PGA REGIONAL AFRICAN WORKSHOP ON CYBERCRIME: IMPACT OF CYBERCIME AND THE ROLE OF PARLIAMENTARIANS IN PROMOTING CYBERSECURITY AND PREVENTING CYBERCRIME

ADV. LUFUNO T KHOROMMBI
AWARD WINNING DATA PRIVACY
AND CYBERLAW PROFESSIONAL

AGENDA

- OUTLOOK OF THE REGULATORY FRAMEWORK
- MALABO CONVENTION SIGNATORIES AND RATIFICATIONS
- OUTLOOK OF THE MEMBER STATES CYBERSECURITY CULTURE
- OVERVIEW OF CYBERCRIME IN AFRICA
- IMPACT OF CYBERCRIME ON WOMEN
- OVERVIEW OF CYBERCRIME IN SOUTH AFRICAN
- OUTLOOK OF THE REGULATORY ENVIRONMENT IN SOUTH AFRICA
- CHALLENGES
- RECOMMENDATIONS / ACTION PLAN
- CONCLUDING REMARKS

Outlook of the regulatory framework

AU Agenda 2063	Malabo convention	Digital Transformation Strategy 2030
CYBER SECURITY is included as part of the flagship programme of Agenda 2063, a clear indication that Africa needs to not only incorporate in its development plans the rapid changes brought about by emerging technologies, but also to ensure that these technologies are used for the benefit of African individuals, institutions or nation states by ensuring data protection and safety online. **The Cyber Security project is guided by the African Union Convention on Cyber Security and Personal Data Protection.**	The Malabo Convention envisions Africa as a single entity in terms of data and privacy protection and **calls for a harmonized, independent, and robust legal framework which protects all people from processors and data controllers**. The unified legal framework, therefore, aims at strengthening accountability from data controllers by defining the roles and responsibilities of state parties in precise terms as liable entities. It provides **for collaboration between public and private actors, civil society, and academia and encourages international partnerships in the promotion and enhancement** of a culture of cybersecurity.	The strategy objectives includes inter alia "**Entry into force of the Malabo Convention and for all Members States to adopt a complete set of legislation** covering e-Transactions, Data Protection and Privacy, Cybercrime and Consumer Protection." **Enable the coherence** of existing, future digital policies and strategies at regional and national levels and **mobilize effective cooperation** between institutions. Recognizes that digitalization is creating jobs, addressing poverty, reducing inequality, facilitating the delivery of goods and services, and **contributing to the achievement of Agenda 2063 and the Sustainable Development Goals**.

Malabo Convention signatories and ratification

No.	Member State	Signature	Ratification	Deposited
1)	Angola	X	2020	2020
2)	Benin	2015	X	X
3)	Cameroon	2021	X	X
4)	Cape Verde	X	2020	2022
5)	Chad	2015	X	X
6)	Comoros	2018	X	X
7)	Congo	2015	2020	2020
8)	The Gambia	2022	X	X
9)	Ghana	2017	2019	2019
10)	Guinea	X	2018	2018
11)	Guinea Bissau	2015	X	X
12)	Mozambique	2018	2019	2020
13)	Mauritania	2015	X	X
14)	Mauritius	X	2018	2018
15)	Namibia	X	2019	2019
16)	Niger	X	2022	2022
17)	Rwanda	2019	2019	2019
18)	Senegal	X	2016	2016
19)	Sierra Leone	2016	X	X
20)	Sa Tome and Prencipe	2016	X	X
21)	Togo	2019	2021	2021
22)	Tunisia	2019	X	X
23)	Zambia	2016	X	X

Out of 55 Member States, only 16 have signed the Malabo Convention between 2015 and 2022; and only 13 have ratified and deposited between 2016 – 2022; which constitute about 29.091% and 23.64% respectively.

Outlook of the Member States Cybersecurity Posture

No.	Member State	Malabo	Budapest	Rankings – Africa	Rankings - Global	Rankings - Africa	Rankings - Global	Maturity
1.	Cameroon	2021 (Signed)	X	13 – 2020	93 - 2020	09 – 2017	75 - 2017	Regressed
2.	Comoros **	2018 (Signed)	X	20 listed with Arab region	175	20	161	Regressed
3.	DRC	X	X	40	170	40	161	Initiating
4.	ESwatini	X	X	26	135	38	160	Advanced
5.	The Gambia	2022 (Signed)	X	20	107	25	130	Advanced
6.	Kenya	X	X	5	51	3	45	Regressed
7.	Malawi	X	X	16	97	29	145	Advanced
8.	Seychelles **	X	X	30	149	19	115	Regressed
9.	South Africa **	X	Signed / yet to accede	8	59	6	58	Regressed
10.	Tanzania	X	X	2	37	11	88	Matured
11.	Togo	Ratified 2019 /2021	X	19	105	15	107	Improved
12.	Uganda	X	X	9	72	5	50	Regressed
13.	Zimbabwe	X	X	17	98	18	113	Advanced

The Regional rankings are directly derived from the Global rankings. E.g. Tanzania is rated 45 in the global rankings, which translate to number 2 in the Regional rankings.

**** means no response to the questionnaire/data collected by GCI Team (2020)**

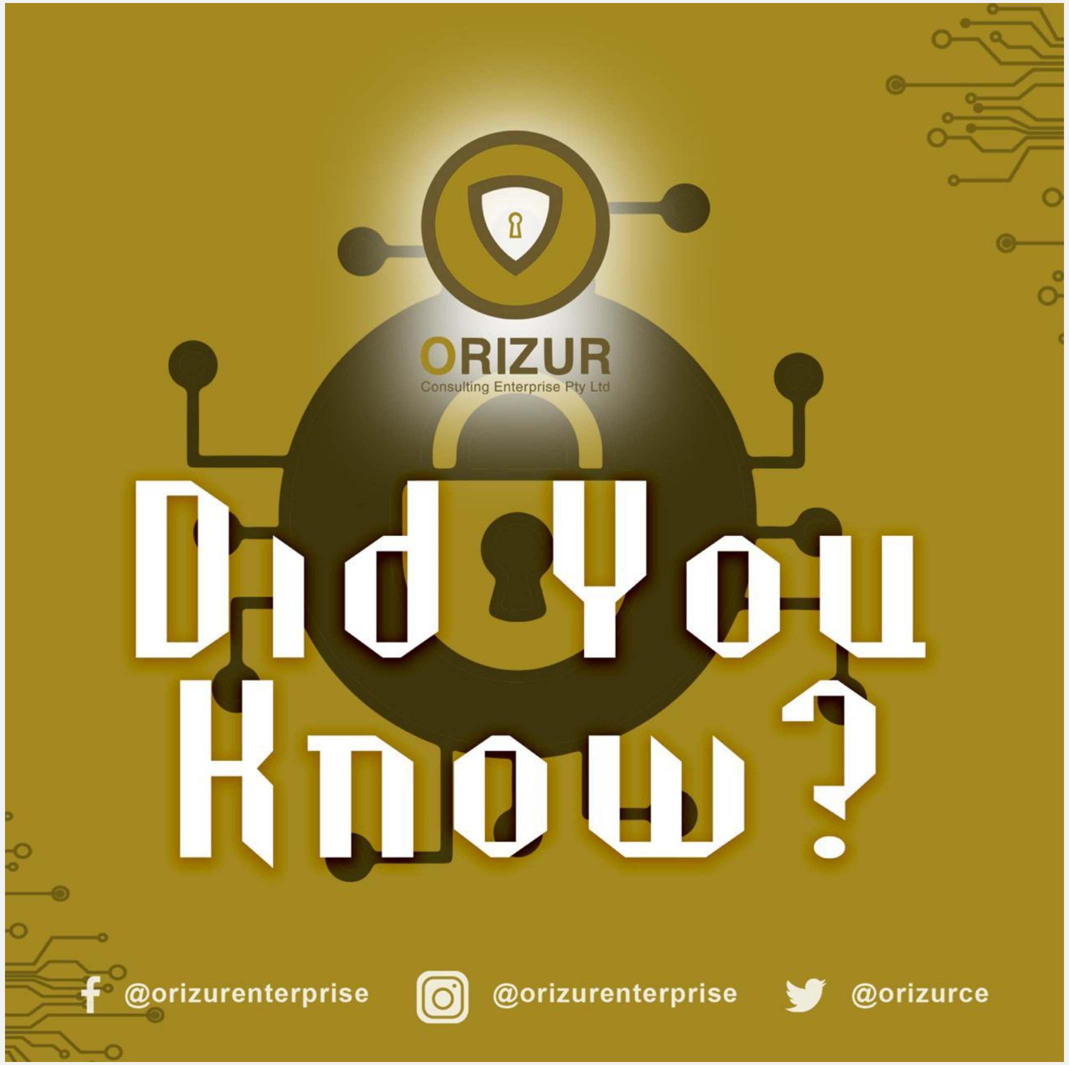
Outlook of the Member States Cybersecurity Posture

- ITU Global Cybersecurity Index (GCI) assessment report published in June 2021 looks into the following assessment measures to rank countries on their cybersecurity journey:
  - legal, technical, organizational measures, capacity development, and cooperation.
  - {* means no data collected / ** means no response to the questionnaire}
- Leading countries are Mauritius (17 – dropped from number 7 in 2017 report), Egypt (23 from 14), **Tanzania** (37 from 88) and **Ghana** (43 from no. 87).
- Though Mauritius regressed from top 10, to top 17 in the global ranking, it retained its first position in the Region.
- Tanzania moved from 11 to 2, displacing Rwanda, Ghana moved from 10 to number 3, displacing Kenya. Nigeria kept its spot @ no. 4.
- There were no African countries in the top 16. Based on the ITU Global Cybersecurity Index, published in 2021, Africa is lagging behind, with only 20 countries in the top 100 out of 182
- **None of the Member States have ratified the Malabo Convention, whilst only 6 have acceded to the Budapest Convention** – Cabo Verde (2017), **Ghana** (2017), Mauritius (2013), Morocco (2021), **Nigeria** (2022), and Senegal (2016)

Overview of cybercrime in Africa - What is Cybercrime?

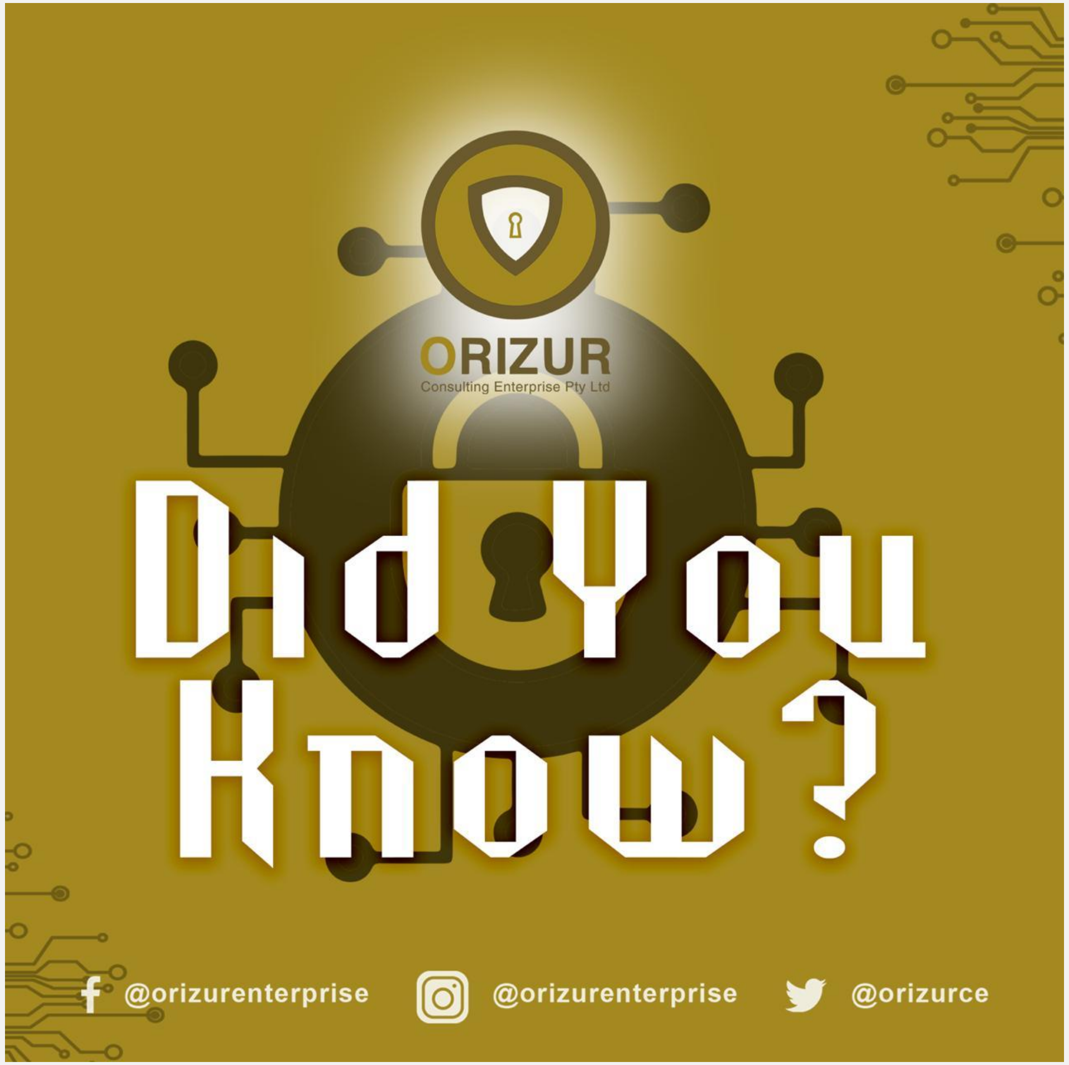
- Cybercrime is defined as the use of computers and digital platforms to commit illegal activities and can be driven by different motives, such as revenge or monetary gain.
- As information technology becomes more embedded in our society, cybercrime has become a common hazard on a global scale.
- It is one of the fastest growing criminal industries worldwide.
- It is estimated to cost the world more than $10 trillion annually in 2025, making the illicit industry more profitable than the cross-border trade of illegal drugs.
- The evolving cybercrime landscape and skills gaps in the teams investigating cybercrimes remain a significant challenge for law enforcement agencies and prosecutors, especially for cross-border enforcement.

Overview – cybercrime in Africa



- Cybercrime is one of the top risk factors likely to jeopardise Africa's economy especially at this time when the Continent is transitioning to e-commerce under the African Continental Free Trade Agreement (AfCFTA).
- The more reason why the ratification of the Malabo Convention has become a necessity to inter alia ensure a safe digital space for AfCFTA participants.
- It is said that Africa loses a '**minimum**' of \$4.2 billion per annum from GDP to cybercrime, an increase of 10 % from \$3.5 billion in 2017.
- South, Nigeria, and Kenya are said to be accounting for most of the loses respectively.

Overview – cybercrime in Africa



- ITU GCI 2021 report highlights that cybersecurity efforts, level of commitment to cybersecurity as well as capacity building for response to threat remain low compared to other regions.
- Thus, the lack of interest in ratifying and accession both the Malabo and Budapest Conventions has made Member States negligent in setting up institutional and human capital investment in this area.
- Based on the ITU Global Cybersecurity Index, published in 2021, Africa is lagging behind, with **only 20 countries in the top 100 out of 182.**

Top 20 Countries in the Top 100 based on their Global Ranking of the ITU GCI Report

Top 20 listed under African Region

Mauritius - 17

Tanzania - 37

Ghana -43

Nigeria – 47

Kenya – 51

Benin- 56

Rwanda – 57

South Africa – 58

Uganda – 72

Zambia -73

Cote d’Ivoire – 75

Botswana – 88

Cameroon – 93

Chad – 95

Burkina Faso – 96

Malawi – 97

Zimbabwe – 98

Senegal - 100

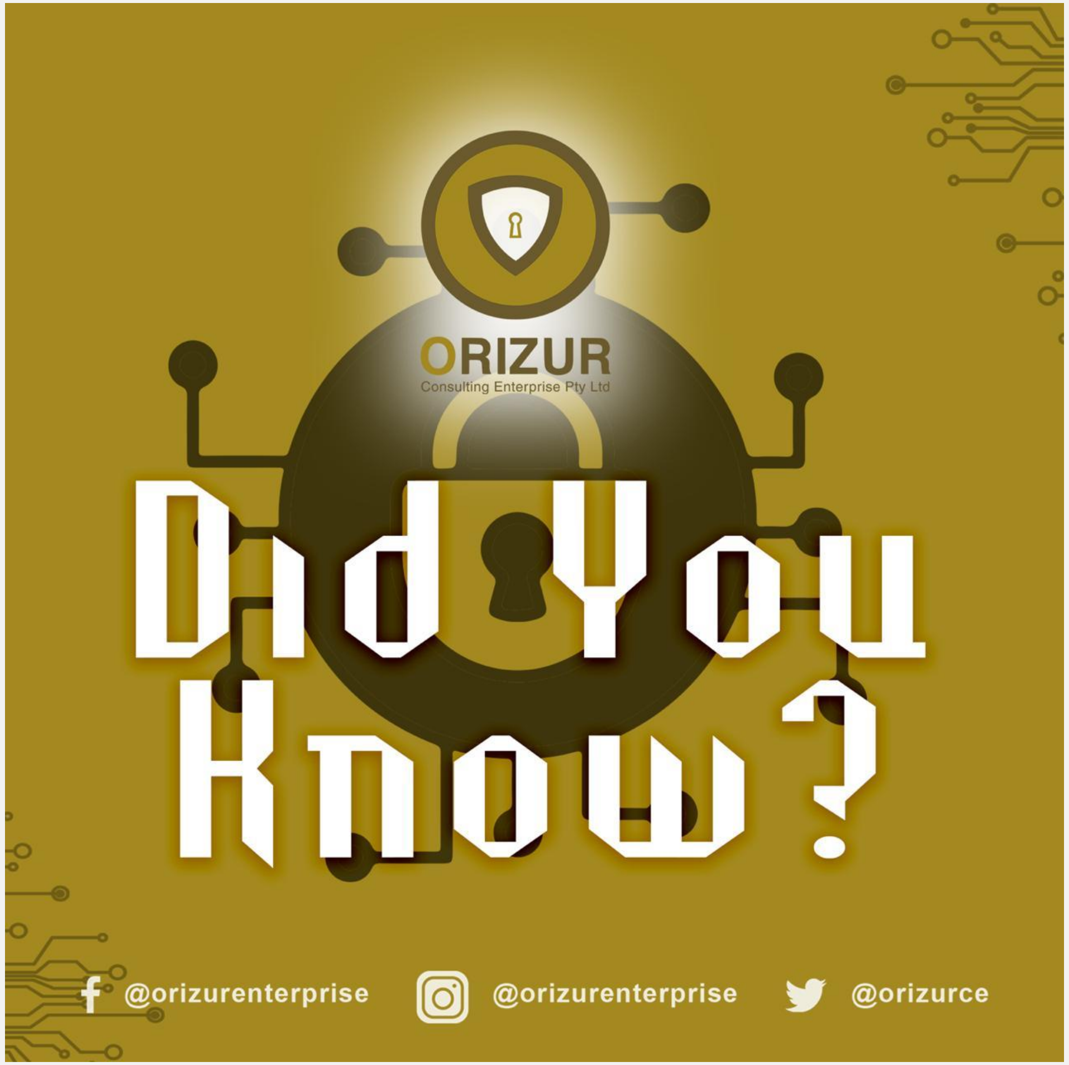
Too 20 listed under Arab States

Egypt - 23

Tunisia – 45

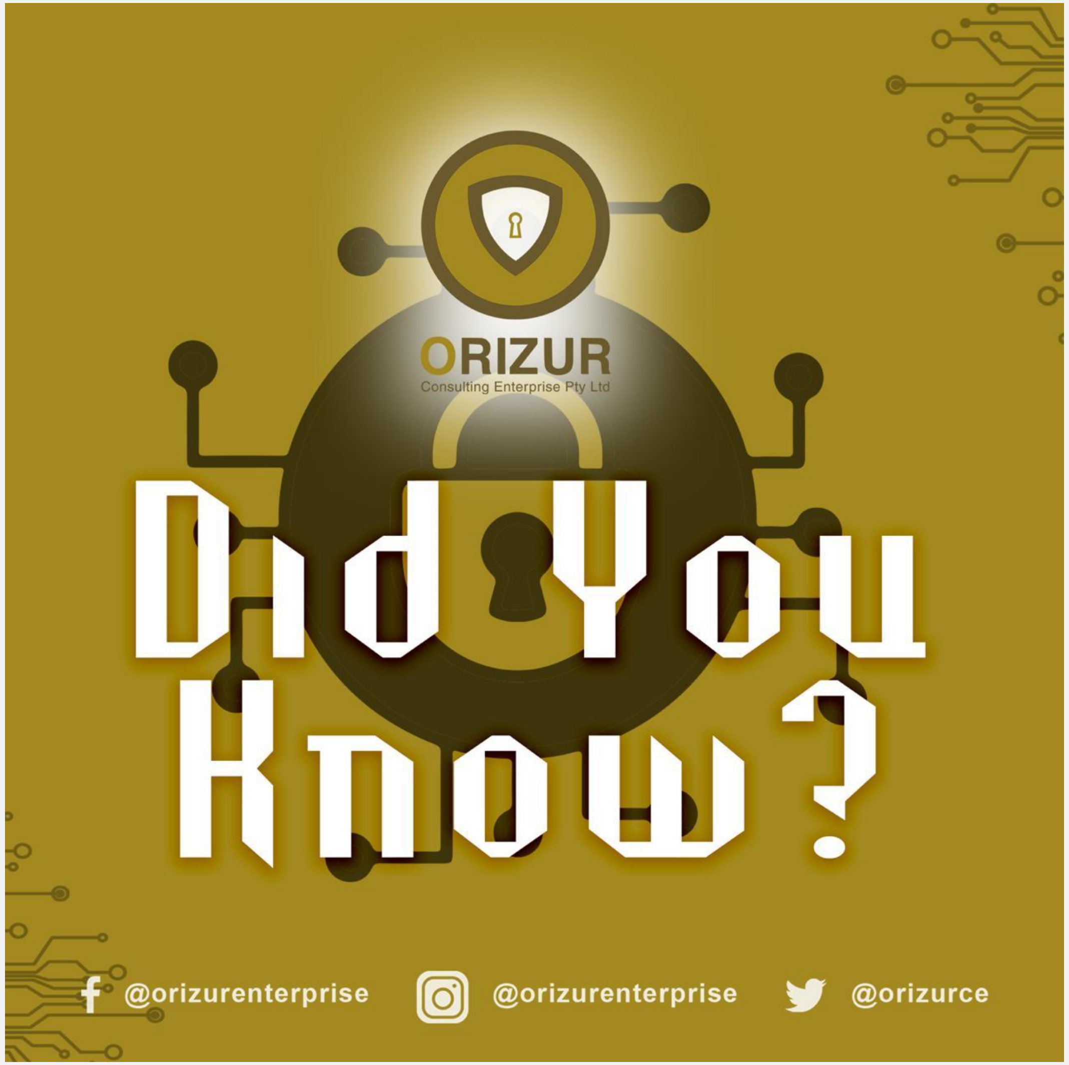
Morocco - 50

Impact of cybercrime on Women



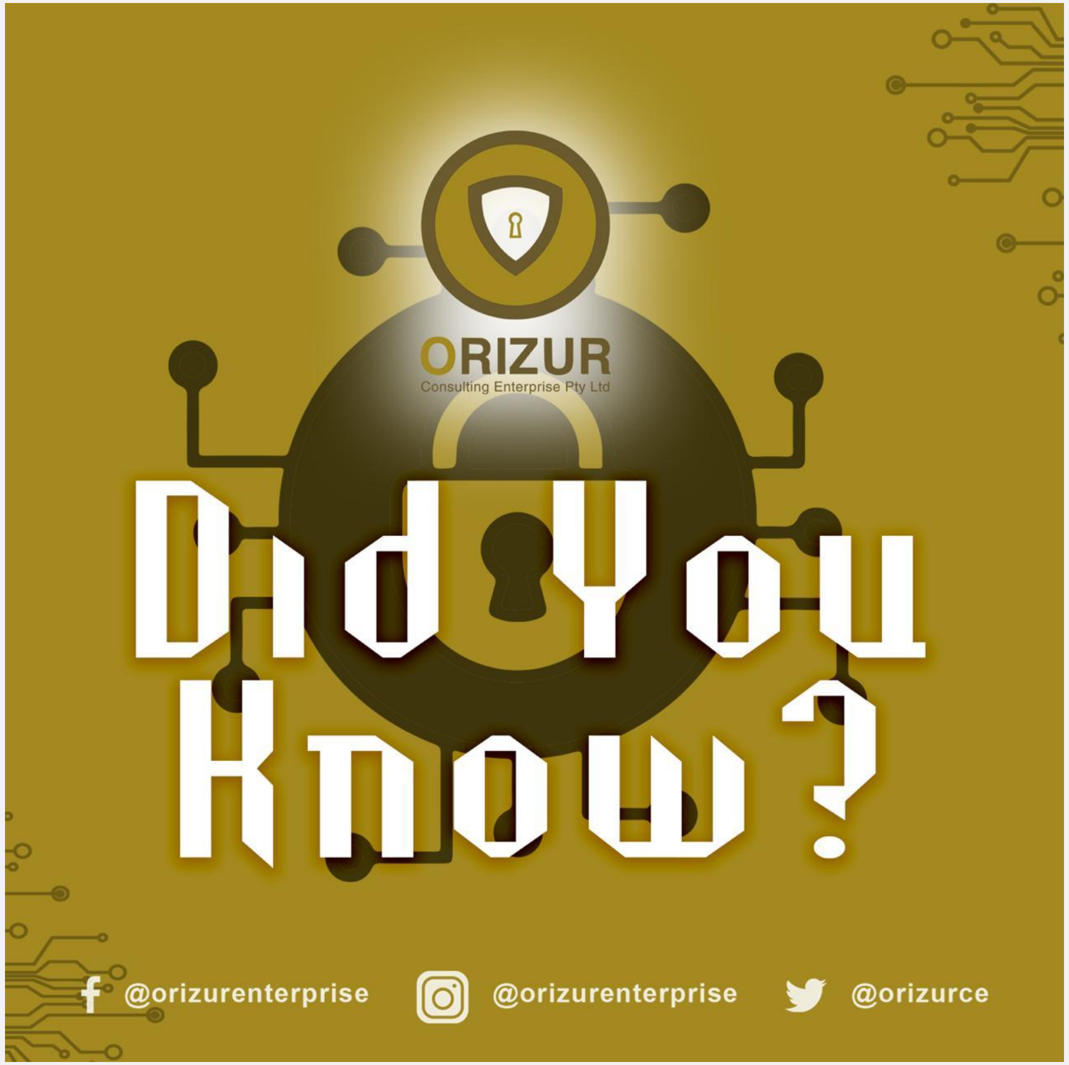
- Technological innovation has profoundly transformed societies around the world. Harnessing ICTs to advance gender equality and women’s empowerment is not only vital for women and girls, but critical for achieving the 2030 Agenda for Sustainable Development.
- However, it is often said that technologies such as the internet or mobile phones are a double-edged sword, since these digital spaces have also provided tools and platforms for the replication and continuation of the perpetration of violence against women and girls.
- E.g. Social networking websites make it easier for perpetrators to monitor their targets, obtain personal information, and repeatedly send undesirable messages.

Impact of cybercrime on Women



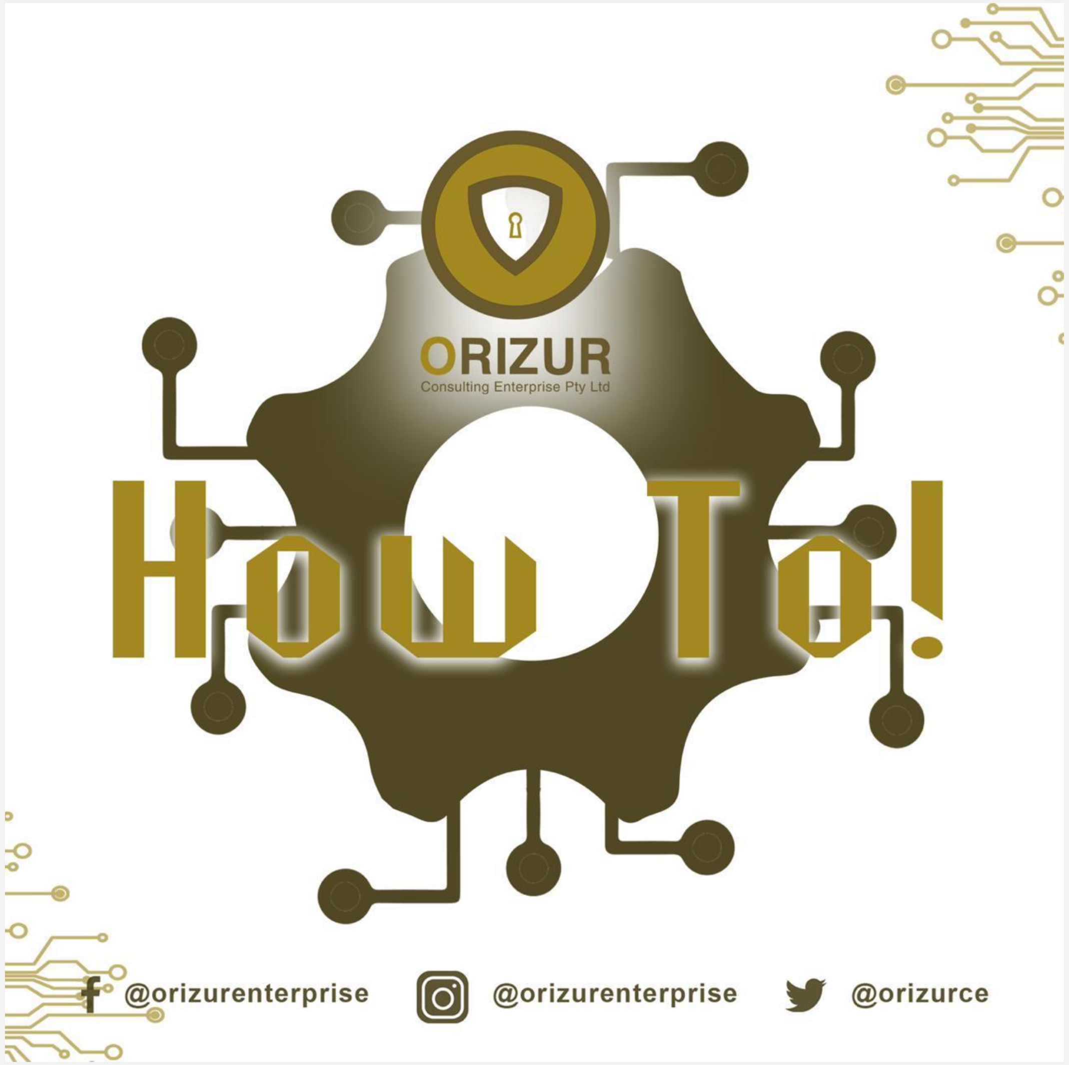
- Technology assisted violence against women and girls could significantly increase this staggering number, as reports suggest that 73 per cent of women have already been exposed to or have experienced some form of online violence in what must still be considered a relatively new and growing technology.
- Statistics on violence against women showed that more than 1 in 3 women (36.6 per cent) in Africa report having experienced physical, and/or sexual violence by a partner or a non-partner.
- **I concur with UN's assertion that Violence against women and girls is a grave violation of human rights**, which led to the adoption of the 1993 Declaration on the Elimination of Violence against Women.

Impact of cybercrime on Women



- It is most unfortunate that online threats of violence against women and girls are often trivialized or minimized by the public (and the authorities), with perpetrators experiencing little or no consequences for their behavior. Technology therefore facilitates the proliferation of gender biase hate and harassment.
- Thus, though the African Union Agenda 2063 recognises the role of women and youth in driving digital transformation and economic development, their being exposed to cyber vulnerabilities is counterproductive.
- The reason why I agree with WEF that Africa must act now to address cybersecurity threats.

Impact of cybercrime on Women



- In addition to implementing the generally applicable rules of international law, as provided under the UN Charter and other human rights treaties, Member States are encouraged to implement sectoral and regional treaties that have been adopted to regulate the cyber activities including:
  - 2014 Malabo Convention;
  - the 2001 Budapest Convention on Cybercrime & its two protocols 2006 and 2021;
  - the 2009 Shanghai Cooperation Organization's Information Security Agreement;
  - the Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa 2003 (Maputo Protocol).
  - 1993 Declaration on the Elimination of Violence against Women (UN Resolution 48/104)
  - 1992 Constitution of the International Telecommunication Union

Overview of cybercrime in South Africa

ORIZUR Consulting Enterprise Pty Ltd

Outlook

- FBI 2021 survey revealed prevalent threats include malware (like ransomware), viruses (like Trojan), hacking (like data breach), cyber-fraud (like bank fraud), and cyber-theft (like identity theft).
- Most of the victims come from the three of the BRICS countries: Russia (85%), China (77%), South Africa (73%).

Regulatory environment

- ICT policies and laws are for the most part gender-blind and do not focus on how men and women are impacted differently. Even less do they consider violence against women and girls.
- For example, the national ICT legislation on cybercrimes only focus on high-profile crimes not on the violation of the women specific digital human rights.

Prevalence of Cybercrime

- South Africa is a country with high levels of inequality, with the first and second economies, majority of its people falling under the second economy.
- Digital divide is also widening due to inter alia issues of connectivity and digital illiteracy.
- Moreover, South Africans loses a minimum of R2.2 billion per annum to cybercriminals, and women are most at risk

SA's rankings & participation in the regional and international community

Ranked 6th in cybercrime density in the world - Surfshark

Have not signed or ratified Malabo Convention

Ranked 1st in the Interpol Cybercrime Report 2021

Have not ratified and or implemented SADC Model Laws

Ranked 59th in the ITU Global Cybersecurity Index

Signatory, but yet to accede to the Budapest Convention

Comparison of ITU GCI Ranking For BRICS Countries

No.	BRICS	Ranking (out of 182) - 2020	Ranking - Regional	Ranking (out of 193) - 2017	Ranking - Regional
1)	Russia	4	1	10	2
2)	India	10	4	23	8
3)	Brazil	18	3	38	5
4)	China	33	8	38	9
5)	South Africa	59	8	58	6
Cyber Defense Index 2022/23					
1)	China	12			
2)	India	17			
3)	Brazil	18			

- ITU GCI – All of the BRICS Countries have tremendously improved with the exception of South Africa.
- *Cyber Defense Index assesses top 20 of the world’s major economies.

Consequences of Cybercrime in South Africa

- In May 2022, a data leak at Transunion, a credit management company, reportedly compromised the personal information of 54 million South Africans. Victims of this attack included President Cyril Ramaphosa.
- In 2021, a successful cyber-attack on Transnet, the container terminals of the transport parastatal was brought to a standstill, disrupting imports and exports.

- I fully agree with Dlamini & Mbambo (2019) that "the policing of cybercrime is generally an afterthought for many organisations, including government, and individuals in South Africa."
- Based on the statistics and increase in cyber-attacks, it is evidenced that cybercrime continues to be a detrimental problem for South Africa.

Outlook of the regulatory environment in south Africa

- Constitution of 1996
- Minimum Information Security Standards (MISS) approved by Cabinet 1996
- Presidential Review Commission, 1998
- State Information Technology Act (SITA) 1998 as amended and Regulations 2005
- E-Government Policy, 2001
- Minimum Interoperability Standards (MIOS) 2002, as amended
- Electronic Communications and Transactions Act, 2002

‘

- Regulation of Interception of Communications and Provision of Communication-related Information Act (RICA), 2002
- Electronic Communications Act, 2005 (the ECA)
- Information Society and Development (ISAD) Plan, 2007
- National Development Plan (NDP), 2011 – vision 2030 (Chapters 4 &13)
- The Protection from Harassment Act, 2011 – came into effect 27th April 2013

Outlook of the regulatory environment in south Africa

- National Cybersecurity Framework, 2015
- **National ICT Integrated Policy White Paper**, 2016 – All encompassing convergence policy document on ICT
- National e-Government Strategy 2016/17
- **Protection of Personal Information Act, 2013** – came into effect on 1 July 2020, & enforcement 1 July 2021
- **Critical Infrastructure Protection Act**, 2019 – yet to come into effect
- **Cybercrime Act, 2020** – effective date of some of the provisions of the Act was 1 December 2021
- **Film and Publication Amendment Act 2019** - came into effect on 1 March 2022.

Are The Regulatory Frameworks Effective, If Not, What Are The Current Challenges?

ORIZUR
Consulting Enterprise Pty Ltd

The regulatory environment has not been effective, and the following are inter alia the reasons:

Apart from the fact that the tech world is dynamic, making it difficult for the legislature to keep up. It does seem like despite all its efforts, the **implementation of legislation to counter cybercrime and ensure data protection remains challenging**.

Siloed approach – currently, **a number of legislations are in place, governed by different departments**. Coordinating efforts that would result into one legislation for cybersecurity would add value to the cyber security environment. **At present, the current legal framework relating to cybersecurity is hybrid of different pieces of legislation and common law**

Lack of skills remains a thorny issue. Moreover, SITA Strategic Plan 2020-2024 states that **SITA is well positioned to be an enabler for the Government's digital transformation journey. However, acknowledges that there is lack of skills for within SITA (and the public sector in** general).

Cyber security culture remain the number one contributor to data breaches due to inter alia non-compliance and poor cybersecurity governance, possibly as a result of inter alia skills shortage

Cyber security is yet to become a priority – the advent of covid-19 dictated that we effectively deal with two pandemics – one being covid-19 and the other being cybercrime. However, **cybersecurity has remained a by the way.**

Lack of political will and cybersecurity awareness remain the biggest challenge for both the industry and the nation in general. Most probably, one of the main contributing factors to the persisting cyber challenges

What Should Be Done To Enable Implementation / Enforcement

Fighting cybercrimes must be a governance issue - Driven from the Head of State and Cabinet

Skilled cyber practitioners and advisors are vital

N.B. development of a responsive curriculum is key to afford talented young people opportunities for employment

Promote local content by developing regional capacity and capabilities to combat cybercrime

Public-private partnership is imperative - and must be established as soon as possible to combat cybercrimes as provided for in the original National Cybersecurity Policy Framework of 2013.

Do away with silos (across the board) in favour of collaborative efforts that enable sharing of scarce cybersecurity skills and other resources to reduce vulnerabilities and duplication

Political leaders should champion and resource the capacity building and skills development efforts to enable implementation and enforcement of the existing legal framework

Recommendations / Action Plan

- At the rate within which cybercrime is happening, I want to agree with Ms. Awa Ndiaye, President of the Commission for Data Protection (CDP), Senegal, who was speaking at the 2021 3rd Data Privacy Symposium that "*African States need to prioritize the ratification of the Malabo Convention as a document of relevance to the lives of their people*."

- This requires political will, mainly because cybersecurity is a governance issue, first.
- Existing national legislation are commendable, but limited in terms of jurisdiction. Moreover, it is often difficult to identify and trace cyber criminals, assesses the extent and impact of their offenses, and collect and analyse related digital evidence.

Recommendations / Action Plan

- In essence, cybercrime is a borderless crime which cannot be effectively dealt with using domestic laws and limited human, technological, and financial resources.
- It will serve South Africa and other Member States well to participate in the regional and international forums, which is likely to help curb cybercrime in the country and within the region of Africa.
- Cooperation with regional and international community within the ambit of Malabo Convention and Budapest Convention is likely to improve South Africa's rankings and reduce the high rate of cybercrime.
- Similarly, it is likely to assist other Member States to improve their cybersecurity posture.

Recommendations / Action Plan

- The panelist at the 2021 3rd Data Privacy Symposium, submitted that the lack of interest in the Convention has made States negligent in:
  - evaluating the cost of cybercrime to national economies,
  - setting up institutional and human capital investment in cybersecurity and
  - fighting against the cybercrime pandemic.
- As part of the implementation of the critical Infrastructure protection act, it will also serve a great purpose for South Africa to have a thorough understanding of the cyber threats and attacks because the implementation of an effective cybersecurity governance framework has never been so urgent.
- This requirement applies to all Member States.

Recommendations / Action Plan

Prioritisation of the implementation of legal prescripts	Harmonisation of the regulatory environment	Improved cyber environment	Trust driven environment	Security by design – not checklist
The unpredictable data safety environment does not only threaten Africa's emerging e-commerce industry but other sectors such as the Civil Society, Academia among others, which are crucial for the socio-economic growth and development in Africa.	Malabo Convention provides for collaboration amongst multi-stakeholders and encourages international partnerships in the promotion and enhancement of a culture of cybersecurity.	Collaboration and partnerships amongst role players to share resources and insights would lead to a risk-based and globalized strategy – mainly because "Muima woga" (standalone) culture in a networked digital world is no longer sustainable.	Risk base approach to enforce digital human rights will minimize online vulnerabilities. Therefore, Government should adopt and establish a zero trust framework. NIIST has some great reference resources.	POPI Act requires organisations to develop and improve their own cybersecurity measures to limit the risk of a data breach. OpenChain ISO/IEC 5230, is the Open-Source Software Supply Chain Management Standard that embeds security by design.

Concluding remarks

- Africa is yet to recognize the importance of cybersecurity and the devastating impact of cybercrime.
- This is evident in the lack of political will to bring into effect the Malabo Convention and to join forces with the international community in the fight of cybercrime through the Budapest Convention.
- Considering the borderless nature of cybercrime, making the need for global collaboration a strategic must, I believe it is imperative that African Heads of State, and Parliamentarians come to a realization that the devastation nature of cybercrime threatens the very sovereignty of their States. Thus, cybersecurity can no longer be an afterthought, but critical to the effective functioning of every State.

Cybercrime is:
A pandemic that can no longer be an afterthought.
A well-funded organised crime.
A lucrative business that thrives on ignorance of its victims.
Estimated to cost the world more than $10 trillion annually in 2025, making the illicit industry more profitable than the cross-border trade of illegal drugs.

Within this context, a passive approach in fighting cybercrime is no longer good enough. Thus, the by the way approach only exacerbates the devastating nature of cybercrime.

References

- Malabo Convention
- List of Member States Which Have Signed, Ratified / Acceded To The Convention - https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION.pdf
- UN Agenda 2063 – Flagship projects - https://au.int/en/agenda2063/flagship-projects
- The African Union Digital Transformation Strategy for Africa (2020-2030) - https://au.int/en/documents/20200518/digital-transformation-strategy-africa-2020-2030
- ITU GCI 2017 Report - https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf
- ITU GCI 2020 Report - https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
- Budapest Convention accession - https://www.coe.int/en/web/cybercrime/parties-observers
- Overview cybercrime - https://www.controlrisks.com/our-thinking/insights/how-the-south-african-cybercrimes-act-19-of-2022-will-affect-individuals-and-businesses
- Safe Digital Spaces: Protection Of Women And Girls From Technological Violence – Un Women 2019
- Research synthesis of cybercrime laws and COVID-19 in Indonesia: lessons for developed and developing countries - https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9464486/#CR23
- Cybercrime, A barrier to Africa’s thriving digital economy: https://repository.uneca.org/handle/10855/46669
- Cost of cybercrime - file:///C:/Users/USER/Downloads/AfricanCyberthreatAssessment_ENGLISH-2.pdf
- Technology- Facilitated Gender- Based Violence: What Is It, And How Do We Measure It? International Centre for Research on Women – 2018
- Malabo Convention: African Data Regulators call for Action - https://www.unwantedwitness.org/malabo-convention-african-data-regulators-call-for-action/
- Understanding policing of cybe-rcrime in South Africa: The phenomena, challenges and effective responses file:///C:/Users/USER/Downloads/DlaminiandMbambo-1.pdf
- OPINION | 5 things SA must do to beat cybercrime - https://www.news24.com/fin24/opinion/opinion-5-things-sa-must-do-to-beat-cybercrime-20220906