Exercise Background Material

Kenya
Country Profile

Points of Contact: Rebecca Beigel, Julia Schuetze | Stiftung Neue Verantwortung e. V.
Beisheim Center | Berliner Freiheit 2 | 10785 Berlin

This document is exercise-specific information material and was developed for the purpose of a cybersecurity policy exercise only.

Disclaimer:

The research only represents a country's cybersecurity policy to a limited extent and is not an in-depth or complete analysis or assessment of current policy. In order to adapt the exercises to specific countries, it is important to understand the broader strokes of cybersecurity policies of other countries. Our team, therefore, researches publicly available information on cybersecurity policies of countries to adapt the exercises to country-specific needs. The research is shared with participants as background material in preparation for the exercise. Therefore, the documents have a timestamp and consider policy up until the date of publication. In the interests of non-profitability, we decided to make the background research publicly available. If you are using these materials, please include the disclaimer. Please also do not hesitate to contact us.

Points of Contact:

Rebecca Beigel

Project Manager for International Cybersecurity Policy

rbeigel@stiftung-nv.de

+49 (0)30 40 36 76 98 3

Julia Schuetze

Junior Project Director for International Cybersecurity Policy

jschuetze@stiftung-nv.de

+49 (0)30 81 45 03 78 82

Table of Contents

Political System and Socio-Political Background

Kenya‘s Cybersecurity Policy

1. Kenya – Political System and Socio-Political Background

Key Facts

- Official Country Name: Republic of Kenya, Nairobi is the capital[1]
- Population: About 52,57 million people (2019)[2]
- Official languages: Kiswahili, English[3]
- Currency: Kenya shilling[4]

Political System

- Form of Government: Presidential Republic[5]
  - Head of State and Government: President Uhuru Muigai Kenyatta[6]
    - President is Commander-in-Chief of the Armed Forces[7]
  - The Kenyan government consists of 20 ministries.[8]
- Bicameral Parliament that consists of Senate (67 seats) and National Assembly (349 seats).[9]
- Kenya is a unitary state divided into 47 counties that each have their local governments.[10]

Socio-Political Context

- Kenya is one of the fastest-growing economies in Africa, with an annual average growth of 5.9 percent from 2010 to 2018.[11] It is ranked as a lower middle-income country and has set a target to become a middle-income nation by 2030.
  - Agriculture as the most significant sector contributes to 20 percent of the GDP.[12]
  - In 2021, however, two-thirds of Kenyans continue to live under the poverty line.[13] One-third continue to live in extreme poverty.[14]
- Especially Nairobi has seen drastic developments in the digital economy. The capital has continued to develop into a regional tech hub earning itself the nickname "Silicon Savannah".[15]
  - In 2018, it was home to more than 200 startups and well-established US-tech firms like Microsoft or Intel.[16]

- The widely popular money-transferring app M-Pesa was founded in Nairobi. It allows customers to send money via text messages and is used by 42 million active customers across seven countries.[17]

- In the World Economic Forum's Global Competitiveness Report 2019, Kenya's ICT adoption ranks 116th place out of 141 countries. Around 17.8 percent of adults use the internet.[18]

Vulnerability and Threat Landscape

With Kenya having one of the highest internet penetrations in Africa, the country is more exposed to cyber crime than other African states. Kaspersky reported that in Africa, Kenya, together with South Africa and Nigeria was the most affected African state by malware incidents in 2020.[19] In 2017, Kenya lost approximately 161,1 million euros due to various cyber crime incidents.[20] Microsoft warned that with the rapid rise of digitalization in Kenya, especially the financial service industry would become vulnerable to cyber crime.[21] The Communications Authority of Kenya, the regulator of the Kenyan internet economy, stated that more than 56 million cyber threats were detected in 2020: "A majority of the threats were malware attacks at 46 million, followed by web application attacks at 7.8 million while 2.2 million Distributed Denial of Service (DDos) threats were detected during the same period."[22]

The following exemplary cases of cyber incidents gained national and international media attention:

- In February 2021, intruders gained access to Kenya's world cancer day virtual meeting, taking control of the event posting obscene pictures, messages, and videos. The event was attended by the Kenyan Health secretary Muthai Kagwe. Organizers consequently shut down the event.[23]

- In 2020, the cybersecurity firm Group-IB reported that it only considers five groups of cybercriminals as a threat to the financial sector. Among them is the Kenyan group SilentCard that operates in Kenya. According to Group-IB, SilentCard has less sophisticated technical capabilities than comparable groups but maintains to be quite effective. The group targets Kenyan banks and their ATMs through various methods.[24] In April 2019, the group heisted 83.700 Euros by jackpotting several ATMs. In 2019 the group accessed a local Kenyan banks credit card processing system transferring payments of 3,04 Million Euros. SilentCard is well known for recruiting students and university graduates to expand its missions.[25]

- In May 2017, the ransomware WannaCry spread globally on unpatched Windows systems through the so-called EternalBlue exploit. Infected networks were encrypted and were being held ransom against the payment of bitcoin.[26] The Communications Authority of Kenya reported that the WannaCry incident affected at least 19 companies in Kenya.[27] While individual firms are unknown, the Cabinet Secretary for Ministry of Information and Communications Joseph Mucheru announced that Kenyan banks were among the targets. The respective firms reported the incidents to the National Kenya Computer Incident Response Team Coordination Center (National KE-CIRT/CC).[28] The Communications Authority of Kenya issued a press statement to warn users against a possible ransomware incident and recommended steps to secure computer systems.[29]

- In January 2017, a group referring to itself as AnonPlus gained access to the website of the Communications Authority of Kenya. The group replaced the homepage with their manifesto stating to "defend freedom of information, freedom of the people and emancipation of the latter from the oppression of media and those who govern us." At the same time, a group that referred to itself as the Moroccan Islamic Union Mail gained access to the website of the National Environment Management Authority (Nema). The websites remained offline for several days.[30]

2. Overview: Kenya‘s Cybersecurity Policy

Cybersecurity Policy

According to the Global Cybersecurity Index (GCI) 2020, Kenya ranks fifth in the African region regarding its commitment to cybersecurity policy.[31] The GCI is calculated by the International Telecommunications Union (ITU) based on five pillars, such as legal measures or international cooperation.[32]

The **National Cybersecurity Strategy** primarily defines Kenya's interest in cyberspace. It was released in 2014 by the Ministry of Information, Communications, and Technology. With its strategy, the government recognizes cybersecurity as a national priority to protect its ICT infrastructure against an evolving cyber threat landscape. The strategy bolsters existing government strategies like the **National ICT Master Plan** that sets out to create a regulatory environment for e-government services and ICT-related business[33] and the **Kenya Vision 2030**, a long-term development plan to transform Kenya into an industrial middle-income country.[34] The National Cybersecurity Strategy pursues four goals that are supplemented with underlying objectives[35]:

1. Enhance the nation's cybersecurity posture: By coordinating with international partners and national stakeholders, the government commits to secure critical infrastructure and services.
2. Build national capabilities: The government commits to building capacities through awareness programs and training that inform the Kenyan public and train a professional workforce on cybersecurity.
3. Foster information sharing and collaboration: The government commits to developing a "comprehensive governance framework"[36] that coordinates stakeholders to develop appropriate cybersecurity policies and balance various policy priorities (e.g., security, privacy, economic priorities).
4. Provide national leadership: The government commits to continuously refresh the National Cybersecurity Strategy and establish a roadmap to achieve set objectives.

Moreover, the **Kenya National ICT Masterplan 2014-2017**, by the Ministry of Information, Communications and Technology, also includes cybersecurity objectives under its various goals. Firstly, the plan sets the aim to develop, implement and institutionalize a cybersecurity management framework. This legal framework aims at protecting infrastructure, information, and application, thus enhancing trust in ICT-related services like electronic commodity exchanges. The Masterplan recognizes an absence of a law governing cybersecurity and the organization of government agencies within the field of cybersecurity. It consequently recommends to "fast track development of cyber security law"[37] and commits to develop a concrete cybersecurity policy.[38]

According to the Kenya National ICT Masterplan 2014-2017, a National Cybersecurity Master Plan by the Kenyan governmet has already been drafted.[39] The master plan "addresses emerging cyber risks and the challenges that the ICT may face in the future".[40]

Additionally, the Central Bank of Kenya (CBK) issued a **Guideline on Cybersecurity for Payment Service Providers** in 2019.[41] The guideline requires Payment Service Providers (PSPs) to maintain a cybersecurity program and implement cybersecurity governance frameworks. They set specific requirements on cybersecurity governance, cybersecurity policies, risk management, outsourcing, and auditing and testing of cybersecurity systems. All PSPs are required to submit a cybersecurity policy to the CBK and review their policies annually. In case of a cybersecurity incident, the CBK has to be notified within 24 hours. Large-scale payment services have to be notified within 2 hours. Quarterly, PSPs have to submit a record of occurred incidents.[42]

Legal Framework

Provisions that are related to cybersecurity and the protection of ICTs are included in the **Kenya Information and Communications Act (KICA)**.[43][44] Furthermore, cybercrime is regulated through the **Computer Misuse and Cybercrimes Act**.[45] This section solely focuses on laws that have been passed; it does not discuss bills or amendments.

Kenya Information and Communications Act (KICA) of 1998 established the Communications Authority of Kenya tasked with facilitating development in the ICT sector.[46] While KICA is not explicitly directed towards cybersecurity, sections 83Q – 84I regulate IT security. Section 83Q states that the Minister of ICT may, in consultation with the Commission, prescribe regulations that ensure adequate integrity, security, and confidentiality of electronic records and payments.[47]

Computer Misuse and Cybercrimes Act, which came into effect in 2018, creates offenses in regard to the infringement on IT-security measures "with the intent to gain access, and knowing such access is unauthorized".[48] After critique that the act violated constitutionally guaranteed rights and freedoms, the High Court of Kenya temporarily suspended 26 sections of the bill two days before it came into force. On February 20th, 2020, the High Court lifted the suspension and dismissed the critiques as unjustified.[49] The Computer Misuse and Cybercrimes Act establishes the National Computer and Cybercrimes Coordination Committee (NCCCC), which is currently being implemented and presented in more detail in the following section.[50]

Cybersecurity Architecture – Selected Institutions

Various government actors work on enhancing Kenyan cybersecurity. Most agencies operate under the umbrella of the Ministry of Information, Communication and Technology, Innovation and Youth Affairs, which has a broad mission of facilitating ICT infrastructure.[51]

The **Ministry of Information, Communication and Technology, Innovation and Youth Affairs (Ministry of ICT)** is responsible for "administering, managing and developing the Information, Broadcasting and Communication policy"[52]. In May 2016, the ministry was internally organized into the State Department of Broadcasting and Telecommunications and the State Department of ICT and Innovation.[53]

The **Information and Communication Technology (ICT) Authority** works as a state corporation under the Ministry of ICT. It is tasked with "enforcing ICT standards in Government and enhancing the supervision of its electronic communication"[54]. Within the ICTA, the Information Security Department promotes information security, evaluates organization's cybersecurity, and supervises and implements security policies and guidelines for the government.[55]

The **Communications Authority of Kenya (CA)** is the regulatory authority for cybersecurity (and the communications sector more broadly). Among others, the CA licenses systems in the communications industry, manages frequency spectrums, and protects consumer rights in the communication sector. The CA was established by KICA in 1998 and facilitated the development and management of a national cybersecurity framework as envisioned in the National Cybersecurity Strategy.[56] For regulations on IT security, the Cabinet Secretary in the Ministry of Information and Communications can consult with the CA.[57]

The **National Kenya Computer Security Incident Response Team – Coordination Centre (KECIRT/CC)** is Kenya's national Computer Security Incident Response Team (CSIRT) and was established by the CA. As a national point of contact for all stakeholders, it detects, prevents, and responds to cyber threats. Furthermore, it is tasked with implementing cybersecurity policies that promote awareness and capacity building and conduct Research and Development (R&D).[58] KE-CIRT/CC states that it collaborates with CIRTs outside its jurisdiction (e.g., the US-CERT or the Global Forum for Incident Response and Security Teams (FIRST)). However, it does not name specific instances of collaboration.[59]

A **National Computer and Cybercrimes Coordination Committee (NCCCC)** was effectively created via the Computer Misuse and Cybercrimes Act (as stated above). The NCCCC will prospectively be tasked with advising the government on security-related aspects of "blockchain technology, critical infrastructure, mobile money and trust accounts"[60]. It will advise the National Security Council on computer and cyber crimes and coordinate strategies and practices on cybersecurity. The NCCCC will consist, among others, of high-ranking officials from the Communications Authority of Kenya, the military, law enforcement, and the Central Bank of Kenya.[61]

The **Directorate of Criminal Investigations**, which is part of the National Police Service, has the mandate to undertake investigations on cyber crimes.[62] Within the directorate, a Digital Forensic Laboratory (DFL) analyzes electronic devices "related to all cyber-enabled offences"[63]. The DFL conducts malware analysis, computer, and mobile forensics and serves as a CIRT to respond to cybersecurity incidents.[64]

Bilateral and Multilateral Cooperation

Kenya is a member of the African Union (AU), the Commonwealth, the International Telecommunications Union, and the United Nations (UN).[65] All these international organizations deal with and discuss cybersecurity-related topics. The AU, for example, adopted the **Convention on Cyber Security and Personal Data Protection (Malabo Convention)** in 2014 to address cybersecurity and cyber crime.[66] Kenya has neither signed the **Malabo Convention** of the African Union[67] nor the **Budapest Convention on Cybercrime** (Treaty No. 185).[68]

Within the UN, Kenya was represented in the Group of Governmental Experts (GGE) on advancing responsible state behavior in cyberspace in the context of international security.[69] Additionally, Kenya was part of the Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security (OEWG), established in 2018. As opposed to the GGE, the OEWG is open to all UN members and establishes a continuing dialogue on cybersecurity issues within the UN.[70] In its final report in March 2021, the OEWG supported the notion that international law and the UN Charter should be applicable in cyberspace and that states should voluntarily identify and cooperate on confidence-building measures in their local contexts. With the 1st substantive session of the OEWG, Kenya stated its expectations of the working group, reiterating its wish for a harmonized framework for cyber crime management.[71]

Regarding multilateral cooperation outside the UN, Kenya is part of several platforms and initiatives:

- Kenya is part of the **Global Forum on Cyber Expertise (GFCE)**, founded by the ITU.[72][73] The GFCE is a multi-stakeholder platform that collaborates on cyber capacity building by coordinating projects, sharing knowledge, developing research, and addressing capacity gaps by mutual support.[74]

- The (ICT) Authority is also a member of the **Cybersecurity Alliance for Mutual Progress initiative (CAMP)**.[75] CAMP was initiated by the Korean government in 2016 and is a network of countries that share experiences and trends in cybersecurity to enhance each other's cybersecurity capacity.[76] In addition, Kenya hosted the **Africa Cyber Defense Summit** with the theme "Accelerating Africa's Cyber Security Dialogue" in 2018. The African Cyber Defense Summit describes itself as the largest cybersecurity gathering in Africa.[77]

Regarding direct bilateral cooperation, Kenya maintains several agreements with third states:

- In 2015 Kenya signed the MoU on a **Cyber Security Framework for Cooperation and Collaboration between the Northern Corridor Integration Projects Partner States** with Rwanda, Uganda, and South Sudan.[78] The MoU aims at protecting regional oil and infrastructure projects from cyber threats.[79] It acknowledges the heightened threat of cyber incidents and commits partnering countries to cooperate by establishing a Northern Corridor CIRT.[80] The states will thus collaborate on cybersecurity through information sharing, incident handling, and capacity building.[81]
- In 2017, the United States and Kenya commenced the **Cyber and Digital Economy Policy Dialogue** in Nairobi. The dialogue aims to protect the economic interest of both countries from cyber crime and will "serve as a policy-level channel"[82] to identify issues and develop joint initiatives around cybersecurity in the digital economy.[83]

Sources

1 BBC (2018): Kenya country profile. https://www.bbc.com/news/world-africa-13681341

2 World Bank: Population, Kenya. https://data.worldbank.org/indicator/SP.POP.TOTL?locations=KE

3 CIA (2021): World Factbook. Kenya. https://www.cia.gov/the-world-factbook/static/474ff6aa6a4aee27c94b984aa1089b74/KE-summary.pdf

4 BBC (2018): Kenya country profile. https://www.bbc.com/news/world-africa-13681341

5 Auswärtiges Amt: Überblick. Kenya. https://www.auswaertiges-amt.de/de/aussenpolitik/laender/kenia-node/kenia/208042

6 Ibid.

7 President of the Republic of Kenya: Executive Office of the President. https://www.president.go.ke/presidency/

8 Embassy of the Republic of Kenya in Japan: The Government Ministries. http://www.kenyarep-jp.com/kenya/ministries_e.html

9 CIA (2021): World Factbook. Kenya. https://www.cia.gov/the-world-factbook/static/474ff6aa6a4aee27c94b984aa1089b74/KE-summary.pdf

10 Embassy of the Republic of Kenya in Japan: The Government Ministries. http://www.kenyarep-jp.com/kenya/ministries_e.html

11 USAID (2021): Kenya. Economic growth and trade. https://www.usaid.gov/kenya/economic-growth-and-trade

12 GIZ: Kenya. https://www.giz.de/en/worldwide/317.html

13 USAID (2021): Kenya. Economic growth and trade. https://www.usaid.gov/kenya/economic-growth-and-trade

14 GIZ: Kenya. https://www.giz.de/en/worldwide/317.html

15 Henry (2015): Nairobi Used to be a Terrible Place to Do Business. How Did It Transform Into a Tech Hub? https://slate.com/business/2015/08/nairobi-as-silicon-savannah-how-the-kenyan-capitol-grew-in-to-a-hub-for-digital-entrepreneurship.html

16 Mallonee (2018): The Techies Turning Kenya into a Silicon Savannah. https://www.wired.com/story/kenya-silicon-savannah-photo-gallery/

17 Piper (2020). What Kenya can teach its neighbors – and the US – about improving the lives of the "unbanked". https://www.vox.com/future-perfect/21420357/kenya-mobile-banking-unbanked-cellphone-money

18 Schwab (2019): The Global Competitiveness Report 2019. http://www3.weforum.org/docs/WEF_TheGlobalCompetitivenessReport2019.pdf

19 Mwita (2021): Kenya faces increased cybercrime in 2021 – Kaspersky. https://www.the-star.co.ke/business/kenya/2021-01-12-kenya-faces-increased-cybercrime-in-2021kaspersky/

20 HapaKenya: Cyber Security in Kenya. The latest threats and how best to protect against them. https://hapakenya.com/info/cyber-security-in-kenya-the-latest-threats-and-how-best-to-protect-against-them/

21 Amadala (2019): Revealed. Here are hacker groups looting banks in Kenya. https://www.the-star.co.ke/business/2019-05-02-revealed-here-are-hacker-groups-looting-banks-in-kenya/

[22] Rotich (2021): Cyber-attacks in Kenya up by half to hit 56m in three months. https://www.businessdailyafrica.com/bd/corporate/companies/cyber-attacks-in-kenya-56m-in-three-months-3285438

[23] Vidija (2021): Kenya at high risk as cyberattacks continue to plague businesses. https://www.the-star.co.ke/news/big-read/2021-02-18-kenya-at-high-risk-as-cyberattacks-continue-to-plague-businesses/

[24] Siele (2020): Inside Kenyan Hacker Group Gaining International Fame. https://www.kenyans.co.ke/news/49809-inside-kenyan-hacker-group-gaining-international-fame

[25] Tai (2020): This hacker group is famous for attacking banks and financial institutions worldwide, and they are hiring new members. https://www.exploitone.com/cyber-security/this-hacker-group-is-famous-for-attacking-banks-and-financial-institutions-worldwide-and-they-are-hiring-new-members/

[26] Kaspersky (2021): What is WannaCry ransomware? https://www.kaspersky.com/resource-center/threats/ransomware-wannacry

[27] Kamau (2017): 19 Kenyan firms hit by costly ransomware cyber attack. https://www.standardmedia.co.ke/news/article/2001240392/19-kenyan-firms-hit-by-costly-ransomware-cyber-attack

[28] The Star (2017): Panic as 'WannaCry' virus hits 19 Kenyan firms. https://www.the-star.co.ke/news/2017-05-22-panic-as-wannacry-virus-hits-19-kenyan-firms/

[29] Communications Authority of Kenya (2017): Statement by the Director-General of the Communications Authority of Kenya (CA), Mr. Francis Wagusi, on the "Wannacrypt0r" ransomware cyber attack. https://ca.go.ke/wp-content/uploads/2018/01/Press-Statement-By-Communications-Authority-of-Kenya-on-WannaCrypt0r-Ransomware-Virus.pdf

[30] Sunday (2017): Shame as Kenya's Internet regulator website hacked. https://www.standardmedia.co.ke/business/article/2000228978/shame-as-kenyas-internet-regulator-website-hacked

[31] ITU (2020): Global Cybersecurity Index 2020. https://www.itu.int/epublications/publication/global-cybersecurity-index-2020/en/

[32] ITU (2018): Global Cybersecurity Index v4. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cyber-security-index.aspx

[33] ICT Authority (2017): National ICT Masterplan. http://icta.go.ke/national-ict-masterplan/

[34] Vision 2030 Delivery Secretariat (2021): About Vision 2030. https://vision2030.go.ke/about-vision-2030/

[35] Government of Kenya (2014): Cybersecurity Strategy. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Kenya_2014_GOK-national-cybersecurity-strategy.pdf

[36] Ibid.

[37] Kenya ICT Authority (2014): National ICT Masterplan. http://icta.go.ke/national-ict-masterplan/

[38] Ibid.

[39] Ibid.

[40] Government of Kenya (2014): Cybersecurity Strategy. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Kenya_2014_GOK-national-cybersecurity-strategy.pdf

[41] Central Bank of Kenya (2019): Guideline on Cybersecurity for Payment Service Providers. https://www.centralbank.go.ke/wp-content/uploads/2019/07/GuidelinesonCybersecurityforPSPs.pdf

[42] Central Bank of Kenya (2019): Guideline on Cybersecurity for Payment Service Providers. https://www.centralbank.go.ke/wp-content/uploads/2019/07/GuidelinesonCybersecurityforPSPs.pdf

[43] Vidija (2021): Kenya at high risk as cyberattacks continue to plague businesses. https://www.the-star.co.ke/news/big-read/2021-02-18-kenya-at-high-risk-as-cyberattacks-continue-to-plague-businesses/

[44] Communications Authority of Kenya: Sector Legislation. https://ca.go.ke/about-us/statutes-regulations/sector-legislation/

[45] National Council for Law Reporting (2018): The Computer Misuse and Cybercrimes Act, 2018. http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf

[46] National Council for Law Reporting (2011): The Kenya Information And Communications Act. https://ca.go.ke/wp-content/uploads/2018/02/Kenya-Information-Communications-Act-1.pdf

[47] Ibid.

[48] National Council for Law Reporting (2018): The Computer Misuse and Cybercrimes Act, 2018. http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf

[49] Acharya / O (2020): Kenya's Computer Misuse and Cybercrimes Act, 2018: suspended provisions now effective. https://www.lexology.com/library/detail.aspx?g=ed5937e1-b7e3-42bb-baa9-2cef53cced5a#:~:text=Kenya's%20Computer%20Misuse%20and%20Cybercrimes%20Act%2C%202018%3A%20suspended%20provisions%20now%20effective,-ENSafrica&text=protecting%20the%20confidentiality%2C%20integrity%20and,of%20computer%20and%20cybercrimes%3B%20and

[50] National Council for Law Reporting (2018): The Computer Misuse and Cybercrimes Act, 2018. http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf

[51] Ministry of ICT: About the Ministry. https://ict.go.ke/about-the-ministry/#

[52] Ibid.

[53] Ibid.

[54] ICT Authority: About ICT Authority. https://icta.go.ke/who-we-are/

[55] ICT Authority: About ICT Authority. https://icta.go.ke/who-we-are/

[56] Communications Authority of Kenya: What We Do. https://ca.go.ke/about-us/who-we-are/what-we-do/ Government of Kenya (2014): Cybersecurity Strategy. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/National_Strategies_Repository/Kenya_2014_GOK-national-cybersecurity-strategy.pdf

[57] National Council for Law Reporting (2011): The Kenya Information And Communications Act. https://ca.go.ke/wp-content/uploads/2018/02/Kenya-Information-Communications-Act-1.pdf

[58] Communications Authority of Kenya: The national KE-CIRT/CC. https://ke-cirt.go.ke/

[59] Communications Authority of Kenya: Collaboration in Cybercrime Management. https://ke-cirt.go.ke/partners/

[60] National Council for Law Reporting (2018): The Computer Misuse and Cybercrimes Act, 2018. http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf

[61] Ibid.

[62] Directorate of Criminal Investigations: Functions. https://www.cid.go.ke/index.php/aboutus/our-functions.html

[63] Directorate of Criminal Investigations: Digital Forensic Laboratory (DFL). https://www.cid.go.ke/index.php/sections/forensic-sections/cyber-crime.html

[64] Ibid.

[65] UNIDIR: Kenya. https://unidir.org/cpp/en/states/kenya

[66] CCDCOE: African Union. https://ccdcoe.org/organisations/au/

[67] African Union (2020): African Union Convention on Cyber security and Personal Data Protection. https://au.int/sites/default/files/treaties/29560-sl-AFRICAN%20UNION%20CONVENTION%20ON%20CYBER%20SECURITY%20AND%20PERSONAL%20DATA%20PROTECTION.pdf

[68] Council of Europe (2021): Chart of signatures and ratifications of Treaty 185. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=O4NuhJKq

[69] Digwatch: UN GGE and OEWG. https://dig.watch/processes/un-gge

[70] Ibid.

[71] Permanent Mission of the Republic of Kenya to the United Nations (2019): Kenya Statement to the Open-Ended Working Group (OEWG) in Information and Communications. http://statements.unmeetings.org/media2/21997042/kenya.pdf

[72] Global Forum on Cyber Expertise: Our Members. https://thegfce.org/member-overview/

[73] ITU: Global Forum on Cyber Expertise. https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Global-Partners/global-forum-cyber-expertise.aspx

[74] Global Forum on Cyber Expertise: Strengthening cyber capacity and expertise globally through international collaboration. https://thegfce.org/

[75] CAMP (2020): Members. https://www.cybersec-alliance.org/camp/membership.do

[76] CAMP: About CAMP. https://www.cybersec-alliance.org/camp/about.do

[77] Africa Cyber Defence Summit: The largest cyber security gathering in Africa. https://naseba.com/what-we-do/commercial-services/cyber-defence-summit-africa-2018-2/#:~:text=On%20July%209%2D10%2C%202018,Nairobi%2Dbased%20Africa%20Cyberspace%20Network

[78] Jackson (2015): 'Northern Corridor' states vs. cybercrime. https://itweb.africa/content/dgp45Ma6Gx8qX9l8

[79] AT editor (2015): Northern Corridor member states sign cyber security agreement. https://africatimes.com/2015/06/23/northern-corridor-member-states-sign-cyber-security-agreement/

[80] Jackson (2015): 'Northern Corridor' states vs. cybercrime. https://itweb.africa/content/dgp45Ma6Gx8qX9l8

[81] UNIDIR: Kenya. https://unidir.org/cpp/en/states/kenya

[82] U.S. Department of State (2017): The United States and Kenya Strengthen Partnership on Cyber and Digital Economy Policy. https://2017-2021.state.gov/the-united-states-and-kenya-strengthen-partnership-on-cyber-and-digital-economy-policy/index.html

[83] Ibid.