Cybersecurity in Africa: Challenges and measures

Dr. DEHBI Abdelhakim

Ali lounici Blida 2 university Algeria
a.dehbi@univ-blida2.dz

Submission date: 27/02/2022 Acceptance date: 12/11/2022 Publication date: 29/12/2022

Abstract:

Cybercrime is a very complex phenomenon as it is constantly evolving; neither the state nor any other actor in the international system is immune to threats from cyberspace. In the 2015 International Telecommunication Union (ITU) report, "Global Cybersecurity Index", most African countries were ranked at the bottom of the world in terms of their commitment and preparedness to cyber security. In 2018, the same ranking confirmed that the vast majority of African countries are still weak in the face of cyber threats. Out of 54 countries, only a few countries such as Kenya and Rwanda are reported to have a high level of preparedness against cyber threats. This illustrates a vulnerability that needs to be diagnosed and addressed.

Key words: *cybersecurity, Cybercrime, global cybersecurity, Africa and cybersecurity*

ملخص

تعد الجريمة السيبرانية ظاهرة معقدة للغاية لأنها تتطور باستمرار، ولا يمكن لاي دولة او فاعل أخر في النظام الدولي ان يقوم بصدها بمفرده. حيث ان كل التدابير التي اتخذتها الدول المتقدمة في إطار الأمن السيبراني لم تكن كافية بأي حال من الأحوال لردع هذه الظاهرة.

في تقرير للاتحاد الدولي للاتصالات لعام 2015 ، تحت عنوان "مؤشر الأمن السيبراني العالمي" ، صُنفت معظم البلدان الأفريقية في أسفل السلم العالمي من حيث الالتزام بالأمن السيبراني والاستعداد لمختلف تحدياته. و في عام 2018 ، أكد هذا الترتيب نفسه حيث أن الغالبية العظمى من البلدان الأفريقية لا تزال ضعيفة في مواجهة التهديدات السيبرانية. فمن بين 54 دولة ، هناك عدد قليل فقط من الدول مثل كينيا ورواندا لديها مستوى عال من التأهب ضد التهديدات السيبرانية. مما يوضح الثغرة الأمنية الكبيرة التي يجب تشخيصها ومعالجتها.

الكلمات المفتاحية: *الفضاء السيبراني ، الأمن السيبراني ، النظام الدولي و الأمن السيبراني افريقيا و الأمن السبيراني*

Introduction:

For decades, physical security has been the priority for policy makers, but in recent years the need for protection has shifted from the "physical" to the "virtual", in other words, since cyberspace is used for geostrategic objectives, political activities, disinformation, and criminal and terrorist activities. It has also become an extension of power struggles, a powerful vehicle for political mobilisation and a new arena for political and social protest.

In cybersecurity, as in all aspects of security, states play a fundamental role. The regulation, management and establishment of mechanisms to ensure the rights and duties of users is a fundamental task in order to achieve the secure use of information systems that make it possible to exploit the advantages associated with the connected society.

A question that frequently arises at cybersecurity events is the question of where a given country ranks in terms of cybersecurity, both absolutely and relatively. It is difficult to provide a concrete and precise answer in a field where evolution is fast-paced and systems that are one day secure can be attacked by a new vulnerability at any time.

In the light of this uncertainty, it is generally accepted that the commitment of states to cybersecurity is an essential ingredient for the secure use of information systems by citizens. This commitment establishes the rights and obligations of the actors involved (users, providers, etc.) and provides the necessary mechanisms to take the necessary measures in the event of a breach of users' rights.

The assessment of states' commitment to cybersecurity is a complicated exercise that depends on a wide range of factors. Along these lines, numerous initiatives are emerging that aim to obtain an accurate picture with which to compare and detect the points of improvement on which a country can work.

Initiatives are taking place at different levels, whether global, as in the case of the United Nations through the International Telecommunications Union, regional, such as the European Union, the Organization of American States or the Union of South American Nations, or even national in those cases where there is no international body that brings together the interests in the field of cybersecurity of the members of the region.

Although attempts have been made to provide global coverage, in the case of Africa no specific document has been identified in which data from the region is specifically collected.

The problematic:

From all that has been said above, the States has to develop cybersecurity strategies to strengthen their control and power in order to tackle the cyber threats that will affect national cyberspace, so:

What are the cybersecurity challenges?

What are the different existing kinds of cyberattacks?

What are the measures and solutions by the world's states to ensure cybersecurity?

What predictions for the African national cyberspace?

Article structure:

Introduction

1- Terms Definition
2- The different kind of cybercrime and cybersecurity challenges
3- The global measures to ensure cybersecurity
4- Countries commitment and rankings for cyber security efforts
5- America and the European Union's vision
6- Africa cybersecurity efforts.

Conclusions

-1 - Terms Definition:

Global challenge definition:

1. **A challenge** is something new and difficult which requires great effort and determination.

2. **Global:** we can use global to describe something that happens in all parts of the world or affects all parts of the world (collinsdictionary., 2021, p. 22)

Kirsten Gelsdorf Definition:

According to Kirsten Gelsdorf global challenges are defined as any major trend, shock, or development that has the potential for serious global impacts. (Gelsdorf, 2010, p. 4)

Definition of the term "cybercrime

There is no precise and universal definition of the term "cybercrime". In general, terms, a crime is committed using a computer network or the Internet.

It can cover a wide range of activities, including terrorist activities and espionage conducted using the Internet and illegal hacking of computer

systems, content-related offences, theft and manipulation of data, and cyber-stalking (Dan Craigen & Thibault, 2014, p. 127).

Cyber Security definition

Here is some definitions of cybersecurity that we felt provided the right meaning and aims of cybersecurity (Dan Craigen & Thibault, 2014, pp. 14-15):

1. Cyber security is the application of technologies, processes and controls to protect systems, networks, programs, devices and data from cyber-attacks. It aims to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems, networks and technologies.
2. "Cybersecurity entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption."
3. "Cyber Security involves reducing the risk of malicious attack to software, computers and networks. This includes tools used to detect break-ins, stop viruses, block malicious access, enforce authentication, enable encrypted communications, and on and on.
4. "Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets.

2- The cybersecurity challenges

The more digital our society becomes, the more critical the issues become. Take the Covid-19 crisis and the role that digital technology has played in social relations, education, teleworking, trade and public information. The Internet and digital technology, in general, are at the heart of the issue of resilience, sovereignty and even economic competitiveness.

In the end, digitalization or digital transformation is only limited by the trust and resilience we give it. Cybersecurity will remain intimately linked to the digitalization of our society.
Every time a new system is put in place, potentially new risks can be created. With a digital world in constant evolution, today's difficulties will be different from tomorrows, and we must be aware of this dynamic of permanent change.

We have had cybersecurity topics on digitalization in factories, including sensitive and critical ones, digitalization of everyday objects, such as connected objects. We have to start dealing with the problems of hyper connectivity, or the increasingly massive use of artificial intelligence, big data and social media.

This is even a democratic issue today. What about tomorrow? We will have other topics, such as the massive use of drones and autonomous vehicles, the arrival of quantum technology, or the space revival.

- **The different kinds of cyber attacks**

Cyberattacks: cyberattacks are growing in number but also in ingenuity and no longer focus on one target but on its ecosystem, like the hacking of Airbus via its subcontractors like Altran.
Here are a few examples that have been on the rise in recent years (Ayofe & Irwin, 2010, pp. 58-68):

Ransonware: This software encrypts data and holds it hostage for ransom. The victim is forced to pay a ransom to regain access to their data. The FBI estimates that over the past six years, ransomware has earned hackers more than $140 million.

DDOS (distributed denial of service attack): the denial of service attack aims at over-soliciting a website, for example to saturate the site and force it to stop providing its service, for this or another purpose. In 2019, 8.4 million DDoS attacks were detected.

Acts of cyber warfare: Although still isolated, acts of cyber warfare are increasing. Examples include the US retaliation to attack a Russian troll factory or the attack on Iranian centrifuges by the Stuxnet malware.
There are as many reasons for attacking as there are attackers: money, political stakes, geopolitics, revenge, malice.

3- The global measures to ensure cybersecurity

Before taking a close look at the global measures taken to counteract cybercrime, the following question must be asked:
Why is international cooperation necessary to combat cyber threats?
The answer is this:
Due to the unpredictable nature of cyber threats, an incident that may initially appear to be a financially motivated act of hacking or cybercrime can quickly escalate into a national security incident or even a cyber war.

- **The role of the UN in cyberspace**

The objective of the UN is to strengthen security and consensus building on norms of behavior in cyberspace. However, currently there is no international cyber defence treaty-regulating cyberspace. Each state develops its national

defence policy and strategies with reference to its own legislation. States define their needs, expectations, the types of threats they face and the means to protect themselves, repair and prevent future attacks. Political and diplomatic negotiations for the elaboration of common doctrines as well as resolutions, conventions, codes of conduct to secure cyberspace and telecommunications come in a second stage. All this depends above all on the willingness of states to cooperate with other nations with the aim of creating a common regulated space. (Maurer Tim, 2011, pp. 41-43)

This process is moving quite quickly, as each state's legislation is evolving internally and, in parallel, negotiations on agreements are taking place at the United Nations. However, it remains complex, as the technical reality imposes its own frenetic pace and its own laws.

- **The Budapest Convention on Cybercrime 2001**

As legislators, parliamentarians can advocate for the ratification of and accession to international treaties that promote cybersecurity, as well as for the adoption and implementation of cybersecurity legislation in their respective countries to give effect to the obligations they assume under these international treaties. In this area, parliamentarians can encourage their respective governments to support, draft and pass the necessary implementing legislation.

The Budapest Convention on Cybercrime, which has 66 States Parties, serves as a guideline for any country developing comprehensive national legislation against cybercrime and as a framework for international cooperation among States Parties to this treaty. (New Zealand government, 2020, pp. 1-3) The Convention was adopted in November 2001. The year 2003 saw the adoption of a first additional protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems. Reflecting the new realities, important and urgent work is underway for the adoption of a Second Additional Protocol on strengthening international cooperation and access to evidence in the cloud.

Although it is a Council of Europe Convention, several non-member States of the Council of Europe were actively involved in the adoption of the Budapest Convention, including Canada and the United States, and it is open for ratification/accession by all countries. An increasing number of non-member countries of the Council of Europe have already taken this step in several regions of the world. There is therefore a great potential for PGA members to make essential contributions in many of today's non-state countries to promote the universality and implementation of the Budapest Convention. Cybercrime,

both direct and indirect, is one of the greatest, if not the greatest, threat to international peace and security today.

4- Countries commitment and rankings for cyber security efforts

The international telecommunication union **"ITU "** released on 9 December 2020, at the ITU Telecom World conference , the Global Cybersecurity Index, a research paper developing an index to assess nations commitment to cybersecurity. Countries were invited to participate on a voluntary basis by completing a form covering five aspects of the assessment (Global Cybersecurity Index2020, 2021, p. 8):

Legal measures

◦ Criminal legislation

◦ Regulation and compliance

Technical measures

◦ CERT-CIRT-CSIRT (CERT is Computer Emergency Response Team) - also called CSIRT (Computer security incident response team) - is a computer incident response team. The CERT-FR acts as the French governmental CSIRT.

◦ Standards

◦ Certification

Organic measures

◦ Policy

◦ Roadmap for governance

◦ Responsible body

◦ National benchmarking

Training

◦ Development of standardisation

◦ Workforce Development

◦ Professional certification

◦ Certification of bodies

Cooperation

◦ Intra-state cooperation

◦ Intra-agency cooperation

◦ Public-private partnerships

◦ International cooperation

After consulting all the countries in the world, 134 of the 193 member countries agreed to respond to the survey sent by the UN to the respondents. The countries that did not bother to answer the questions asked are not excluded from the ranking: the authors of the report used open source data to "fill in the blanks" and include all UN member countries in the study. and these are the results (Global Cybersecurity Index2020, 2021, p. 8):

Unsurprisingly, African countries are lagging behind on these issues. While Europe and North America are among the top-ranked countries in the index, Asia and South America show a more mixed picture, with some countries leading the way and others falling short.
In Europe, Estonia is the obvious leader. This country has decided to place the development of IT and networks at the heart of its policy, and the massive computer attack suffered in 2007 made it a forerunner in terms of cyber security. Estonia, in the city of Tallinn, is home to NATO's cyber defence cooperation centre and she made efforts in terms of its ability to raise awareness of cybersecurity issues.
Across the Atlantic, the United States leads the way, closely followed by Canada. Mexico comes third, but has a significant gap with the scores of the top two in several categories.
In Africa, the Republic of Mauritius takes first place, followed by Rwanda in second and Kenya in third. In the Middle East, the Sultanate of Oman came first, while Singapore took the top spot for the Asian regions.

5- America and the European Union's vision

The EU's assessment of a country's cybersecurity gives special attention to the existence of a cybersecurity strategy. On its website, it is possible to consult the list of countries that currently have a strategy or are in the process of developing one (Anagnostakis, 2021, pp. 243-261).

By region, Europe stands out, with a high percentage of countries that have already published a strategy or are in the process of developing one like (Ireland, Sweden and Montenegro), however Portugal, Iceland, Switzerland, Slovenia, Bosnia, Serbia, Croatia, the former Yugoslav Republic of Macedonia, Albania, Bulgaria, Moldova, Ukraine and Belarus are not on the list (Anagnostakis, 2021, pp. 243-261).
In North America, the United States and Canada also have their own cyber security strategies.
In South America, it is significant that only one country has a cybersecurity strategy, Trinidad and Tobago, while the other territories in the region that have a strategy are the overseas territories of France, the United Kingdom and the Netherlands. The remaining countries do not have a cybersecurity strategy, or at

least have not communicated it to ENISA.(ENISA is The European Union Agency for Cybersecurity.)

On the Asian continent, India, Russia and, although still in preparation, South Korea have a cybersecurity strategy. Notably absent from this list are Japan and all the countries of Southeast Asia, the first due to the deep penetration of new technologies in its population and the others due to the intense economic and commercial activity that is being concentrated in the area. China's absence from this list is also notable, which clashes with the intense cyber activity attributed to them internationally.

In Oceania, the two main countries in the region, Australia and New Zealand, have a cybersecurity strategy, as might be expected as a result of their close relationship with the United States, the United Kingdom and Canada, forming the Five Eyes group that collaborates in cybersecurity activities (Anagnostakis, 2021, pp. 243-261).

In contrast to this criterion, countries that do not have a security strategy score well in the ITU report, such as Brazil, Japan, Oman and Colombia, which exceed or equal Spain's ranking (Anagnostakis, 2021, pp. 243-261).

6- Africa’s cybersecurity efforts

Despite the fact that over the past decade, the African continent has made great strides in building the necessary information and communication technology (ICT) infrastructure ,only four African countries which are : South Africa, Kenya, Uganda and Rwanda, has a cyber-security strategy. However To strengthen the fight against cybercrime, the African Union (AU) adopted in 2014 - after four years of negotiation - a convention on cybersecurity and personal data protection.

The African Union Convention on Cyber Security

In recognition of the legislative challenges posed by criminal activities committed on ICT networks, in a regionally and continentally compatible manner, and also in response to the need to harmonize legislation in the area of cyber security and personal data protection in the Member States of the African Union The 23rd Assembly of Heads of State and Government of the AU, held in Malabo on 26-27 June 2014 adopted the African Union "Convention on Cyber Security and Protection of Personal Data" which is also known as the "**Malabo Convention".**

This convention aims to provide signatory states with a common legal framework regulating the activities of internet users. Although the initiative goes in a direction conducive to the fight against cybercrime, here too, some of the text's measures can be used to limit the freedom of expression of citizens of the countries concerned. As a result, the text has been hotly contested and, to date,

no AU country has ratified it, making the initiative a failure (Bada, 2021, p. 22). A handful of African countries have, however, acceded or are in the process of acceding to the Budapest Convention, drafted by the Council of Europe, which is more consensual in its content as it has already been ratified by 44, mostly European, countries.

Other initiatives are emerging to support the actions of States in the fight against cybercrime, such as the International Organization de la Francophonie (OIF), which aspires to become a framework for the exchange of best practices between the 80 Member States concerning cybercrime. Initiatives are also being structured at regional level, as shown by the rapprochement on these issues between the States of the Economic Community of West African States (ECOWAS) and the Council of Europe and the States of the East African Community (EAC) and the UN (Orji, 2015, pp. 115-118). Lastly, there are bilateral partnerships that countries can forge, such as the cooperation program between the ANSSI and the Senegalese Agence De l'Informatique de l'Etat (ADIE), the aim of which is to increase Senegal's cybersecurity capacities. Similar programs exist with Gabon and Morocco (Bada, 2021, p. 24).

The various regional initiatives mentioned are beneficial on two counts. They allow, within the same region, States at different levels of maturity to participate in a mutual assistance dynamic, whether in terms of judicial cooperation or the sharing of information and good practices. Furthermore, these initiatives involve non-African actors (international organizations or states) that have the expertise (training, education, knowledge of threats) and/or financial and material resources to support the efforts of African states. However, these cooperation mechanisms will only be effective, in the long term, if they are supported at national level by credible tools and instruments that serve a real political will to strengthen cybersecurity. This requires, among other things, the creation and effective implementation of a legal framework to combat cybercrime, dedicated police forces, a national information systems security strategy, a dedicated authority or a CERT.

Cyber security policy priorities in Africa:

a) Developing a strategic approach to dealing with different cyber threats.
b) Urging African states to put in place a National Cyber Security Framework:
c) Fight against all types of cybercrime at continental level.
d) Protection of Personal Data.
e) Capacity building and awareness raising
f) Strengthening regional and international cooperation. (Orji, 2015, pp. 115-118)

Some African case studies:

South Africa:

South Africa is among the top-ranked countries in terms of cyber security in Africa, of course, In March 2019 and in order to reinforce his cybersecurité strategie, the South African Parliament passed what called : the critical infrastructure legislation that aims to, enable the identification and designation of certain facilities as critical infrastructure; provide guidelines and factors to be taken into account to ensure the transparent identification and designation of certain facilities as critical infrastructure; and provide for measures to ensure the protection, preservation and resilience of such critical infrastructure. The Act also established a Critical Infrastructure Council; gave the Minister of Police the discretion to designate certain facilities as critical infrastructure; and prescribed the manner in which they are to be protected in the interests of national security (Sutherland, 2017, pp. 83-112).

Ghana:

Ghana is also one of the top-ranked countries in Africa in terms of cybersecurity and has its own strategy in this area and in In order to examine its cybersecurity capabilities, Ghana has developed a model to assess its level of cyber maturity by considering five dimensions:

- Cyber security policy and strategy
- Cyber culture and society
- Cybersecurity education, training and skills
- Legal and regulatory frameworks
- Standards, organisations and technologies.

The assessment was intended to help Ghanaian state authorities to better understanding of the country's cybersecurity strengths and weaknesses in order to invest more effectively in capacity building (Guide to good Gouvernance of e-Security, 2019, pp. 55-70).

Nigeria

Nigeria's National Cyber Security Strategy identifies individual users as the weakest link in the cyber security chain. Accordingly, the strategy calls for "initiatives and measures to help protect Internet users, and to provide materials and tools to protect Nigerian citizens from cyber threats and malicious acts"

The Algerian cybersecurity efforts:

At the international level Algeria has moved up 36 places from 112th to 67th position out of 193 countries concerned by the Global Security Index (GSI) for 2017. This is what emerges from a ranking established by the International Telecommunication Union (ITU), a body under the United Nations (UN). And in its Global Cybersecurity Index 2020, Algeria ranks 23rd in Africa for its level of cybersecurity.

Since the promulgation of Law 09-04 of 5 August 2009, which sets out special rules for preventing and combating offences related to information and communication technologies, Algeria has continued to invest in cyberdefence and new information systems, particularly through the toughening of crimes and offences committed by means of information and communication technologies, including malicious acts committed using mobile telephones (Global security index, 2021, p. 23).

Indeed, the proliferation of legal texts governing the abusive use of information systems and the protection of people and property has led to the ratification of numerous international conventions and protocols. This has given Algeria a place in the Geneva-based World Information Association.

A presidential decree was signed in January 2020 on the establishment of a "national information security and create a council and an agency whose respective missions are to draw up and implement this national information security strategy. It will make it possible to impose controls and protection standards. The implementation of this strategy, which is urgent, should face the challenges of cybersecurity, despite the accumulated delay.

Algeria's ranking in Comparison with its Neighbouring Countries

Ranking of Maghreb countries in terms of cybersecurity, according to the ITU (Global security index, 2021):

Tunisia: Index of 86.23/100 | 5 th in Africa.

Morocco: Index of 82.41/100 | 7 th in Africa.

Algeria: Index of 33.93/100 | 23 rd in Africa.

Libya: Index of 28.78/100 | 26th in Africa.

Mauritania: Index of 18.94/100 | 32nd in Africa.

Despite this ranking compared to our neighbours, Algeria has made a lot of progress. "However, it is necessary to move on to the phase of developing local content by creating a specialized center and encouraging the training of the necessary human resources

Conclusion

There is a growing awareness of the need to address cybersecurity issues jointly. This is evidenced by the increasing participation of states in various international initiatives that contribute to the sharing of information on risks and threats and provide the means to achieve a higher level of cybersecurity, such as exercises, training courses and the creation of points of contact between experts.

Against this trend towards collaboration, differences are also emerging due to the importance of information protection in today's knowledge society. Thus,

despite the increasing sharing of information, nations are also increasingly interested in having their own tools to preserve their independence and security.
The speed at which these initiatives are progressing contrasts with the rapid development that is taking place in the field of information technology and, above all, in the field of attacks and threats against systems. It is worth noting in this regard that countries that have been the target of attacks on their territory or information, such as the United States, Brazil, South Korea, etc., are the ones that currently have a higher degree of commitment and are moving more quickly in implementing standards and policies.
Finally, if there is a difference in the degree of commitment of Western countries to cybersecurity, the question arises; where the Arab and African countries stand in all this.

The following recommendation was made:

I. Cybersecurity is not just a matter for individuals and companies. At the government level, a whole range of political, legislative and organizational factors need to be taken into account to properly protect infrastructures and their users.
II. Accelerate the ratification and implementation of the AU Convention on Cyber Security
III. We should urges countries to increase their awareness of these issues, and reminds them that a high level of network and IT deployment does not automatically mean that this investment affects a country's cyber security capabilities.
IV. Cybersecurity, which should be a state of mind by default and a culture, is evolving very rapidly and is a growing challenge that Africa in general and Algeria in particular has no choice but to take up to defend its national strategic interests.
V. Develop capacity in cyber diplomacy and participate in international discussions discussions at the international level such as the United Nations Group of Governmental Experts.
VI. African nations, including Algeria, need to build a series of digital barriers in the form of legislation to address cybercrime, multilateral agreements, and the development of technical capacity in this area such as cyber security centers.

Bibliography:

Review:

1. Azeez Nureni Ayofe, Barry Irwin **Cyber security: challenges and the way forward,** GESJ: Computer Science and Telecommunications |No.6(29) 2010
2. Dan Craigen, Nadia Diakun-Thibault, and Randy Purse , **Defining Cybersecurity** , Technology Innovation Management Review , North Carolina State University , USA ,October 2014
3. Dimitrios Anagnostakis , **The European Union-United States cybersecurity relationship: a transatlantic functional cooperation** Journal of Cyber Policy Volume 6- Issue 2, Taylor & Francis UK 2021 .
4. Maurer, Tim, **—Cyber Norm Emergence at the United Nations – An Analysis of the UN's Activities Regarding Cyber-security?**, Discussion Paper 2011-11, Cambridge, Mass.: Belfer Center for Science and International Affairs, Harvard Kennedy School, September 2011
5. Sutherland, EMEN **Governance of cybersecurity – the case of South Africa**. The African Journal of Information and Communication (AJIC), 2017
6. Uchenna Jerome Orji Multilateral **Legal Responses to Cyber Security in Africa: Any Hope for Effective International Cooperation**? 7th International Conference on Cyber Conflict: Architectures in Cyberspace NATO CCD COE Publications, Tallinn Estonia. 2015
7. **Guide to good Gouvernance of e-Security** , Le Centre pour la gouvernance du secteur de la sécurité, Genève – 2019.
8. **Global Challenges and Their Impact on International Humanitarian Action** , OCHA Occasional Policy Briefing Series Brief No. 1, OCHA Policy Development and Studies Branch,2010 .

Electronic sources:

1. **Global Cybersecurity Index 2020** International Telecommunication Union ITU, Geneva, 2021 p 08 available at : https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
2. Maria Bada Reviewing National Cybersecurity Awareness in Africa available at https://core.ac.uk/download/pdf/211243124.pdf
3. **What is the Budapest Convention?** New Zealand government, cybersecurity. 15 July 2020 page 1-3 at https://consultations.justice.govt.nz/policy/budapest-convention/user_uploads/1.-what-is-the-budapest-convention.pdf