development, anything "cyber" is a moving target, and therefore the source of these changes, dubbed "change agents" are important stakeholders if we are to keep up with changes in the environment. Change agents include innovators, researchers and activists.

The third group of important stakeholders are the technology industry who provides the products and services which drive and maintain the industry. They are important because they own and understand the technology, they can have a huge impact on cyber-hygiene progress, for example by adopting good practices such as security-by-design, and because it is important to continuously influence the technology industry to adopt citizen-friendly strategies and practices.

Vulnerability exploiters are also important actors at the table. While we obviously cannot bring criminals to the table, it is important to bring communities such as ethical hackers, who profoundly understand the risk landscape to the table. CIRTS and other technical communities can also assist in this role.

The primary stakeholder is the citizen, including very small enterprises which often do not have a voice in this space. Technology consumers as well as the digitally excluded (who obviously have the potential to join the technology consumers if the right policies are adopted) are included in this community. We have attempted to define why certain citizens are vulnerable or disadvantaged as digital citizens and contend that all these groups should be suitably represented in any policy development or review process.

The main elements to be covered in any citizen cyber-hygiene policy are: User (including potential user) empowerment, technology and the regulatory environment.

Technology is considered along four lines: safe, secure, sustainable and transparent technology. The issues go beyond cybersecurity towards any issue that would make the technology unavailable or unsustainable for ordinary users.

Both the local and international environments are considered towards having a cyber-hygienic legal and regulatory environment.

Finally, user empowerment encompasses instilling the right values to users (to protect them from each other), the administrative elements of empowering users, and the orientation of users with the right orientation and skills to protect themselves in cyberspace, as well as take up the opportunities afforded by digital technology.

5. POLICY DEVELOPMENT AND REVIEW PROPOSALS

The key elements necessary to the insertion of the issue of citizen cyber-hygiene into the national policy dialogue are

- A clear appreciation of the motivation for bringing this issue to the foreground. This involves identifying the issues, including currently-observed and events which demonstrate that this issue has become significant for citizens and the national opportunity to use digital technology to fast-track the achievement of national goals, which may be lost or damaged if citizen cyber-hygiene is ignored. It is also important to identify the affected stakeholders – the number and proportion of citizens who are affected by this issue.

- The policy must also define the goals and targets to be achieved through the interventions which will be spurred by the policy so that its success and significance can be accurately measured.

- With the cybersecurity mandate currently shared between a number of very different institutions and groups, it will be important for the policy to clearly set out the institutional responsibility for cyber-hygiene. What is not assigned is unlikely to be done and any parts of the general effort which are implemented are unlikely to be sustainable.

- The policy must clearly set out the major responsibilities to be borne and the major initiatives to be implemented.

- A monitoring, evaluation and reporting mechanism is essential for measuring the success of any effective policy.

- Lastly, the policy must define its review cycle so that it is periodically updated to align with changing technology and social conditions.

The major contention of this review is, therefore, that, while the current policy, legal and regulatory environment for cybersecurity in Kenya is robust for a developing country, in view of the widespread use of digital technology by ordinary Kenyans for essential life functions such as financial transactions, and the digital divide experienced by disadvantaged and vulnerable people it would be wise to develop and implement an exclusive citizen cyber-hygiene policy instead of relying on existing provisions spread over a wide variety of legal and policy documents.

Such a policy would include an effective approach to awareness creation and training of citizens to enable them to adopt good cyber-hygiene practices.

The second major recommendation is that an existing organization, I would recommend the ICT Authority, should specifically be assigned the mandate for the national implementation of cyber-hygiene, while the coordinating institutions and committees referred to earlier in this document should have their mandates reviewed to reflect this new assignment of responsibility. ICTA is ideal for this role since it is already involved in assisting public institutions to adopt cybersecurity practices.

The third major recommendation is that KENET, the education ISP and NREN should be officially recognized as a public institution and should have its mandate extended to encompass the research and review of the technology cycle including conceptual, emerging, current, aging and obsolete technology and to report on the security and economic impact of technology within these stages to the general public. Such reports would include an analysis of the steps the Government should take to mitigate risks and exploit opportunities for innovation and prosperity.

KENET is well-placed to take up this role since it has close ties with all universities and research institutions and could easily share this task with the research community.

The fourth major recommendation is that KE-CIRT/CC should have its mandate enhanced and should be financially and operationally assisted to develop a citizen communication centre and helpline to assist small businesses and citizens to easily communicate cybersecurity concerns.

A fifth major recommendation would concern the mainstreaming of a Cyber-hygiene policy within Kenya's negotiation position in bilateral, regional and international Cyber-security processes. This would further enhance Kenya's cyber-security position and assert her leadership as Africa's digital economy.

A sixth recommendation would be the review of the citizen engagement policy developed by the Kenya Law Reform position to further enhance the participation of disadvantaged and vulnerable populations in policy-making processes.

It is clear that, if Kenya is to take her place as Africa's digital economy, it is necessary to create a globally-trusted digital environment within Kenya, to give both investors and users around the world the confidence to use Kenya's digital tools, services and workforce.
This will not only involve robust infrastructure, critical infrastructure protection, high-level technical capacity development and a robust legal and regulatory environment. It will also involve the cyber-hygiene attitudes and behaviours of millions of ordinary Kenyan users of digital goods and services. A cyber-hygiene policy, awareness creation and training is an important first step toward creating a good cyber-hygiene culture among ordinary Kenyans, including disadvantaged and vulnerable groups.
'

6. BIBLIOGRAPHY

- **Anke Hassel,** in International Encyclopedia of the Social & Behavioral Sciences (Second Edition), 2015
- **Jackson R.;** Planning, Politics and Administration; in Development Administration:The Kenyan Experience; Haden G., Jackson R., Okumu J. (Eds.); Oxford University Press, 1970.
- **Leonard D.K.;** Communication and Deconcentration; Planning, Politics and Administration; in Development Administration: The Kenyan Experience; Haden G., Jackson R., Okumu J. (Eds.); Oxford University Press, 1970..
- **Beck T. et al;** Banking Sector Stability, Efficiency and Outreach in Kenya; in Kenya: Policies for Prosperity; Adam C.S., Collier P., Ndung'u N. (Eds); Oxford University Press; 2010.
- **Nderitu A.M.;** Kenya, Bridging Ethnic Divides: A Commissioner's Experience on Cohesion and Integration; Mdahalo Bridging Divides Ltd.; 2018.
- **Burbridge D.;** The Shadow of Kenyan Democracy: Widespread Expectations of Widespread Corruption; Ashgate Publishing; 2015.
- **Kibua T. N.;** Kenya, Economic Governance and Management; Soyounique Publishers; 2020.
- **Kusimba S.;** Reimagining Money: Kenya in the Digital Finance Revolution; Stanford University Press, 2021.
- **Watson R.;** Future Minds: how the digital age is changing our minds, why this matters and what we can do about it; Nicholas Bealy Publishing; 2010.
- **Negroponte N.;** Being Digital; Hodder & Stoughton; 1996
- **Susskind D.;** A world without work: technology, automation and how we should respond; Penguin; 2020.
- **Moore, G. A.;** Crossing the Chasm: Marketing and selling high tech products to mainstream customers, Harper Business, 1991.
- **Baeza-Yates R.,** Ribeiro-Neto B.; Modern Information retrieval; Addison Wesley; 1999
- **Tranberg H., Rachbass J.;** Medical Records: Use and abuse; Radcliffe; 2004.

KICTANet
The Power of Communities

Email: info@kictanet.orke
Web: www.kictanet.or.ke
Twitter: @kictanet

UKaid
from the British people