

# Governance and Society Review (GSR)

Volume 3 Issue 2, Fall 2024

ISSN(P): 2959-1619, ISSN(E): 2959-1627

Homepage: <https://journals.umt.edu.pk/index.php/gsr>



Article QR



**Title:** **Combatting Cybercrime in West Africa: Assessing the Role of the Economic Community of West African States (ECOWAS) as a Capable Guardian**

**Author (s):** Tahir Adekunle Ijaiya


**Affiliation (s):** Nigerian Institute of Social and Economic Research (NISER), Ibadan, Nigeria

**DOI:** <https://doi.org/10.32350/gsr.32.02>

**History:** Received: January 22, 2024, Revised: June 15, 2024, Accepted: November 14, 2024,  
Published: Dec 24, 2024

**Citation:** Ijaiya, T. A. (2024). Combatting cybercrime in west Africa: Assessing the role of the Economic Community of West African States (ECOWAS) as a capable guardian. *Governance and Society Review*, 3(2), 24–51.  
<https://doi.org/10.32350/gsr.32.02>

**Copyright:** © The Authors

**Licensing:**  This article is open access and is distributed under the terms of [Creative Commons Attribution 4.0 International License](https://creativecommons.org/licenses/by/4.0/)

**Conflict of Interest:** Author(s) declared no conflict of interest



A publication of The School of Governance and Society  
University of Management and Technology, Lahore, Pakistan

# Combating Cybercrime in West Africa: Assessing the Role of the Economic Community of West African States (ECOWAS) as a Capable Guardian

Tahir Adekunle Ijaiya\*

Nigerian Institute of Social and Economic Research (NISER), Nigeria

## Abstract

The study examines the role of the Economic Community of West African States (ECOWAS) as a capable guardian in combating cybercrime within West Africa. To do this, the study adopts routine activity theory (RAT) as a theoretical framework. RAT states that crime can only occur when likely offenders and potential targets converge in place and time without a capable guardian, underscoring the vital role of a capable guardian in crime prevention. Relying on secondary data, the study reveals that the ECOWAS has initiated various measures (legislation, workshops, regional meetings, capacity-building programmes, and partnerships) in its bid to play the role of a capable guardian. Furthermore, ECOWAS's efforts to combat cybercrime have been hampered by several challenges, including poor commitment and inadequate funding for cybercrime and cybersecurity initiatives. The study thus suggests that the ECOWAS ought to invest in improving cybersecurity expertise and cyber law harmonisation within the sub-region.

**Keywords:** ECOWAS, cybercrime, West Africa, Routine Activity Theory

## Introduction

Cybercrime activities in the West African sub-region are motivated mainly by financial gains and usually involve advance fee fraud, phishing, spamming, and hacking (Adelaja, [n.d.](#)). Moreover, two main types of cybercriminals in the sub-region are Yahoo boys or Sakawa boys and Next Level Criminals. The Yahoo boys/Sakawa boys engage in activities such as advance fee fraud, travellers' scams and romance scams. In contrast, Next Level criminals engage in more advanced activities requiring technical skills (hacking), including corporation and tax scams (Shaw, [2018](#)). Furthermore, Trend Micro and I International Criminal Police Organization

---

\*Corresponding Author: [ijaiyatahir@gmail.com](mailto:ijaiyatahir@gmail.com)

School of Governance and Society

(NTERPOL) noted that the emergence of cybercrime markets where cybercriminals trade products and services with one another in the West Africa sub-region is eminent (Global Initiative, [2016](#)).

Most of these cybercriminals are driven by a variety of factors. Malby et al. ([2013](#)) contend that some of these factors include the anonymous nature of cybercrime, access to global victims, socialisation and economic conditions. Furthermore, Shinder and Cross ([2008](#)) assert that these factors depend on individual cybercriminals, with each offender being motivated by different factors. Thus, generalisation is not feasible. Nonetheless, regardless of the offenders motivation, cybercrime activities have caused enormous damages including monetary loss, damages to big, medium and small businesses, and bad image and reputation for countries (Paoli et al., [2018](#)).

Alternatively, according to Routine Activity Theory (RAT), cybercrime is driven by three factors: likely offenders, potential victims and lack of capable guardians (Miro, [2014](#)). According to the proponents, cybercrime can only occur when these factors converge i.e., cybercrime is driven by a condition where a likely offender and a potential victim converge in cyberspace without a capable guardian to prevent such an offender from attacking the potential victim (Felson & Cohen, [1980](#)). According to this perspective, cybercrime can be prevented and curbed when a capable guardian disrupts the convergence of the offender and the potential victim. In other words, a guardian can protect the potential victim and limit their vulnerabilities.

The Economic Community of West African States (ECOWAS) has been playing the role of a capable guardian through its Directive on Cybercrime 2011, the Electronic Transaction Act 2010 and Personal Data Protection Act 2010 to harmonise sub-regional cyber laws and secure West African cyberspace. Despite this, challenges still abound and the commitment towards tackling cybercrime remains low, as reported by the 2018 Global Cybersecurity Index, with only 5 West African countries having a medium commitment to more secure cyberspace (International Telecommunication Union [ITU], [2019](#)). Therefore, it is imperative to examine the role of ECOWAS (as a capable guardian) in combating cybercrime in West Africa through the lens of RAT. Specifically, the study examines the nature of cybercrime in West Africa, the role of ECOWAS as a capable guardian, and the challenges militating against ECOWAS's efforts.

---

## Materials and Methods

This study adopts a qualitative research strategy. The collected data was sourced from journal articles, newspapers, reports and books. Journal articles were sourced from reputable publishers through Semantic Scholar and Google Scholar. Reports were sourced from relevant organisations addressing cybercrime-related issues in West Africa. This includes the ECOWAS, INTERPOL, ITU and UNODC. The study adopts routine activity theory (RAT) as a theoretical framework, situating ECOWAS as a capable guardian in the fight against cybercrime in West Africa. Moreover, the study adopts thematic analysis to examine data and elicit relevant themes that capture ECOWAS's anti-cybercrime efforts and the challenges of combating cybercrime in West Africa.

### Routine Activity Theory

Lawrence Cohen and Marcus Felson developed routine activity theory (RAT) in 1979, further expanded by Marcus Felson. RAT was initially based on the idea that alterations in people's daily activity patterns after the Second World War could explain increased crime (Miro, [2014](#)). In other words, the theory expounds that crime opportunities are created through daily activities individuals engage in to meet their needs (Madero-Hernandez & Fisher, [2012](#)). They hypothesised that postmodernity had created more situations whereby potential offenders and "suitable targets" have direct contact without the presence of "capable guardians" (Miro, [2014](#), p.1). In essence, the convergence, in "space" and "time", of a likely criminal and a victim is more likely to occur without any form of deterrence to prevent the crime (p.1).

They also gave an alternative explanation for the increased crime rate, which is different from the traditional socioeconomic explanations such as poverty, illiteracy and unemployment. The reason for this was a persistent increase in crime rate in the US in the 1960s despite the improvement in the socio-economic conditions (Madero-Hernandez & Fisher, [2012](#); Miro, [2014](#)). Hence, they posit that the changes in patterns of people's routine activities have created more criminal opportunities. For instance, the changes in daily routine, such as increased participation in the labour force (especially for women), led to an increase in contact with the possible offender and leaving the houses empty and unprotected. Furthermore, technological advances in the 60s led to the proliferation of small electronic

appliances with very high value and low weight, making them attractive to a likely offender and easy to remove and transport. This increase in valuable objects, contact between offenders and potential victims, and unprotected homes have led to more targets for criminals and a lack of capable guardians to prevent crimes. The theory emphasises how unrelated elements, like routine activities and legitimate use of technologies, can influence the nature of crime. For example, electronic devices and automobiles intended for lawful use can be used for criminal purposes. Similarly, cybercriminals exploit computers, smartphones, emails and the internet designed initially for legitimate purposes (Miro, [2014](#)).

RAT is different from other popular theories in the field of criminology as it does not identify the criminal motivation or the sources of such motivation. It also does not explain why people vary in their tendency to commit a crime or offend while not denying the existence of these issues. Secondly, other popular theories choose the offender as the unit of analysis and focus less on the importance of the actual crime event (Madero-Hernandez & Fisher, [2012](#)). According to RAT, the offender alone is not enough for crime to occur; there must be three elements, which are a potential offenders criminal dispositions and the ability to offend, a suitable target for the offender such as persons or objects, and a lack of capable guardian competent enough to prevent the crime. None of these factors is good enough to prevent crime (Felson & Cohen, [1980](#)). In sum, the three elements are (a) a likely offender, (b) a suitable target and (c) the absence of a capable guardian.

According to Felson and Cohen ([1980](#)), a likely offender is someone with a disposition towards crime. They emphasise the importance of focusing on the crime rather than solely on the motivations of offenders, while still acknowledging the significance of motives. Miró ([2014](#)) identify four factors that determine the suitability of a target, known as VIVA: value, inertia, visibility and access. Value refers to what an offender deems valuable, while inertia relates to the physical attributes of a target that either hinder or encourage an offender. Visibility measures the exposure of a target to an offender and access considers the environmental and locational aspects that facilitate an attack. Miro ([2014](#)) defines a capable guardian as a person or object that hinders or prevents a crime. Guardianship encompasses various forms, including social guardianship provided by family, friends, neighbours and co-workers, and physical guardianship in

the form of tools that potential targets can use for protection. Unlike other factors contributing to risk, guardianship is a protective factor (Madero-Hernandez & Fisher, [2012](#)).

However, as the theory expanded, in 1981, Cohen and his colleagues replaced the concept of “likely offender” with “exposure to the offender” and “proximity to the offender”, making the factors needed for a crime to occur four in number. Exposure to offenders exists when a potential target is within a risky environment. Individuals who place themselves in a vulnerable environment are more likely to be victims. Proximity to offenders, on the other hand, means the distance between the environment where potential targets are located and the areas where large numbers of potential offenders are located (Madero-Hernandez & Fisher, [2012](#)). Thus, the closer the offenders reach potential targets, the more likely it is for crimes to occur. However, the three traditional elements previously explained still remain the core components of the theory.

RAT explains cybercrime by highlighting how the internet's integration into daily life has changed routine activities, creating opportunities for fraud and victimisation. E-commerce has led to the storage of valuable consumer data, attracting potential offenders. The increased number of internet users provides anonymity and geographical freedom for offenders, while suitable targets include financial institutions and online businesses. Capable guardians in cyberspace encompass online consumers, law enforcement, computer emergency response teams, and individuals equipped to discourage offenders. The nature of targets and guardians depends on the specific form of cybercrime and the motivations of the offenders (Holt & Bossler, [2016](#); Pratt et al., [2010](#)).

Within cybercrime, RAT did not account for online consumers participating in activities from the comfort of their homes. This is antithetical to RAT's claim of increased victimisation when people spend more time away from their homes. However, Pratt et al. ([2010](#)) argue that people spending more time and money online makes them vulnerable to cybercrime. Yar ([2006](#)) further argues that routine activities are challenging to transfer online because the online world is ephemeral and unstable. Also, the offenders and targets do not converge in physical space and time but interact across different locations. These contravene the basic assumptions of RAT: crimes occur when offenders and targets converge in space and time without a capable guardian.

Nonetheless, Yar's assertions have been challenged by various scholars (e.g., Holt & Bossler, [2016](#); Stalans & Donner, [2018](#)). They argue that the basic assumptions of RAT can be applied to the online space. Victims' or targets' interactions with malware or potential offenders online are similar to physical world interactions. Online space (or cyberspace) is stable because it consists of stable networks of computers where offenders and targets converge and interact through interconnected devices and networks. Moreover, technological advancement has merged both online and physical space, making routine activities transposable to the online space (Holt & Bossler, [2016](#); Stalans & Donner, [2018](#)).

Given that Routine Activity Theory (RAT) was developed before the widespread use of the internet, it offers limited explanations for applying its concepts and constructs to the virtual world, measuring variables, and understanding the intertwining of virtual and real behaviours (Holt & Bossler, [2016](#)). Its applicability to cybercrime is not universally consistent, as evident from the mixed results of the reviewed studies depending on the specific type of cybercrime and aspects of RAT examined (Leukfeldt & Yar, [2016](#)). Critics argue that RAT lacks moral considerations, showing little interest in offenders and potentially blaming victims for being in the wrong place at the wrong time (Miro, [2014](#)). However, RAT does not claim to be a moral theory but seeks to explain crime based on changes in routine activities.

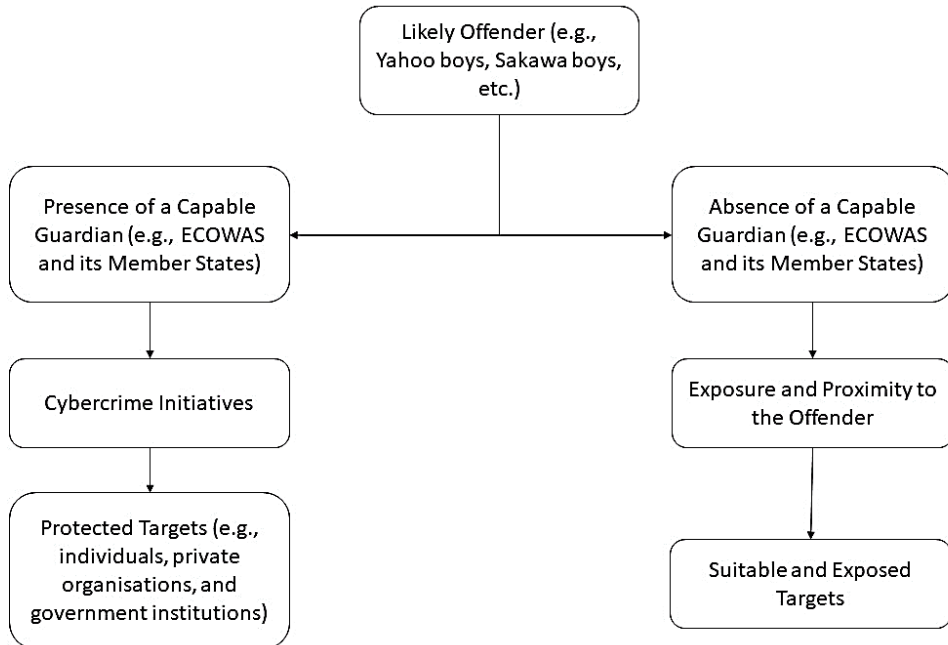
This theory is relevant to this study because it explains that cybercrime can only occur when offenders and targets converge in time and space with the absence of a capable guardian to prevent the crime, and within the context of this study, ECOWAS and its member states are the most compelling actors that can displace this convergence by providing capable guardianship through legislations, multilateral efforts, law enforcement, harmonisation of policy, public education and enlightenment among others to prevent cybercrime.

The likely offenders within the West Africa sub-region include Yahoo boys/Sakawa boys and Next Level Criminals. Exposed or protected targets include private and public institutions and individuals. ECOWAS and its member states assume the role of capable guardian with its cybercrime initiatives, such as legislation, capacity building, regional meetings and forums, international cooperation and cybersecurity agenda, among others. The schematic diagram shows that in the absence of ECOWAS and its

cybercrime initiatives, public institutions, the private sector and individuals will be exposed to cyber criminals and become suitable targets

### Figure 1

*Schematic Diagram Showing the Interaction between ECOWAS and Cybercrime in West Africa within the RAT Framework*



### Cybercrime as a Global Crime

The increasing prevalence of organised crime groups in the globalised online environment adds to the dynamic character of crime. Cybercrime impacts society worldwide, and its perpetrators and victims may be found in different places (Interpol, [n.d.](#)).

Malby et al. (2013) argue that global cybercrime is driven by various factors, including the anonymous nature of the crime, access to global victims, social learning (socialisation) and socio-economic pressure. Pasculli (2020) notes that these drivers can be proximate or remote. Proximate drivers of cybercrime include factors that motivate individuals to commit cybercrimes and also provide the opportunity to commit crimes (e.g., having access to potential victims), while the remote drivers of cybercrime include socioeconomic, political and cultural factors (e.g.,



cultural emphasis on wealth, power, and status, poverty and inequality) that are independent of individuals but have an impact on individuals' motivations and the opportunities to commit crimes. Shinder and Cross (2008) note that the drivers of global cybercrime are as diverse as cybercriminals, with each criminal having different motives.

Cybercrime causes enormous damage to individuals and countries, some of which are monetary loss, damages to big, medium and small businesses (Paoli et al., 2018), and lack of trust and a bad image for countries ridden with cybercrime (Duah & Kwabena, 2015). Paoli et al. (2018) note that the consequences of cybercrime can be both quantifiable and non-quantifiable. However, the prevalence of cybercrime has forced many countries and international organisations to adopt many strategies to curb these activities.

The United Nations have measures to address cybercrime through the UN Office on Drugs and Crime (UNODC), the UN Commission on Crime Prevention and Criminal Justice (CCPCJ), and the UN General Assembly's resolutions. However, most of these measures are resolutions, guidelines and protocols (Vogel, 2007). Furthermore, the UN, through the International Telecommunication Union (ITU) has tried to combat cybercrime at both national and global levels. The ITU has attempted to harmonise global and regional cyber laws, such as the Model Law on Computer Crime and Cybercrime of the Southern African Development Community (Hove, n.d.). The ITU also created the Global Cybersecurity Agenda in 2007 to emphasise the relevance of legal, technical and procedural measures, organisational structures, capacity building, and international cooperation in combating cybercrime (Saravade, 2016). The agenda also aimed to establish model cyber laws with universal application and coherence with existing regional and national cyber laws (Schjolberg, 2008). However, the UN faces challenges, such as the inability to define elements of cybercrime, which have hampered efforts to identify and monitor trends and incidences of cybercrime (Alkaabi et al., 2010). The UN cybercrime policies are dispersed, posing the challenge of having a coherent scope of UN cybercrime policy (Vogel, 2007).

The first and most comprehensive multilateral effort against cybercrime is the Council of Europe Convention on Cybercrime 2001 (or Budapest Convention) (Cerezo et al., 2007). The Convention obliged countries to establish laws against cybercrime or computer-related crime, provide

necessary tools and give law enforcement agencies the authority to track, investigate and prosecute computer-related crime, while providing essential cooperation and support to other parties in their efforts against cybercrime (Clough, [2012](#); Jamil, [2012](#);). The Convention is the first international treaty to address copyright violations, computer-related fraud, child pornography and network security violations (Cerezo et al., [2007](#)). Calderoni ([2010](#)) notes that the convention provides a three-path solution to the problem of cybercrime, including reducing frictions among national legislations, introducing new investigative powers and improving international cooperation. However, critics note that the Convention has been poorly enforced due to a lack of global police powerful enough to implement its provisions. Moreover, there were inconsistencies with the laws of various states, party to the Convention, despite its effort to harmonise cyber laws (Hill & Marion, [2016](#)).

### **Cybercrime in West Africa**

Cybercrime is any crime that uses a computer or a networked device to harm others or cause inconvenience. This can include hacking, phishing, malware attacks and identity theft. Individuals or organisations can commit cybercrime, which can be motivated by profit, ideology or personal vendetta (Hill & Marion, [2016](#)).

Before the emergence and proliferation of information and communication technologies (ICTs) such as the internet in West Africa, certain countries in this region, notably Nigeria, had already gained global notoriety as the epicenter of fraudulent activities known as "advance fee fraud" or the "West African Letter scam" (Orji, [2019a](#)). This fraudulent scheme involves utilising deception as a means of obtaining financial gains. With the widespread adoption of ICTs in the region, these fraudulent practices have experienced a surge and transitioned to the online realm, with Nigeria and Ghana emerging as particularly notorious countries for internet scams. One prevalent form of internet fraud in the region is the "Nigerian email scam" or the "West African email scam." These scams commonly manifest as deceptive job offers, fraudulent romance and marriage proposals, fictitious lottery winnings, money laundering propositions, scholarship scams, immigration scams, property sale scams, inheritance claim scams and spurious business opportunities (Orji, [2019a](#)).

Cybercriminals in West Africa are known as Yahoo boys and Sakawa boys in Nigeria and Ghana, respectively. These cybercriminals consist mainly of unemployed youths (dropouts, secondary school graduates, university graduates and undergraduates) who mostly fall under the age group of 18 to 39 (Atta-Asamoah, [2009](#); Flores et al., [2017](#)). In addition, Flores et al. ([2017](#)) note two types of cybercriminals in West Africa: Yahoo boys or Sakawa boys and the Next-Level Cybercriminals. The Yahoo boys, who earned their name due to heavy use of the Yahoo App to communicate with potential victims, especially in the early 2000s, are known to engage in less complex cybercrime activities such as advance fee fraud, romance or dating scams, or the stranded traveller fraud (this became infamous in early 2010s and it involves using a compromised social media account while impersonating the account owner to request money from their contacts, claiming falsely that the account owner is stranded and needs financial help).

On the other hand, the next-level cybercriminals are more sophisticated, engage in money laundry and have multiple foreign bank accounts to facilitate their more complex cybercrime activities. They engage mainly in business email compromise and tax fraud, and their victims are mostly big corporations instead of random individuals. The Yahoo boys and the Next Level criminals are also similar to what Atta-Asamoah ([2009](#)) terms as first and second-generation cybercriminals respectively. The activities of the second-generation cybercriminals, just like the Next Level cybercriminals, are more complex and require advanced computer skills (Attah-Asamoah, [2009](#)).

Flores et al. ([2017](#)) note five (5) common types of cybercrime (most of which are geared towards financial gains) observed in West Africa: advance fee fraud, stranded-traveller fraud, romance fraud, business email compromise fraud and tax fraud.

- Advance fee fraud: This type of fraud requires an individual or a business to pay a fee before receiving a promised reward in the form of money, products, services and sometimes stocks that are never delivered. This is regarded as the simplest and the oldest form of cybercrime. It also involves myriad false storylines.
- Stranded-traveller fraud: This became popular in the early 2010s. This occurs when compromised Facebook and other social media accounts

are used to ask for money from the account owners contacts (friends or followers). In this form of cybercrime, cybercriminals hack and take control of an account. The fraudster impersonates the account owner and asks the account owners contacts for emergency assistance. Sometimes, this fraud does not require hacking but duplication of accounts (creating new accounts with photos and personal information of real people).

- Romance fraud: This usually happens when a cybercriminal adopts a fake online identity to gain the trust and affection of a victim. Then, the cybercriminal uses the illusion of romantic affection and relationship to swindle the victim.
- Business email compromise fraud (BEC fraud): A cybercriminal uses a compromised business email address to intercept and imitate in-office communication to trick top company personnel or individuals into transferring money to bank accounts controlled by the criminal.
- Tax fraud: This recently became popular in the West African region, and US-based companies are usually the victims, especially toward the end of tax season (from January to April). Tax fraud is similar to BEC fraud, which follows the same pattern. In tax fraud, a cybercriminal impersonates a company executive or top official and then asks for payroll and W2 form information from the human resources (HR) or finance department via email. If the HR or finance department falls for the trick and sends the information, a cybercriminal can use this information to steal tax refunds meant for taxpayers.

To commit these crimes, West African cybercriminals adopt various tools, including malware and hacking tools such as banking Trojans, RATs, keyloggers, as well as phishing hosts, bots, Command and Control servers, Spam, etc. (Adelaja, [n.d.](#); African Union Commission & Symantec, [2016](#); Flores et al., [2017](#); Hill & Marion, [2016](#)).

### **Economic Community of West Africa States (ECOWAS) as a Capable Guardian**

In the quest to be the capable guardian responsible for preventing cybercrime, the Economic Community of West African States (ECOWAS) and its member states have developed numerous cybercrime countermeasures and policies, some of which are discussed below.

## Legislation

One of the legal measures put in place by the ECOWAS is Directive C/DIR.1/1/08/11 on Fighting Cybercrime (also known as the Directive on Cybercrime), which was adopted in 2011 during the 66th Ordinary Session of the Council of Ministers and it consists of six chapters (Digwatch, [2011](#)). According to Article 3, the objective of the Directive is to “adapt the substantive criminal law and the criminal procedure of the ECOWAS Member States to address the cybercrime phenomenon” (p.3). The Directive also covers all cybercrime-related offences within the region and all criminal offences requiring electronic evidence to be detected.

The Directive on Cybercrime is flawed, lacking new offences such as identity theft and protection of human rights (ITU, [2013](#)). However, the 2017 ECOWAS and COE Conference on the Harmonisation of Legislation on Cybercrime and Electronic Evidence is a critical attempt at safeguarding human rights (European Union, [2017](#)). Regardless, the Directive provides a basis for holding member states accountable or sanctioned for non-compliance (Orji, [2019b](#)).

## ECOWAS Cybersecurity Agenda

The Cybersecurity Agenda comprises policies and strategies formulated to address cybercrime and cybersecurity concerns in West Africa. It is specifically aimed at ensuring a secure cyberspace and improving the capability of member states to respond to cyber-attacks. The agenda includes Cybersecurity and Cybercrime Strategy, Critical Infrastructure Protection Policy, West Africa Response to Cybersecurity and the Fight against Cybercrime. The ECOWAS Cybersecurity and Cybercrime Strategy was designed to establish a coordinated regional effort to address the consequences of cybercrime and improve cybersecurity by implementing a strategic framework by the member states by 2022 (ECOWAS Parliament, [2021](#)).

## Regional Meetings, Forums, and Workshops

ECOWAS has been addressing cybercrime in West Africa through regional meetings, forums and workshops. An example is the West Africa Internet Governance Forum (WAIGF), which encourages dialogues among relevant actors on internet governance-related issues, including cybercrime (Internet Governance Forum [IGF], [n.d.](#)). The 12th WAIGF, held in July 2020, focused on using the internet and digital landscape during the

COVID-19 pandemic, especially trust and privacy issues, and cybercrime in the digital era (Economic Community of West African States, [2020](#)). ECOWAS also participated in the first Africa Forum on Cybercrime in 2018, organised by the African Union, to address cybercrime policies, legislation, international cooperation and capacity building (The NATO Cooperative Cyber Defence Centre of Excellence [CCDCOE], [n.d.](#)). Inter-ministerial meetings have been utilised to prioritise cybercrime issues, exemplified by the 15th and 17th meetings of ECOWAS Ministers in charge of telecommunication and ICT, which aimed to promote cybersecurity and combat cybercrime for a safer cyber environment (Economic Community of West African States, [2017](#)). In January 2020, a workshop was conducted to review and validate the ECOWAS Regional Cybersecurity and Cybercrime Strategy and the Regional Critical Information Infrastructure Policy (Economic Community of West African States, [2020](#)). Law enforcement agencies, represented by the West Africa Police Chief Committee (WAPCCO), have also emphasised the need for collective expertise and effective enforcement of existing policy frameworks to combat cybercrime and money laundering (Economic Community of West African States, [2019](#)).

### **International Cooperation and Partnership**

Cybercrime is a transnational crime; hence the reason for ECOWAS to seek international collaborations to address the threats of cybercrime. ECOWAS has done this through collaboration with organisations such as the International Telecommunication Union (ITU), United Nations Office on Drugs and Crime (UNODC), INTERPOL, Council of Europe (COE), and the European Union (EU), among others. For instance, ECOWAS and ITU signed a memorandum of understanding (MOU) in 2015 on cooperation within the ITU Global Cybersecurity Agenda framework, designed to improve cybersecurity. The MOU focuses on regional cybersecurity programmes, national Computer Emergency Response Team (CERT) programmes, capacity building, online protection of children, and harmonisation of cybercrime laws (ITU, [2015](#)).

Furthermore, ECOWAS and INTERPOL launched the West Africa Police Information System (WAPIS) in 2015 in Ghana. WAPIS aims to improve information sharing and coordination among various law enforcement bodies in West Africa. WAPIS consists of national electronic databases connected to regional information-sharing systems monitored by

the ECOWAS (Interpol, [2015](#)). Under WAPIS, national police information systems are also associated with the INTERPOL Global Police Communication System. This fosters global information sharing and allows law enforcement agencies across West Africa to coordinate their efforts against cybercrime (Interpol, [2020](#)).

### **Capacity Building**

Capacity-building programmes are essential to strengthen member states' capability to address cybercrime and its impact. ECOWAS capacity-building initiatives include its collaboration with the United Nations Conference on Trade and Development (UNCTAD) to organise online training sessions and workshops to improve the implementation of regional acts (the Directive on Cybercrime and e-commerce law) in 2013 (United Nations Conference on Trade and Development [UNCTAD], [2015](#)). ECOWAS, Global Prosecutors E-crime Network (GPEN) and CoE also collaborated to train prosecutors and investigators in West Africa in 2016. The training attempts to help prosecutors and investigators overcome challenges relating to cybercrime detection, investigation and prosecution (Economic Community of West African States, [2015](#)). Moreover, CoE and the ECOWAS Commission established courses on cybercrime and electronic evidence for judges and prosecutors in West Africa in 2017 and 2018 (The Council of Europe [COE], [2018](#)). Furthermore, ECOWAS, EU, Expertise France and the Government of Burkina Faso collaborated to provide a cybersecurity awareness campaign and relevant equipment to Burkina Faso's Digital Investigation Laboratory of the Central Cybercrime Brigade (Economic Community of West African States, [2021](#)).

### **Factors Militating ECOWAS s Role as a Capable Guardian**

Despite these initiatives, the ability of ECOWAS to play the role of a capable guardian has been impeded by several factors.

#### ***Inadequate Expertise***

West Africa and Africa face a shortage of cybersecurity experts to combat cybercrime. The African continent has only around 6,892 certified cybersecurity professionals, while Nigeria and Ghana have approximately 1,500 and 460 experts, respectively, according to the 2016 African Cybersecurity Report (Musuva-Kigen et al., [2016](#)). In 2017, the numbers increased to around 10,000 certified professionals in Africa out of the total 1 billion population (Kaimba, [2017](#)), still significantly fewer than countries

such as the UK, with 98,000 to 171,000 cybersecurity professionals for its population of 66 million (Scroxtton, [2021](#)). Moreover, West Africa lacks dedicated cyber criminologists and research centres compared to the West. This shortage of expertise forces ECOWAS to rely on the INTERPOL, among others, for assistance. Expertise and research centres are needed to contribute to the formulation of effective cyber laws and policies based on evidence and within the context and peculiarity of West Africa's cybercrime problems (Ndubueze, [2020](#)).

### ***The Problem of Political Commitment***

There is a low level of commitment among ECOWAS member states to combat cybercrime. ECOWAS annual reports give little attention to cybercrime compared to other policy areas. This may be because cybersecurity is often viewed as a luxury rather than a necessity in Africa (Kshetri, [2019](#)).

The 2018 Global Cybersecurity Index report shows that no West African country has a high commitment to cybersecurity, with most having a low or medium commitment. Only Nigeria, Benin, Ivory Coast, Ghana and Burkina Faso have a medium level of commitment, while the remaining ten ECOWAS member states have a low commitment towards cybersecurity (ITU, [2019](#)). Low commitment to cybersecurity in ECOWAS member states leads to reluctance in implementing regional cybersecurity and anti-cybercrime policies nationally. As of 2021, only two countries in West Africa (Guinea Bissau and Liberia) lack cybercrime legislation, an improvement from it being four countries in 2019 (United Nations Trade and Development, [2021](#)). However, this still falls short of the requirement set by Article 35(1) of the ECOWAS Directive on Fighting Cybercrime, which requires all member states to have functional cybercrime legislation by January 1, 2014 (Orji, [2019b](#)). Furthermore, only three ECOWAS members (Cabo Verde, Ghana, and Senegal) have ratified the Budapest Convention, the major international convention on cybercrime (COE, [n.d.](#)). Table 1 also sheds light on the level of commitment to cybercrime and cybersecurity in West Africa.



**Table 1**

*Level of Commitment to Cybersecurity of each ECOWAS Member State according to the 2018 Global Cybersecurity Index.*

Country	Global Rank	Score	Commitment Level
Nigeria	57	0.65	Medium
Benin	80	0.49	Medium
Ivory Coast	86	0.46	Medium
Ghana	89	0.44	Medium
Burkina Faso	96	0.40	Medium
Senegal	102	0.31	Low
Gambia	104	0.28	Low
Liberia	117	0.21	Low
Guinea	122	0.19	Low
Sierra Leone	136	0.18	Low
Niger	150	0.09	Low
Togo	151	0.09	Low
Mali	152	0.09	Low
Guinea-Bissau	162	0.06	Low
Cabo Verde	163	0.05	Low

*Note.* Source: ITU (2019). The 2018 ITU Global Cybersecurity Index report examines countries’ level of commitment towards cybersecurity from five dimensions: legality, technicality, capacity-building and cooperation.

### ***Inadequate Funding***

Financial resources are an essential piece to solving the puzzle of the cybercrime problem. A shortage of funds always poses a big challenge. The ECOWAS region is poor, but the ECOWAS is one of the few regional organisations that have the capacity to devise a mechanism to help gather financial resources. In 2000, it instituted a 0.5 per cent on values of all goods imported into the region, which would then be collected by member states and paid into a special account. This is called the community levy. Despite this mechanism, the challenge for the ECOWAS lies in accessing the levy. There is also an “accessed contribution system” for the member states to fund the ECOWAS operational budget (Vanheukelom, 2017). However, many countries have accumulated massive arrears. Another challenge for the ECOWAS is that it cannot attract additional contributions from member

states for emergencies, such as in the case of the Ebola epidemic (Vanheukelom, [2017](#)).

In 2021, the ECOWAS passed a 557 million US dollar budget, which saw a 6.5 per cent increase compared to the 2020 budget (ECOWAS Parliament, [2021](#)). This is quite impressive given the financial impact of the 2020 pandemic, but it is also relatively low compared to the EU 2021 budget of about 166 billion euros (European Commission, [2020](#)). Considering cybersecurity's cost, 557 million dollars is insufficient for ECOWAS to cover cybersecurity and other regional priorities and projects.

### ***Imperfect Legal Framework***

No legal framework or document can be perfect. However, every loophole in a legislation can be a challenge to its effectiveness. Many loopholes have been noted in the ECOWAS regional instruments against cybercrime, especially the Cybercrime Directive. One such loophole is that the Directive lacks a dedicated and effective regional monitoring mechanism to facilitate the implementation of the provisions of the Directive at the national level. This challenge is an obstacle to the success of the Directive (Orji, [2019a](#)). Also, the ECOWAS and the Directive itself did not provide for sanctions against member states that refuse to implement the provisions in the Directive within the recommended timeframe (January 1, 2014). This poses a threat of nonchalance from member states that are reluctant and non-compliant (Orji, [2019b](#)).

Furthermore, the International Communication Union (ITU) has some essential items and provisions that were excluded from the Directive. For example, the criminalisation of novel phenomena such as identity theft was excluded from the Directive. The procedural provision only covers search and seizure. Legal interception of data and real-time collection of traffic data, which are present in the ITU Toolkit for cybercrime legislation and Budapest Convention of 2001, were not present in the Directive. Also, the Directive has one provision for judicial cooperation among member states. This is not enough, given that there are many challenges relating to cooperation, such as jurisdictional issues and extradition, in the fight against cybercrime (ITU, [2013](#)).

### ***Slow Pace of Legislation and Law Enforcement***

Another challenge for ECOWAS is that the process of creating and updating cybercrime laws can be too slow and protracted, especially in

countries such as Nigeria that operate a bicameral legislative system. The process could also be protracted due to public hearings and harmonisation (if there are different versions of the same bill) (Ndubueze, [2020](#)). This slow pace of establishing legislation and amending legislation is evident in the fact that about eight West African countries lack cybercrime laws as of 2019 (UNCTAD, [2019](#)). These include the cybercrime laws that were supposed to be due by January 1, 2014, according to the ECOWAS Cybercrime Directive (Orji, [2019a](#)). Furthermore, the enforcement of cybercrime laws is relatively low in this part of the world. For instance, a survey report by Trend Micro and INTERPOL shows that an average of 30 per cent of cybercrime reported each year (2013 to 2015) led to arrest (Flores et al., [2017](#)).

The slow pace of legislation and law enforcement is a challenge for ECOWAS and its member states because it implies their inability to keep up with the ever-evolving nature of ICTs. Technological innovation creates ever-evolving tools to commit crimes. This means law enforcement and the judiciary might find it challenging to keep up with the changes because a large pool of resources is required to constantly improve tools, methods and knowledge (Swiatkowska, [2020](#)), which countries in West Africa cannot afford. As Abdul-Hakeem Ajijola (a cybersecurity expert) puts it, cybercriminals operate at the speed of light while law enforcement moves at the speed of law (Musuva-Kigen, [2016](#)).

### ***Problem of Dependency***

A big problem with international or regional organisations such as ECOWAS is that they cannot fully operate effectively without the effort and willingness of its member states to contribute their quota. The ECOWAS Commission needs its member states to domesticate regional instruments on cybercrime and cybersecurity. The failure of member states to do that results in ECOWAS becoming handicapped. There is little the organisation can do other than persuading or appealing to its members to ratify, adopt, domesticate and implement these regional instruments.

This portends that the effectiveness of ECOWAS anti-cybercrime efforts depends on the capability of individual member states. There are countries (such as Nigeria and Ghana) with the ability to implement ECOWAS anti-cybercrime policy. In contrast, others do not have the capacity because various socioeconomic problems ravage them, leaving

them with a lack of strong infrastructure to ensure a safe cyberspace as intended by ECOWAS. So, the success of ECOWAS largely depends on its members ability and willingness to fight cybercrime. This is the reality of most regional organisations.

### ***The Problem of Digital Literacy***

Ndubueze ([2020](#)) noted that the problem of inadequate digital skills lies in the relatively low digital literacy in the African continent as a whole as compared to other regions of the world. Similarly, most internet users in Africa and West Africa, to be specific, do not have the necessary skills to stay protected from cyber-attacks on the internet (Kshetri, [2019](#)). Another problem is the issue of language. A lot of West Africans do not speak English, which is the language of the internet, and those who speak English, do so reluctantly as it is not their first language. In other words, Francophone and Lusophone countries are in the region where their citizens might have problems understanding English correctly. English is critical because most information, instructions and contents of cybersecurity products are in English, which many people in the region do not speak or understand (Kshetri, [2019](#)).

Apart from the problem of language and digital skills, the problem of literacy within the region can give us an insight into the dearth of digital literacy. For instance, in 2009, an Oxfam study confirmed that West Africa has the highest illiteracy rate in the world, with about 65 million of its adult citizens (40 per cent of the adult population) being unable to read and write (The New Humanitarian, [2009](#)). Also, in 2018, only four countries (Nigeria, Cabo Verde, Ghana, and Togo) within the region had more than 50% female adult literacy rate (Sasu, [2024](#)). The implication of this is that when a sizable number of the citizens in the region are illiterate or digitally literate, they become more vulnerable to cyber-attacks and frauds, especially when they find themselves in the digital environment (e.g., mobile and online banking or financial services). This is a challenge to ECOWAS and its member states because it makes it more difficult to curb cybercrime when the citizens do not have the basic skills to protect themselves from cyber threats.

### **Conclusion**

This paper explored cybercrime in West Africa from the Routine Activity Theory (RAT) perspective, which posits that crime occurs when a likely offender, a suitable target, and the absence of a capable guardian converge

in time and space. The paper has discussed the nature of cybercrime in West Africa and the role of ECOWAS as a capable guardian in combating cybercrime. The study finds that ECOWAS employed various measures to combat cybercrime, including a legal framework, cybersecurity agenda, regional meetings, international cooperation, and capacity building. Furthermore, the study finds that ECOWAS efforts are being hampered by factors such as inadequate expertise, political commitment, funding, imperfect legal framework, slow pace of legislation and law enforcement, and prevalence of digital illiteracy. These challenges have also been confirmed in studies by Kshetri (2019) and Ndubueze (2020). Ndubueze (2020) indicated that digital literacy problems, inadequate skills, and slow legislative process are among the significant challenges of cybercrime countermeasures in Africa.

Ultimately, cybercrime is a serious threat to the security and development of West Africa and it requires a coordinated and comprehensive response from all stakeholders. ECOWAS has a vital role as a capable guardian in fostering concerted efforts to achieve a safer and more secure cyberspace for the sub-region. However, ECOWAS must also address some of the gaps and limitations in its current policies and strategies, such as safeguarding human rights, harmonising cyber laws, enhancing technical capabilities, and promoting public awareness and education.

### **Conflict of Interest**

The authors of the manuscript have no financial or non-financial conflict of interest in the subject matter or materials discussed in this manuscript.

### **Data Availability Statement**

The data associated with this study will be provided by the corresponding author upon request.

### **Funding Details**

No funding has been received for this research.

### **References**

Adelaja, O. (n.d.). *Catching up with the rest of the world: The legal framework of cybercrime in Africa*. Retrieved July 22, 2020, from <http://afsaap.org.au/assets/Adelaja.pdf>

- African Union Commission & Symantec. (2016). *Cybercrime and cybersecurity trends in Africa*. Symantec. [https://securitydelta.nl/media/com\\_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf](https://securitydelta.nl/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf)
- Alkaabi, A., Mohay, G., McCullagh, A., & Chantler, N. (2010, October 4–6). *Dealing with the problem of cybercrime* [Paper presentation]. Proceedings of International Conference on Digital Forensics and Cyber Crime. Abu Dhabi, United Arab Emirates.
- Atta-Asamoah, A. (2009). Understanding the West African cybercrime process. *African Security Review*, 18(4), 106–114. <https://doi.org/10.1080/10246029.2009.9627562>
- Calderoni, F. (2010). The European legal framework on cybercrime: Striving for an effective implementation. *Crime, Law and Social Change*, 54(5), 339–357. <https://doi.org/10.1007/s10611-010-9261-6>
- Cerezo, A. I., Lopez, J., & Patel, A. (2007, August 27–28). *International cooperation to fight transnational cybercrime* [Paper presentation]. Proceedings of Second International Workshop on Digital Forensics and Incident Analysis. Karlovassi, Greece.
- Clough, J. (2012). The council of Europe convention on cybercrime: Defining crime in a digital world. *Criminal Law Forum*, 23(4), 363–391. <https://doi.org/10.1007/s10609-012-9183-3>
- Council of Europe. (n.d.). *Chart of signatures and ratifications of treaty 185*. Retrieved June 5, 2020, from <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?desktop=tru>
- Digwatch. (2011). *Directive C/DIR.1/1/08/11: The directive on fighting cybercrime within ECOWAS*. <https://dig.watch/resource/directive-fighting-cybercrime-within-ecowas>
- Duah, F. A., & Kwabena, A. M. (2015). The impact of cybercrime on the development of electronic business in Ghana. *European Journal of Business and Social Sciences*, 4(1), 22–34
- Economic Community of West African States. (2015, May 31). *ECOWAS, GPEN, COE host cybercrimes training*. <https://tit.comm.ecowas.int/?p=10660>

Economic Community of West African States. (2017). *ECOWAS ICT ministers approve free roaming for west Africa*. <https://old22.ecowas.int/24641/>

Economic Community of West African States. (2019, May 15). *ECOWAS Commission urges harmonised strategies and collective expertise to tackle regional security*. <https://www.ecowas.int/ecowas-commission-urges-harmonised-strategies-and-collective-expertise-to-tackle-regionalsecurity/>

Economic Community of West African States. (2020, July 29). *ECOWAS encourages engagement and cooperation towards the development of a digital economy at the 12th West Africa Internet Governance Forum (WAIGF)*. <https://www.ecowas.int/ecowas-encourages-engagement-and-cooperation-towards-the-development-of-a-digital-economy-at-the-12th-west-africa-internet-governance-forum-waigf/>

Economic Community of West African States. (2021, March 28). *Official handover Ceremony for the digital investigation laboratory equipment in Burkina Faso and launch of the cybersecurity awareness campaign*. <https://www.ecowas.int/official-handover-ceremony-for-the-digital-investigation-laboratory-equipment-in-burkina-faso-and-launch-of-the-cybersecurity-awareness-campaign/>

ECOWAS Parliament. (2021). *ECOWAS Parliament issues favourable opinion on the adoption for of six community acts*. <https://www.parl.ecowas.int/ecowas-parliament-adopts-six-community-acts/>

European Commission (2020, December 18). *EU budget 2021: A kick-start of the European recovery*. [https://ec.europa.eu/commission/presscorner/detail/en/IP\\_20\\_2489](https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2489)

European Union. (2017, September 11–13). *ECOWAS and the Council of Europe join forces to help west African countries in the fight against cybercrime*. <https://www.ecowas.int/ecowas-and-the-council-of-europe-join-forces-to-help-westafrican-countries-in-the-fight-against-cybercrime/>

Felson, M., & Cohen, L. E. (1980). Human ecology and crime: A routine activity approach. *Human Ecology*, 8, 389–406.

- Flores, R., Matsukawa, B., Remorin, A., Sancho, D., Yamakazi, T., & Wong, A. (2017). *Cybercrime in West Africa: Poised for an underground market*. Trend Micro. <https://documents.trendmicro.com/assets/wp/wp-cybercrime-in-west-africa.pdf>
- Global Initiative. (2016). *Cybercrime in West Africa: Poised for an underground market by Trend Micro and Interpol*. <https://globalinitiative.net/cybercrime-in-west-africapoised-for-an-underground-market/>
- Hill, J. B., & Marion, N. A. (2016). *Introduction to cybercrime: Computer crimes, laws, policing in the 21st century*. Praeger Publisher.
- Holt, T. J., & Bossler, A. M. (2015). *Cybercrime in progress: Theory and prevention of technology-enabled offences*. Routledge.
- Hove, K. (n.d.). *The SADC model law on computer crime and cybercrime: A harmonised assault on the right to privacy?* Retrieved November 17, 2020, from <https://www.veritaszim.net/node/1787>
- International Telecommunication Union. (2013). *Cybercrime directive: An explanatory notice*. Geneva: ITU. [https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/cybercrime\\_directive-explanatory\\_notice.pdf](https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPSSA/Documents/FINAL%20DOCUMENTS/FINAL%20DOCS%20ENGLISH/cybercrime_directive-explanatory_notice.pdf)
- International Telecommunication Union. (2015). *ECOWAS*. <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/gpECOWAS.aspx>
- International Telecommunication Union. (2019). *Global cybersecurity index 2018*. [https://www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf)
- Internet Governance Forum. (n.d.). *About us*. Retrieved July 22, 2020, from <https://waigf.ecowas.int/about-us/>
- Interpol. (2015, September 30). *INTERPOL launches first national electronic police information system for West African countries*. <https://www.interpol.int/en/News-andEvents/News/2015/INTERPOL-launches-first-national-electronic-police-informationsystem-for-West-African-countries>



- Interpol. (2020). *West Africa police information system (WAPIS)*. <https://www.interpol.int/en/How-we-work/Capacity-building/WAPIS-Programme>
- Interpol. (n.d.). *Cybercrime*. Retrieved July 22, 2024, from <https://www.interpol.int/Crimes/Cybercrime>
- Jamil, Z. (2012). Global fight against cybercrime: Undoing the paralysis. *Georgetown Journal of International Affairs*, 109–120. <https://www.jstor.org/stable/43134344>
- Kaimba, B. (2017). *Africa cybersecurity report 2017*. Serianu. <https://www.serianu.com/downloads/NigeriaCyberSecurityReport2017.pdf>
- Kshetri, N. (2019). Cybercrime and cybersecurity in Africa. *Journal of Global Information Technology Management*, 22(2), 77–81.
- Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior*, 37(3), 263–280. <https://doi.org/10.1080/01639625.2015.1012409>
- Madero-Hernandez, A., & Fisher, B. S. (2012). Routine activity theory. In F. T. Cullen & P Wilcox (Eds.), *The oxford handbook of criminological theory*. Oxford Academic. <https://doi.org/10.1093/oxfordhb/9780199747238.013.0027>
- Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., & Ignatuschtschenko, E. (2013). *Comprehensive Study on Cybercrime*. United Nations. [https://www.unodc.org/documents/organized-crime/UNODC\\_CCPCJ\\_EG.4\\_2013/CYBERCRIME\\_STUDY\\_21021\\_3.pdf](https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_21021_3.pdf)
- Miró, F. (2014). Routine activity theory. In J. M. Miller (Ed.), *The encyclopedia of theoretical criminology* (pp. 1–7). Wiley Online Library.
- Musuva-Kigen, P., Ekpeke, M., Inkoom, E., Inkoom, B., Masesa, D., Kaimba, B., Kimani, K., Mwangi, M., Munyendo, B., Mueni, F., Ndegwa, D., Wanjuki, S., Rishad, N., Keige, S., Karanja, J., Soita, H., Ngari, A. N., Nturibi, B. M., Ndegwa, D., ... Mbae, K. (2016). *Africa cybersecurity report 2016*. Serianu.

<https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf>

- Ndubueze, P. N. (2020). Cybercrime and legislation in an African context. In T. J. Holt & A. M. Bossler (Eds.), *The palgrave handbook of international cybercrime and cyberdeviance* (pp. 345–364). Springer.
- Orji, U. J. (2015). *Multilateral legal responses to cyber security in Africa: Any hope for effective international cooperation?* [Paper presentation]. Proceedings of 7th International Conference on Cyber Conflict: Architectures in Cyberspace. Tallinn, Estonia.
- Orji, U. J. (2019a). A review of the ECOWAS cybercrime directive- analysis of ICT offences with the Budapest convention and key challenges hindering its implementation in member states. *Computer Law Review International*, 20(2), 40–53.
- Orji, U. J. (2019b). An inquiry into the legal status of the ECOWAS cybercrime directive and the implications of its obligations for member states. *Computer Law & Security Review*, 35(6), Article e105330. <https://doi.org/10.1016/j.clsr.2019.06.001>
- Paoli, L., Visschers, J., & Verstraete, C. (2018). The impact of cybercrime on businesses: A novel conceptual framework and its application to Belgium. *Crime, Law and Social Change*, 70(4), 397–420.
- Pasculli, L. (2020). The global causes of cybercrime and state responsibility: Towards an integrated interdisciplinary theory. *Journal of Ethics and Legal Technologies*, 2(1), 48–74.
- Pratt, T. C., Holtfreter, K., & Reisig, M. D. (2010). Routine online activity and internet fraud targeting: Extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency*, 47(3), 267–296. <https://doi.org/10.1177/0022427810365903>
- Saravade, N. (2016). International and regional responses to cybersecurity challenges. In C. Samuel & M. Sharma (Eds.), *Securing cyberspace: International and Asian perspectives* (pp. 244–254). Pentagon Press and Institute for Defence Studies and Analyses
- Sasu, D. D. (2024, January 30). *Female adult literacy rate in West Africa in 2018, by country*. Statista.

<https://www.statista.com/statistics/1122662/female-adult-literacy-rate-inwest-africa-by-country/>

Schjolberg, J. S. (2008). The history of global harmonization on cybercrime legislation—the road to Geneva. *Journal of International Commercial Law and Technology*, 1(12), 1–19.

Scroxtton, A. (2021, March 24). *UK faces significant cyber talent shortfall*. Computer Weekly. <https://www.computerweekly.com/news/252498337/UK-faces-significant-cyber-talent-shortfall>

Shaw, M. (2018, January 9). *Known unknowns: The threat of cybercrime in Africa*. Institute for Security Studies. <https://issafrica.org/iss-today/known-unknowns-the-threat-of-cybercrime-in-africa>

Shinder, D. L., & Cross, M. (2008). *Scene of the cybercrime* (2nd ed.). Syngress.

Stalans, L. J., & Donner, C. M. (2018). Explaining why cybercrime occurs: Criminological and psychological theories. In H. Jahankhani (Ed.), *Cyber criminology* (pp. 25–45). Springer.

Swiatkowska, J. (2020). *Tackling cybercrime to unleash developing countries' digital potential*. Pathways for Prosperity Commission. <https://pathwayscommission.bsg.ox.ac.uk/node/299/>

The Council of Europe. (2018, November 12–15). *GLACY+: Second regional training on cybercrime for the ECOWAS countries and Mauritania*. [https://www.coe.int/en/web/cybercrime/glacyplusactivities/-/asset\\_publisher/ekq5KxUZwAqU/content/ecowas](https://www.coe.int/en/web/cybercrime/glacyplusactivities/-/asset_publisher/ekq5KxUZwAqU/content/ecowas)

The NATO Cooperative Cyber Defence Centre of Excellence [CCDCOE] (n.d.). *Economic community of West African States*. Retrieved April 30, 2020, from <https://ccdcoe.org/organisations/ecowas/>

The New Humanitarian. (2009, April 22). *Combating world's lowest literacy* rate. <https://www.thenewhumanitarian.org/news/2009/04/22/combating-worlds-lowest-literacy-rates>

United Nations Trade and Development. (2015). *Review of e-commerce legislation harmonization in the Economic Community of West African*

*States.* <https://unctad.org/publication/review-e-commerce-legislation-harmonization-economic-community-west-african-states>

United Nations Trade and Development. (2021, December 14). *Cybercrime legislation worldwide.* <https://unctad.org/page/cybercrime-legislation-worldwide>

United Nations Trade and Development. (2019). *Cybercrime legislation worldwide.* [https://unctad.org/en/Pages/DTL/STI\\_and\\_ICTs/ICT4D-Legislation/eComCybercrimeLaws.aspx](https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eComCybercrimeLaws.aspx)

Vanheukelom, J. (2017). *Understanding the economic community of West African States: Political traction with Africa's oldest regional organization.* The European Centre for Development Policy Management. <https://ecdpm.org/wp-content/uploads/ECOWAS-Background-Paper-PEDRO-PoliticalEconomy-Dynamics-Regional-Organisations-Africa-ECDPM-2017.pdf>

Vogel, J. (2007, November 18–23). *Towards a global convention against cybercrime* [Paper presentation]. Proceedings of First World Conference of Penal Law. Penal Law in the 21st Century, Guadalajara, Mexico.

Yar, M. (2006). *Cybercrime and society.* Sage Publication.