

Cybersecurity in Africa



BY **AYSHA JERIDI**

**Executive Director Network Of African Women In Cybersecurity
(NAWC)**

Agenda

01

Overview

02

Legal Framework

03

Main Challenges

04

Who Attacks
Africa?

05

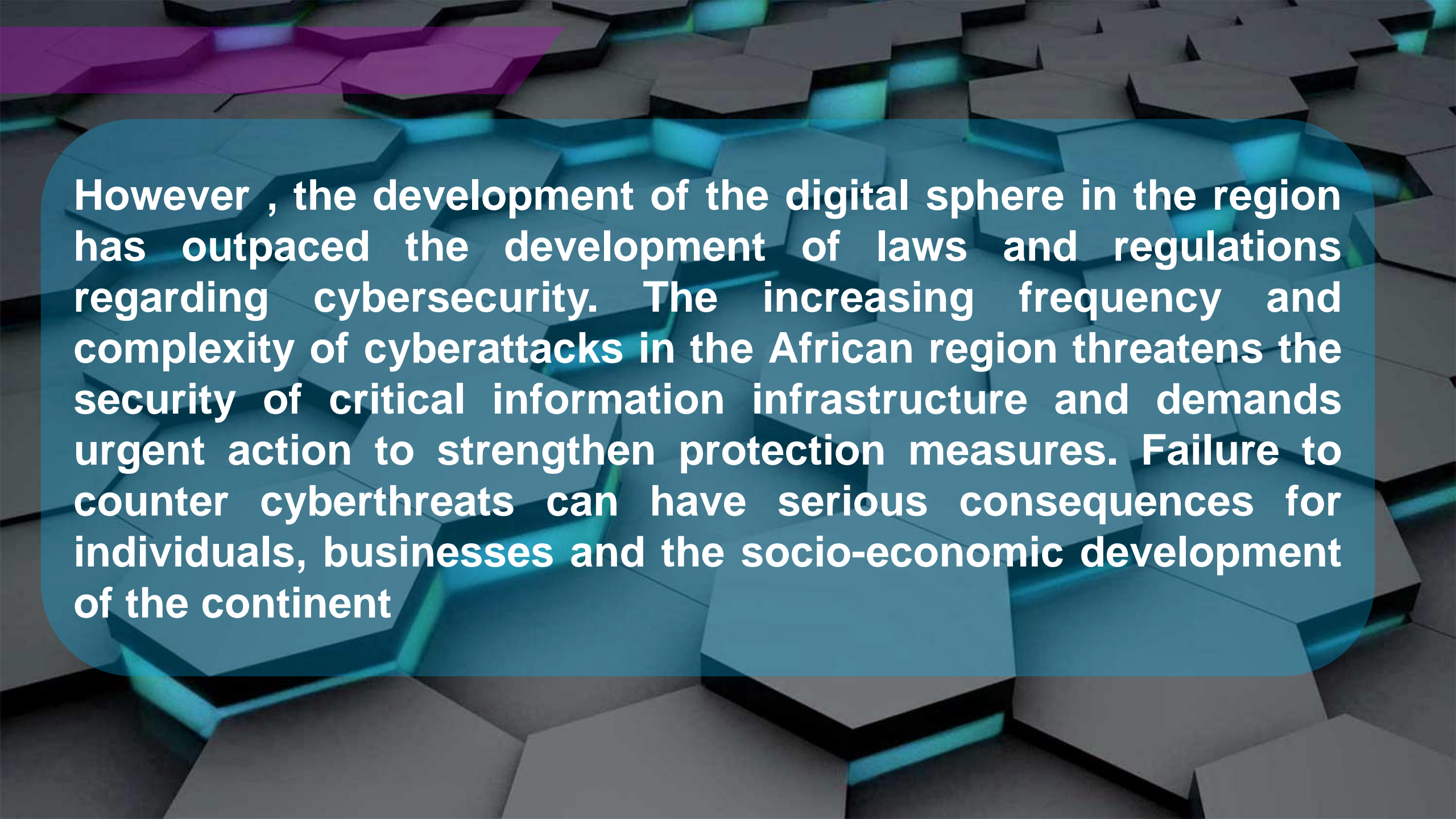
How ?

06

Conclusion

Overview

Africa is a region experiencing rapid economic development. Over the past twenty years, the combined GDP of the region has increased more than fivefold, from USD 695.88 billion in 2002 to USD 2.98 trillion in 2022 and is projected to exceed USD 4 trillion by 2027. The cumulative growth of African economies reflects the region's huge potential and is contributing to an increase in demand for Internet and digital services.



However , the development of the digital sphere in the region has outpaced the development of laws and regulations regarding cybersecurity. The increasing frequency and complexity of cyberattacks in the African region threatens the security of critical information infrastructure and demands urgent action to strengthen protection measures. Failure to counter cyberthreats can have serious consequences for individuals, businesses and the socio-economic development of the continent

Legal Framework

The digital environment in the African region is rapidly evolving, but the lack of proper measures for ensuring cybersecurity, an insufficient legislative framework in the field of information security, and a low level of awareness about cybersecurity issues among the general population are leading to an increase in the number of cyberthreats.

Legal Framework



39

72%

African Countries

Africa's digital transformation processes are speeding up, making cybersecurity issues more urgent. Governments are responding by enacting cybercrime legislation and cybersecurity plans that address topics including establishing robust governance frameworks and enhancing institutional and human capabilities

Main Challenges

In recent years, Africa has experienced a rapid growth in digital technologies, particularly in financial technology and e-commerce, with the COVID-19 pandemic accelerating the shift towards remote work. By 2021, 43% of the continent's population, or 612 million people, had internet access.

Main Challenges

- **Youthful Population:** About 60% of Africa's population was under 25 years old in 2020, driving technology adoption.
- **Mobile Growth:** Sub-Saharan Africa is expected to have 615 million unique mobile subscribers by 2025.
- **Internet Expansion:** The number of internet users across Africa is projected to exceed 1 billion by 2023.
- **Digital Transformation Strategy:** Aims to provide stable internet access for every African by 2030.

Main Challenges

-Economic Constraints: Many African countries face financial challenges, limiting their ability to invest in adequate cybersecurity infrastructure.

-Cybersecurity Challenges: Widespread technology use, insufficient cybersecurity measures, weak legislation, and low public awareness create vulnerabilities for cybercrime.

Who attacks Africa?

Cyber threats have reached alarming levels, posing significant risks worldwide. Since there is rapid advancement in technology, it enables an easy gateway for sophisticated cybercriminals to exploit vulnerabilities for financial gain, data breaches, and disruption.

According to industry reports, 2024 witnessed a staggering surge in reported data breaches, with over 7 billion records exposed, marking a 93% increase from the previous year. The average cost of a data breach exceeded \$4.24 million.

Who attacks Africa?

Key factors contributing to the rise of cyber threats include:

- Proliferation of connected devices, IoT, and cloud computing expands the attack surface, offering more opportunities for cybercriminals.
- Emerging technologies like AI and machine learning are exploited by threat actors to develop sophisticated attack techniques.
- Widespread internet adoption interconnects individuals and organizations, providing more targets for cybercriminals.
- Rise of remote work and digital transformation amplifies risk as people access corporate networks from different devices and locations.

Types of CYBER ATTACKS



**Phishing and
Social Engineering**



**Ransomware
Attacks**



Insider Threats



**Internet of Things
(IoT) Vulnerabilities**



**Cloud Security
Challenges**

PHISHING



THREAT PRIMER





Simulation

CONCLUSION

Tips to STRENGTHEN YOUR CYBER DEFENSE

Security Awareness
and Training

Endpoint Security

Network Security

Data Encryption





Aicha Jeridi

Digital Policy | Internet Governance
Consultant | Events planner | Co...



THANK YOU