Final Report of the Working Group

Cybersecurity Working Group

APRIL 2026

Reference: WATRA/WG/CS/23AGM/26/04/002

Information about the document
Nature of the document: Final Report of the Working Group
Relevant group: Cybersecurity Working Group (WG-Cybersecurity)
Mandate Resolution AGM22/CR/25/R06 – WATRA 2025 Annual Plan/Activity Program
Scope: Telecommunications sector in West Africa
Addressee: WATRA Executive Secretariat and Member States
Status: Final – For adoption

Contents

1 Executive summary

This final report summarizes the work of the Cybersecurity Working Group of the West Africa Telecommunications Regulators Association (WATRA), from the various meetings held in Banjul (2024), Conakry (2024), Accra (2025) and Ouagadougou (2026).

In a context marked by the acceleration of digital transformation and the increase in cyber threats, Member States have faced major challenges, including the resurgence of attacks (phishing, ransomware, mobile fraud), disparities in capabilities between countries, and the inadequacy of harmonized regulatory frameworks.

The work has helped to identify strategic priorities for the sub-region, including:

- the strengthening of human and technical capacities.
- the harmonization of regulatory frameworks.
- the establishment of effective mechanisms for cooperation and information sharing.
- the development of national and sectoral incident response structures (CERT/CSIRT).

The Group recommends the implementation of a structured action plan including the creation of a regional information-sharing platform, the organization of cybersecurity exercises, the strengthening of collaboration between stakeholders and the promotion of a harmonized regional framework.

This report thus constitutes a strategic roadmap for strengthening cybersecurity in the telecommunications sector in West Africa.

2 Foreword and Context

2.1 Mandate of the Working Group

Pursuant to Resolution AGM22/CR/25/R06 adopting the WATRA Annual Plan and Programme of Activities for the 2025 fiscal year, the WATRA Annual General Meeting established three (3) thematic working groups to address critical regulatory issues in the West African sub-region. These groups cover, respectively: (i) infrastructure development, (ii) consumer access and experience, and (iii) cybersecurity.

This report constitutes the final report of the Cybersecurity Working Group (WG-Cybersecurity). It reports on the work carried out, the analyses performed, and the recommendations formulated at the end of the collective reflection process conducted by the group members.

2.2 General Context

The rapid digital transformation taking place in West Africa represents both a significant opportunity for economic and social development and a growing vulnerability to cyber risks. The increasing number of connected users, the deployment of next-generation mobile networks (4G/5G), the rise of digital financial services, and the growth of cross-border data exchanges are further exposing telecommunications infrastructure to sophisticated and constantly evolving threats.

In this context, improving cybersecurity in West Africa now requires a decidedly operational approach. WATRA, as the regional coordinating body, must play a leading role in establishing harmonized, effective, and sustainable mechanisms.

The proposed actions aim to reduce operational gaps between countries, improve collective response capacity and strengthen the region's overall resilience to growing cyber threats.

A phased implementation, supported by strong political commitment and adequate resources, will make it possible to achieve these objectives.

Telecommunications regulators play a key role not only in promoting access and competition, but also in ensuring a safe and resilient digital environment for citizens, businesses and governments in the sub-region.

Regulation has taken a turn towards more holistic and comprehensive frameworks, requiring a collaborative, multi-sectoral, forward-looking and cross-border approach to meet the expectations of this dynamic sector.

2.3 Composition and working method

The Cybersecurity Working Group is composed of representatives from the telecommunications regulatory authorities that are members of WATRA. It worked using a participatory methodology based on technical consultations, exchanges of experiences, and comparative analysis of regulatory frameworks in force in the sub-region and at the international level.

3 Landscape of Cybersecurity Threat

The cyber threat landscape in West Africa is undergoing rapid change, marked by the increasing professionalism of cybercriminals and a diversification of attack vectors. Phishing remains dominant, particularly via SMS (smishing) and messaging applications.

Ransomware attacks are increasingly targeting public administrations due to weak backup and business continuity systems. Furthermore, mobile money fraud is a critical issue given the high penetration of these services in the region.

The analyses also revealed that:

- A significant proportion of organizations do not have adequate cybersecurity measures in place.
- Critical infrastructures remain vulnerable to attacks.
- New technologies (IoT, satellite services, AI) introduce new threat vectors.

These findings underscore the need for a proactive and coordinated approach to anticipate and mitigate risks.

3.1 Overview of Threats in the Telecommunications Sector

The telecommunications sector in West Africa faces a diverse and rapidly evolving cyber threat landscape. Network operators, service providers, and end users are exposed to a wide range of attacks that compromise the availability, confidentiality, and integrity of communications.

3.2 Main Categories of Threats Identified

- Phishing and social engineering: targeted phishing campaigns exploit users' trust in telecom operators to steal personal data and credentials.
- Distributed denial-of-service (DDoS) attacks: targeting critical infrastructure of telecom operators and digital service platforms, these attacks can paralyze entire networks and disrupt essential services.
- Telecom and cyber fraud: SMS scams (smishing), subscription fraud, manipulation of billing systems and financial scams via mobile money

represent considerable economic damage for consumers and operators.

- Signaling network intrusions (SS7/Diameter): vulnerabilities in signaling protocols allow malicious actors to intercept communications, locate subscribers, and bypass authentication mechanisms.
- Malware and ransomware: the spread of malware via mobile networks and digital platforms poses a growing threat to businesses and institutions.
- Attacks on equipment and access networks: vulnerabilities in supplier equipment (routers, antennas, management systems) expose networks to large-scale compromises.

3.3 Specific Challenges to Data Protection

Protecting the personal data of telecommunications users is a key regulatory issue. The massive collection of data (communication metadata, location data, browsing history) by operators creates significant risks in the event of a breach or misuse.

- Absence or inadequacy of data protection legislation in certain member countries
- Insufficient mechanisms for notifying authorities and users of data breaches
- Gaps in the implementation of data conservation and minimization policies
- Risks associated with cross-border data transfers in the context of regional economic integration
- Lack of clear strategies to address the challenges

3.4 Network Confidentiality and Security

The security of electronic communications networks is a prerequisite for user trust. The working group identified several structural vulnerabilities:

- Aging and heterogeneity of network equipment with insufficient update cycles
- Dependence on equipment suppliers that pose potential risks to national security

- Lack of common standards for auditing and certifying the security of telecom equipment
- Underinvestment in monitoring, detection and incident response tools

3.4.1 Operational Recommandations

1. Establish a regional cyber strategic intelligence system.
2. Standardize incident collection methods;
3. Develop predictive threat analysis capabilities.

Key finding – Challenges and threats

West African countries are facing a significant increase in cyber incidents in the telecom sector.

DDoS attacks, mobile fraud, and data breaches are the main threats.

Data protection and network security require strengthened and harmonized regulatory frameworks.

Sub-regional cooperation is essential in the face of the cross-border nature of cyber threats.

4 Strategies and Guidelines for Capacity Building in Member Countries

4.1 Current state of capacities in the sub-region

The comparative analysis conducted by the working group reveals significant disparities in cybersecurity capabilities among WATRA member countries. While some states have developed robust institutional frameworks (Security Operations Centers, national CERT/CSIRT teams, national cybersecurity policies), others are still in the early stages of structuring their cyber governance.

4.1.1 Regional diagnosis

Member States exhibit varying levels of maturity. Some have operational national strategies, while others are still in the process of institutional structuring.

4.1.2 Areas of reinforcement

- Establishment of fully operational national CERTs.
- Strengthening of data protection authorities.
- Development of robust legal frameworks.
- Develop or update national cybersecurity policies by integrating a specific telecommunications component.

The West African region needs practical, harmonized, and affordable cybersecurity measures that can be adapted by communications operators and regulatory authorities despite disparities in infrastructure maturity, connectivity, and technical capabilities. A Cybersecurity and Information Security Directive (CSID), supported by national and sectoral incident response mechanisms, capacity building, reliable information sharing, and public-private cooperation, can provide a common foundation for resilience.

West African countries are accelerating their digital transformation across telecommunications, internet access, broadcasting, financial services, and other critical sectors. This growth increases exposure to cyber threats that can

disrupt services, erode consumer trust, and weaken the digital economy as a whole. At the same time, the region is operating in diverse technical environments, including existing systems, heterogeneous equipment, and uneven connectivity. Regional strategies must therefore be risk-based, realistic, and adaptable to varying levels of institutional and infrastructural maturity.

4.1.3 Regional Directive on Cybersecurity and Information Security (RDIS)

A National Cybersecurity Framework (NCSF) can serve as a common minimum standard for licensees and operators in the communications sector. It clarifies regulations, improves industry-wide preparedness, and fosters coordination between regulatory authorities, operators, and national cybersecurity institutions.

- Promote a secure and resilient communications infrastructure by strengthening the cybersecurity of regulated entities.
- Establish a framework for identifying, protecting against, detecting, countering and recovering from cyber threats affecting critical communications infrastructure and services.
- Require operators to implement structured governance arrangements, including cybersecurity policies, risk assessments, internal reporting channels, audits and board-level oversight, where appropriate.
- Facilitate the rapid and consistent detection and reporting of incidents to a national CERT, or to a designated national focal point when a CERT is not yet in place.
- Enable coordinated incident response and threat intelligence sharing among industry CSIRTs, national CERTs, operators, regulators, and other trusted partners. • Promote compliance with national laws, industry regulations, and emerging regional best practices.
- Strengthening consumer confidence and digital security of mobile, fixed, satellite, Internet access provider, broadcasting and other licensed services.

4.1.4 Regional design considerations

Any regional framework must be designed with local operating conditions in mind. Overly complex, costly, or infrastructure-dependent cybersecurity

controls may not be viable in all Member States. The working group should prioritize proportionate and effective controls in resource-constrained and mixed-technology environments.

- Consider the low connectivity and intermittent availability in some operating environments.
- Recognize the diversity of infrastructures, including legacy systems and heterogeneous equipment.
- Promote low-cost, scalable and easy-to-maintain security solutions.
- Allow for phased implementation so that Member States and operators can progressively meet the minimum requirements.

Proposed strategies to strengthen regional cybersecurity capacities

4.1.5 Strategic area

The following actions are recommended.

- Policies and regulations: Develop national cybersecurity policies and sectoral guidelines aligned with regional principles and adapted to local economic and social realities.

- Public-private cooperation: Strengthening partnerships between regulatory authorities, operators, suppliers, universities and investors to improve cybersecurity funding, preparedness and implementation.

- Capacity building: Implement continuing education and certification programs

4.2 Develop Strategies and Guidelines to Strengthen Members' Cybersecurity Capabilities

4.2.1 Human Resources and Technical Expertise

- Develop specialized cybersecurity training programs for telecommunications regulators
- Create a regional professional certification program recognized by the WATRA member states
- Encourage partnerships with universities and training institutes to develop local expertise
- Establish expert exchange programs between member regulators

Guidelines for Capacity Building
1. Each Member State should have a national telecom cybersecurity policy. 2. The creation of a sector-specific telecom CERT/CSIRT is recommended in each country.
3. WATRA should develop a regional training and certification program. 4. Annual sub-regional cyber incident simulation exercises are recommended.

5 Cooperation and Information Sharing

The rise of increasingly sophisticated, automated, and often transnational cyber threats underscores the need for collective action. Without structured cooperation among stakeholders, countries in the sub-region are exposed to heightened vulnerabilities. The lack of harmonization of regulatory frameworks and insufficient international coordination often result in fragmented, delayed, or even ineffective responses to incidents. Similarly, the absence of collaboration between technical entities, particularly for real-time information sharing, facilitates the spread of attacks and complicates countermeasures efforts. This situation has significant operational and financial consequences, disrupts the continuity of essential services, and undermines the trust of users and partners.

In order to strengthen the regional system to address these shortcomings, the WATRA cybersecurity working group formulates the following recommendations and encourages their adoption.

5.1 Faced with these various challenges, it is essential to adapt the responses through the following measures:

- Develop and implement a secure regional real-time sharing platform.
- Establish information classification protocols;
- Define differentiated access levels.

5.2 Regional Cooperation Mechanisms

The cross-border nature of cyber threats necessitates a collective and coordinated response. The working group examined existing cybersecurity cooperation mechanisms in the sub-region and identified gaps to be addressed in order to strengthen collective resilience.

5.3 Regional Information Sharing Platform

Faced with the rise in cyber threats resulting from the increasing digitalization of services within WATRA member countries, it is crucial to establish a regional cybersecurity information-sharing strategy. A structured and secure framework for information exchange, supported by a suitable digital platform, would not only improve incident management but also standardize

cybersecurity practices and strengthen the collective resilience of the nations involved. Cross-border cooperation, enhanced local capacity building, and the adoption of international standards will play a key role in effectively addressing transnational threats. Furthermore, to ensure the system's effectiveness and sustainability, trust, transparency, and regular monitoring of information-sharing processes are essential. In short, it is vital that WATRA countries adopt a proactive and coordinated approach to protect their national security and economies in the face of rapidly evolving cyber threats.

The working group recommends the creation of a Regional Platform for Sharing Information on Cyber Threats (PRSIC-WATRA), whose main characteristics would be:

- Shared governance among member regulators, with a technical secretariat provided by WATRA
- A mechanism for exchanging indicators of compromise (IoCs) in near real-time
- A threat intelligence bulletin distributed periodically to members
- Clear protocols defining the classification and methods of sharing sensitive information
- The progressive interconnection with continental (AfricaCERT) and international platforms

5.4 Protocols and Cooperation Agreements

To formalize and structure cooperation, the working group recommends:

- The signing of bilateral and multilateral agreements between member regulators on the exchange of cyber information
- Joint participation in international cybersecurity exercises
- The establishment of designated contact points in each national authority for regional coordination

5.5 Strengthening Regional Resilience

Beyond information sharing, the collective resilience of the sub-region relies on:

- The implementation of redundancies and secure interconnections between critical telecommunications infrastructures
- Regular cyber crisis management exercises involving several member countries simultaneously
- Jointly raising awareness among operators and the public about good cybersecurity practices

WATRA member states have already made significant efforts to strengthen cybersecurity in the telecommunications sector. However, current challenges require a more coordinated and structured approach at the regional level.

The implementation of the proposed actions will contribute to improving infrastructure resilience, strengthening data protection, and establishing a climate of trust conducive to digital development in West Africa.

Key Recommendations – Cooperation/Sharing
Institutionalize information sharing by creating the Regional Cyber Threat Information Sharing Platform
Establish a legal framework for cross-border sharing
A mechanism for exchanging indicators of compromise (IoCs) in near real-time
Establish a threat intelligence bulletin distributed periodically to members

6 Cybersecurity Challenges in the Telecom Sector

In a context marked by the acceleration of digital transformation in West Africa, the telecommunications sector occupies a strategic place in the functioning of states, the provision of essential services, and economic development. This evolution, however, is accompanied by increased exposure to increasingly complex cyber threats, capable of affecting networks, critical infrastructure, and service continuity.

Given the cross-border nature of these risks, a strictly national response is insufficient. It is therefore essential to promote a coordinated regional approach, based on cooperation, harmonization of practices, capacity building, and information sharing. In this regard, WATRA is called upon to play a central role in supporting Member States towards greater cyber resilience in the telecommunications sector.

This report aims, in this context, to identify the main cybersecurity challenges in the telecommunications sector in West Africa and to propose practical guidelines for strengthening regional coordination and the effectiveness of responses.

In the vast undertaking of West Africa's digital transformation, the telecommunications sector is no longer simply a service provider; it has become the vital infrastructure upon which finance, administration, and national security depend. While strategic frameworks and governance policies form the foundation of this structure, the reality of the threat now demands a rapid transition to purely operational action. Faced with cybercriminals exploiting even the smallest connectivity vulnerabilities, the time has come to implement robust technical measures capable of protecting data flows and the integrity of West African networks.

This report focuses on concrete actions and recommendations aimed at improving the operational effectiveness of cybersecurity systems in the region.

6.1 Key Operational Challenges Identified

6.1.1 Inadequate Incident Detection and Response Capabilities

In a digital environment characterized by the increasing speed and sophistication of cyber threats, the ability to detect and respond effectively to incidents is a crucial pillar of cybersecurity. Yet, in many countries in the region, this capacity remains limited. The deployment of Security Operations Centers (SOCs) and Computer Security Incident Response Teams (CSIRTs) is still insufficient, while real-time monitoring tools are lacking or not fully adapted to current needs. This situation results in often lengthy response times to incidents, thus reducing the effectiveness of mitigation measures.

6.1.2 Fragmentation of Technical Infrastructures

At the heart of the operational difficulties lies the fragmentation of technical infrastructures, which hinders any coordinated and coherent approach. Information systems, highly heterogeneous from one country to another and sometimes even within the same country, complicate the harmonization of practices. Added to this is the lack of interoperability between different cybersecurity platforms, making the integration of existing solutions difficult and limiting potential synergies.

6.1.3 Weakness in Incident Management Mechanisms

Incident management, while crucial in the cyberattack response chain, suffers from significant structural weaknesses. The lack of standardized procedures prevents a uniform and effective response. Furthermore, coordination between national CERTs/CSIRTs remains limited, weakening the capacity for collective response. Finally, the lack of business continuity and disaster recovery plans exposes organizations to prolonged disruptions in the event of a crisis.

6.1.4 Constraints Related to Technical Resources

Technical constraints represent a major obstacle to the operational effectiveness of cybersecurity systems. Insufficient specialized equipment, combined with a heavy reliance on external suppliers, limits the autonomy of states. Furthermore, difficulties related to system maintenance and updates compromise the sustainability and performance of existing infrastructures.

6.1.5 Low Level of Automation

In the era of digital transformation, process automation has emerged as an essential lever for improving operational efficiency. However, in the region, many processes remain largely manual. This situation makes it difficult to manage increasing volumes of data and alerts, while also increasing the risk of human error, which can compromise the overall security of systems.

6.2 Proposed Priority Actions

6.2.1 Implementation of a Harmonized Operational Framework

Given the diversity of practices and maturity levels, establishing a harmonized operational framework is a priority. This includes developing standardized incident management procedures at the regional level, defining common communication protocols in the event of a crisis, and harmonizing alert levels and notification mechanisms to ensure a coherent and coordinated response.

6.2.2 Deployment and Pooling Of SOC/CSIRT Capabilities

Strengthening surveillance capabilities necessarily involves developing and pooling security operations centers. The creation of interconnected national SOCs/CSIRTs should be encouraged, while also promoting shared regional SOCs for countries with limited resources. Establishing common monitoring platforms would also optimize the use of available resources.

6.2.3 Strengthening of Technical Infrastructure

From an efficiency and sustainability perspective, strengthening technical infrastructure is a key lever. This involves standardizing cybersecurity tools used in the region, promoting interoperable solutions, and deploying centralized log collection and analysis systems to provide better visibility into suspicious activities.

6.2.4 Improved Incident Response Capabilities

An effective response to cyber threats requires responsive and well-coordinated systems. To this end, the establishment of rapid response teams at the regional level is essential. It is also crucial to develop coordinated

response plans for major cyberattacks and to regularly conduct cyber drills to test and improve existing mechanisms.

6.2.5 Automation of Operational Processes

Automation is a key factor in improving operational performance. Deploying SOAR (Security Orchestration, Automation and Response) solutions, integrating automated threat analysis tools, and reducing reliance on manual processing will increase the speed, reliability, and efficiency of cybersecurity operations.

6.3 Strategic Recommendations with Operational Implications

6.3.1 Standardization and Interoperability

In a context marked by the diversity of systems, standardization and interoperability appear as essential conditions for effective cooperation. The adoption of common technical standards, the promotion of standard formats for data exchange, and the guarantee of compatibility between national systems will strengthen the coherence of actions at the regional level.

6.3.2 Implementation of Sustainable Financing Mechanisms

The sustainability of operational actions depends on the existence of appropriate and sustainable financing mechanisms. It is therefore recommended to create regional funds dedicated to cybersecurity infrastructure, to encourage public-private partnerships to support technological investment, and to facilitate access to international funding.

6.3.3 Development of Operational Centers of Excellence

To pool skills and resources, developing operational centers of excellence is a relevant strategic approach. These regional hubs could specialize in incident response, conducting advanced analyses (malware, forensics), and managing critical functions, thereby optimizing the use of scarce and costly resources.

6.3.4 Strengthening the Resilience of Critical Infrastructure

Protecting critical infrastructure is of paramount importance in securing states. It is essential to identify and prioritize this infrastructure, impose minimum

operational security requirements, and implement continuous monitoring mechanisms to ensure its resilience against cyber threats.

6.3.5 Monitoring and Evaluation of Operational Performance

Finally, the continuous improvement of cybersecurity systems requires rigorous monitoring and regular performance evaluation. Defining key performance indicators (KPIs), implementing regular reporting mechanisms, and periodically assessing the operational maturity of Member States will ensure effective and results-oriented governance.

Improving cybersecurity in West Africa now requires a decidedly operational approach. WATRA, as the regional coordinating body, must play a leading role in establishing harmonized, effective, and sustainable mechanisms.

The proposed actions aim to reduce operational gaps between countries, improve collective response capacity and strengthen the region's overall resilience to growing cyber threats.

A phased implementation, supported by strong political commitment and adequate resources, will make it possible to achieve these objectives.

Regulatory Priorities Identified
Adoption of a harmonized minimum regulatory framework on telecom cybersecurity at the WATRA level.
Integration of security obligations into the specifications of operator licenses.
Implementation of a regional mechanism for the certification of network equipment.
Development of common indicators to measure the cyber maturity level of operators.

7 Collaboration with Stakeholders

Telecommunications cybersecurity is a shared responsibility involving a multitude of actors. Effective collaboration among these stakeholders is essential for building a resilient digital ecosystem in West Africa. Collaboration with stakeholders is a fundamental pillar of strengthening cybersecurity preparedness in West Africa. This includes cooperation among national regulatory authorities, CERTs, sector-specific CSIRTs, cybersecurity agencies, and other relevant bodies.

7.1 Collaboration between Member States and National Institutions

It is necessary to strengthen cooperation between national regulatory authorities, national CERTs, sectoral CSIRTs, cybersecurity agencies, and other relevant bodies. Member States have been encouraged to share their national cybersecurity reports, designate focal points, establish CSIRTs, and exchange threat intelligence. Member States have been encouraged to:

Regularly disseminate national cybersecurity reports and threat intelligence to improve situational awareness across the region.

Designate national cybersecurity focal points who will serve as points of contact for regional coordination.

Create sector-specific CSIRT units and support countries that do not yet have functional teams, such as Guinea-Bissau.

Exchange information on emerging threats through agreed mechanisms and protocols, including periodic assessments and standardized questionnaires.

This interstate collaboration is considered crucial for the establishment of a unified regional response to cyber threats.

7.2 Regional and International Partnerships

It is essential to emphasize the importance of collaborating with regional and global entities to accelerate capacity building and promote harmonized cybersecurity practices. Key recommendations include:

In partnership with OCWAR C, which acts as an intermediary between WATRA and national cybersecurity organizations in cases where national CERTs and sectoral CSIRTs do not fall under the telecommunications regulatory authority.

Encourage all national CERTs and sectoral CSIRTs to join FIRST (Forum of Incident Response and Security Teams) and facilitate sponsorship of countries wishing to join.

Leverage existing channels such as Africa CERT for intelligence sharing and coordination.

Explore partnership frameworks aligned with international conventions such as the Malabo Convention.

Consistent with the above, the Nigerian Communications Commission (NCC) Cyber Resilience Framework (CRF-NCS) strengthens regional collaboration by establishing structured public-private partnerships, applying the Zero Trust architecture to telecommunications operators, and mandating the deployment of Security Operations Centers (SOCs).

This framework also deepens cooperation between the NCC-CSIRT and the ngCERT, strengthening cross-border threat intelligence sharing and aligned sectoral resilience efforts, fully complementing WATRA's objectives for harmonized cybersecurity governance.

Collaboration with regional and global entities such as OCWAR-C, FIRST, AfricaCERT, and alignment with conventions such as the Malabo Convention promote a harmonized development of cybersecurity.

7.3 Engagement with the Private Sector, Civil Society And Specialist Groups.

Cybersecurity requires broader stakeholder engagement, including public-private partnerships, cooperation with central banks, support from the ITU's DFS Lab, and expert networks such as the African Women's Cybersecurity Network. Engagement with the private sector, civil society, and specialized groups is also essential.

Member States stressed that cybersecurity cannot be driven solely by regulators and governments. Broader stakeholder involvement is essential, including:

Public-private partnerships to stimulate investment and innovation in cybersecurity infrastructure.

Cooperation with central banks and financial regulatory authorities, particularly in the area of digital financial services security, supported by the ITU's DFS security lab.

Inclusion of the African Women's Cybersecurity Network and similar expert groups in regional forums to ensure diversity and representation.

Establishment of a database of regional experts to facilitate cross-border sharing of resources and advisory assistance.

This multi-stakeholder approach broadens the scope of expertise and strengthens regional resilience, collaboration on standards, guidelines, and capacity building. Joint development of appropriate cybersecurity frameworks and harmonized regulatory approaches is essential. To this end, Member States have committed to:

- Examine and jointly compare existing international cybersecurity standards (ISO/IEC 27001, NIST CSF, CIS Controls, COBIT).
- Collaborating to merge several national or subgroup proposals into a single harmonized document for adoption across WATRA.
- To collectively develop, on an international scale, guidelines on information sharing, incident response and security testing.
- Organize regional workshops and cyber defense exercises led by experts and partner institutions to strengthen capacities. Such initiatives promote collective ownership of frameworks and improve technical capabilities throughout the region.

Furthermore, the NCC framework highlighted in subsection 2 above introduces a unified cybersecurity governance model that aligns with international standards such as ISO 27001 and the NIST CSF, making it a practical national example that supports WATRA's regional harmonization efforts.

Its structured compliance levels, risk management pillars and resilience indicators (e.g., the cyber capability index) demonstrate how national frameworks can operationalize regional cybersecurity objectives.

Member States agreed to evaluate international standards (ISO 27001, NIST CSF, CIS Controls, COBIT), merge proposals into harmonized frameworks, and develop guidelines for information sharing, incident response, and security testing, information exchange mechanisms and communication channels

The establishment and strengthening of structured communication channels were identified as a key factor in collaboration. Key proposals included:

- Creation of a centralized regional information exchange protocol through a multinational working group.
- Establishment of an official communication channel for member countries and a centralized security observatory to aggregate data from CERTs.
- Regular virtual meetings, periodic regional surveys and the publication of bilingual (English/French) reports to ensure inclusion and accessibility.

These mechanisms ensure continuous, structured, and data-driven collaboration.

In conclusion, collaboration with key regional and international stakeholders remains essential to strengthening West Africa's cybersecurity capacity. Concrete measures, such as expert databases, harmonized surveys, and regional forums, contribute to building long-term resilience. Furthermore, the Nigerian Communications Commission's (NCC) cyber resilience framework reinforces regional efforts by introducing a resilience-driven model, mandating a "Zero Trust" architecture, and requiring the continuous operation of Security Operations Centers (SOCs). Its alignment with WATRA objectives, particularly through improved incident response, unified risk management practices and enhanced public-private cooperation via the NCC's Computer Security Incident Response Team (NCC CSIRT) and the Nigerian Computer Emergency Response Team (ngCERT), significantly contributes to the region's collective digital resilience and supports the creation of a secure, coherent, and future-proof cybersecurity ecosystem.

8 Coordination of the Response to Cyber Threats

8.1 Coordinate the Response

A cyber incident is an event that can compromise the confidentiality, integrity, or availability of computer systems or data. These incidents can be caused by accidents, human error, malicious acts, or system failures. Therefore, having a response plan in place is essential to minimize the damage caused by such an incident.The telecommunications sector has a critical characteristic: it is both a target of cyberattacks and the infrastructure supporting the response to those same attacks. A compromise of the telecom network can therefore simultaneously paralyze the victim company and the communication channels necessary for crisis management. This makes prior preparation not just desirable, but absolutely essential.

8.2 Incident Management Framework

An effective response to cyber incidents requires a clear coordination framework, proven procedures, and lines of communication established prior to any crisis.

This framework includes the ANR of member countries and WATRA:

Not all member countries have the same level of capacity. Regional coordination should allow for real-time leveling up.

- Create a regional reserve of cybersecurity experts who can be mobilized to support member countries overwhelmed by an incident: a pool of specialists in forensic analysis, incident response, and crisis management.
- Establish a mechanism for the rapid deployment of these experts, with pre-arranged administrative and financial procedures to avoid bureaucratic delays in crisis situations.
- Developing shared malware analysis capabilities accessible to all members is essential, as each country would otherwise have to invest individually in costly infrastructure.
- Establish a regional stockpile of emergency technical solutions: forensic analysis tools, emergency filtering solutions, and alternative communication capabilities.

8.3 Signaling and Notification Mechanisms

The working group proposes that WATRA play the role of facilitator in coordinating incident responses.

The ANR plays the role of an escalation chain within a country, in that it constitutes the point of contact for WATRA to reach the national CERT team.

The report is symmetrical, meaning that it can come from an ANR or from WATRA.

- Establish a requirement to notify national regulators of significant security incidents within defined timeframes (e.g., initial notification within 24 hours, full report within 72 hours)
- Create a standardized incident notification form harmonized between Member States
- definition of clear reporting thresholds (number of users affected, duration of the interruption, nature of the compromised data)
- Establish a regional telecom incident registry for trend analysis

8.4 Coordination of Mitigation Efforts

In the face of a major cyber incident affecting one or more countries, coordination must be based on:

- A crisis protocol that can be activated quickly, with clearly defined roles;
- Secure communication channels between designated contact points in each regulatory member.
- Prior agreements with national CERTs on mitigation measures that can be deployed in an emergency.
- Mechanisms for the rapid mobilization of technical expertise to support Member States with capacity deficits.

Internally:

- Alternative communication channels, independent of the potentially compromised network
- Secure information sharing protocols between teams

Externally:

- Pre-established contact details with regulators (national regulatory authority, national cybersecurity agency)
- Customer notification protocols, differentiated according to the nature of the incident
- Public and media communication strategy, validated before the crisis

8.5 Exercises and Simulations

Preparing for cyber crises requires regular training.

WATRA must therefore ensure that the response plan is regularly tested by organizing periodic tests and exercises:

- Organises annually a sub-regional cyber crisis simulation exercise involving at least half of the members of WATRA.
- Conduct biennial national exercises in each Member State involving telecommunications operators.
- Sharing only feedback from exercises and real incidents between members.
- Participate in international cyber exercises organized by the ITU and other partners

8.6 Recommendations

The working group proposes the following recommendations

- Encourage WATRA member countries to implement sector-level security incident response plans. All members should be encouraged to establish sector-level CSIRTS/CERTS or at a minimum a national CERT;
- Ensuring, at the level of each Member State, effective coordination between the various actors includes the CERT/CSIRT;
- Elaborate a regional cyber incident response plan defining roles, trigger thresholds and collective decision-making mechanisms;
- Organize regional simulation exercises (cyber drills) involving several countries simultaneously, to test procedures and strengthen collective reflexes;
- Designate a regional coordination unit that can be activated in the event of an incident affecting several Member States, with a clear operational mandate;
- Negotiate cooperation agreements with counterpart organizations (CRASA for Southern Africa, ARICEA for Eastern Africa) to extend coordination beyond the

sub-region

- Assisting national CERTs in their process of joining global incident management entities (FIRST) to benefit from the training courses
- Implement monitoring of incidents affecting third-party operators, as the threat is often systemic.

9 Capacity Building Initiatives

Capacity building for stakeholders is an important lever for enhanced cybersecurity in the sub-regional area.

9.1 WATRA-Cyber Regional Training Program

The working group recommends the creation of a Regional Training Programme in Telecommunications Cybersecurity, structured around several levels of skills adapted to the needs of the sector.

9.2 Strategic Partnerships for Capacity Building

To achieve the ambitious capacity-building objectives, WATRA should develop strategic partnerships with regional and international organizations with recognized expertise and Regional Centres of Excellence in telecom cybersecurity.

- International Telecommunication Union (ITU): training programs and technical assistance
- ENISA (European Union Agency for Cybersecurity): transfer of expertise and best practices
- ITU-IMPACT: Access to global cyber intelligence resources and crisis assistance
- AfricaCERT: Coordination with the African Network of Incident Response Teams
- GSMA: Standards and best practices specific to mobile operators
- Some accredited professionals specializing in countries within the region
- Bilateral partners: cooperation with advanced regulators (ARCEP, Ofcom, etc.)

9.3 Regional Centre of Excellence in Telecom Cybersecurity

In the longer term, the working group is considering the creation of a Regional Center of Excellence in Telecommunications Cybersecurity (CRECT-WATRA), whose missions would be:

- To serve as a training and certification hub for telecom security professionals in the sub-region

- Conducting applied research on emerging threats specific to the West African context
- Provide technical assistance to member regulators with limited capacity.
- Develop and maintain regional telecom cybersecurity repositories, guides and standards.

9.4 The TogoCyber+ and African Centre for Coordination and Research in Cybersecurity (ACCRC) projects.

The TogoCyber+ project, initiated to strengthen cybersecurity in Togo, is part of a structuring dynamic aimed at consolidating national and regional cybersecurity capacities. Designed as a catalyst, its objective is to lay the technical, human, and organizational foundations necessary for the emergence of the African Cybersecurity Coordination and Research Centre (ACCRC), destined to become a leading continental hub. Through capacity building for Computer Emergency Response Teams (CERTs), the promotion of information sharing, the strengthening of regional cooperation, and the mobilization of technical and financial partnerships, TogoCyber+ represents a crucial step towards establishing an integrated cybersecurity ecosystem in Africa. In this context, the ACCRC appears as the strategic culmination of this initiative, providing a structured framework for coordination, research, training, and innovation at the continental level.

In view of these challenges, the cybersecurity working group strongly recommends that WATRA provide institutional and technical support to these initiatives, in particular by promoting the participation of its member states, supporting regional cooperation mechanisms and contributing to the integration of these projects into the strategic priorities of the sub-region, in order to sustainably strengthen collective resilience to cyber threats.

10 Recommendations and Action Plan

The cybersecurity working group makes the following recommendations.

10.1 Strategic Recommendations

Priority	Strategic Recommendation
CRITICAL	Adopt a harmonized regulatory framework for telecom cybersecurity at the WATRA level.
HIGH	Create the Regional Platform for Sharing Information on Cyber Threats (PRSIC-WATRA).
HIGH	Launch the Regional Training Program in Telecommunications Cybersecurity (PRFC-WATRA).
HIGH	Establish a network of interconnected sectoral CERT/CSIRTs in each Member State.
AVERAGE	Organize an annual sub-regional cyber incident simulation exercise.
AVERAGE	Develop a library of cybersecurity best practices adapted to the West African context.
LONG TERM	Create the Regional Centre of Excellence in Telecommunications Cybersecurity (CRECT-WATRA).

10.2 Short-Term Action Plan (2026-2027)

The priority actions for the immediate period are as follows:

- Validation and adoption of this final report by the WATRA General Assembly

- Establishment of a technical monitoring committee responsible for implementing the recommendations
- Development of an introductory training module available online for all member regulators

10.3 Medium-term Action Plan (2026-2029)

- Operational deployment of the PRSIC-WATRA with pilot countries followed by progressive expansion
- Launch of the PRFC-WATRA with the first training modules
- Adoption of a harmonized minimum regulatory framework for telecom cybersecurity
- First sub-regional cyber crisis simulation exercise
- Mid-term evaluation and adjustment of the capacity-building program

11 CONCLUSION

Cybersecurity in the region requires a coordinated, structured, and sustainable approach. WATRA plays a central role in building a robust regional cybersecurity ecosystem.

The Group's work highlighted that cybersecurity in telecommunications is no longer a secondary concern, but a strategic priority essential to user trust, the continuity of essential services and, ultimately, the digital economic development of the sub-region.

Faced with the borderless nature of cyber threats, the response must be collective, coordinated and based on solidarity between the member states of WATRA.

Cybersecurity in West Africa requires a coordinated, structured, and sustainable approach. WATRA has a central role to play in building a robust regional ecosystem.

This final report of the WATRA Cybersecurity Working Group provides a comprehensive overview of the challenges, opportunities and priority actions to strengthen the cyber resilience of the telecommunications sector in West Africa.

The group's work has highlighted that telecommunications cybersecurity is no longer a secondary concern but a key strategic issue, on which user trust, the continuity of essential services and, ultimately, the digital economic development of the sub-region depend.

Faced with threats that know no borders, the response must be collective, coordinated, and based on solidarity among WATRA member states. The recommendations in this report aim to progressively build this framework of collective security, taking into account the realities and constraints specific to each national context.

The working group respectfully submits this report for approval by the WATRA General Assembly and calls for the diligent and concerted implementation of the recommended measures, in the interest of all users of telecommunications services in West Africa.

Summary of recommended commitments to Member States
1. Development of an incident notification system.
2. Establish a regional cyber strategic intelligence system.
3. Standardize incident collection methods.
4. Establishment of a regional incident response mechanism.
5. Organization of a regional cybersecurity forum and regional cyberdrills exercises.
6. Participation in international exercises and collaboration with international organizations.