الإرهاب السيبراني والأمن القومي للدول الإفريقية في بيئة متغيرة

د. مصطفى شفيق علام
خبير في الشؤون الإفريقية والأمن الإقليمي

ألقت التطورات الثورية غير المسبوقة في عالم التكنولوجيا والاتصالات بظلالها على قارة إفريقيا، التي أضحت ساحة تحوّل رقمي سريعة وواعدة، في ظل اعتبار البيئة الرقمية عنصراً أساسياً في تعزيز التنافسية الدولية على الساحة العالمية.

فقد أدت التحولات الرقمية السريعة في القارة الإفريقية إلى تزايد الاعتماد على تكنولوجيا الاتصال، ودفعت إلى اعتماد تقنيات متقدمة، مثل الخدمات المصرفية عبر الهاتف المحمول، والتجارة الإلكترونية، والحوسبة السحابية على نطاقٍ واسع، مما عزز من بيئة النمو الاقتصادي والابتكار.

لكن على الجانب الآخر؛ طرح ذلك التوسع التقني (التكنولوجي والاتصالي)، في إفريقيا، العديد من التحديات في مجال الأمن السيبراني، إذ تحولت البنى التحتية الرقمية إلى أهدافٍ ذات جاذبيةٍ خاصّة للجهات الفاعلة، من الدول ومن غير الدول على حدٍّ سواء، في مجال التهديدات السيبرانية.

وعلى الرغم من وجود أكثر من ٥٧٠ مليون مستخدم للإنترنت في المنطقة، وفقاً للتقديرات الدولية المعتمدة لعام ٢٠٢٥م[١]، فلا تزال العديد من البلدان الإفريقية تفتقر إلى تدابير كافية لحفظ الأمن السيبراني، مما يجعل الشركات والأفراد وحتى الحكومات عرضةً للجرائم والاختراقات الإلكترونية والإرهاب السيبراني، فيما تواجه العديد من البلدان في جميع أنحاء القارة الإفريقية تحدياتٍ متزايدة، مثل الأطر القانونية التي لا تزال في طور التشكل، ومحدودية الاستثمار في الأمن السيبراني، وتنامي فجوات المعرفة الرقمية، مما يزيد من تفاقم هذه المخاطر.

وقد أدى الاستخدام الواسع للهواتف الذكية والأجهزة الإلكترونية المحمولة إلى جعل تلك المنصات أهدافاً أمنية رخوة لمجرمي الإنترنت، سواءً من الأفراد أو عصابات الجريمة المنظمة وصولاً إلى الجماعات الإرهابية، وخاصةً في المناطق التي تشهد انتشاراً كبيراً للخدمات المصرفية عبر الهاتف المحمول. بالإضافة إلى ذلك، يُشكّل التكامل المتزايد لأجهزة إنترنت الأشياء IoT في قطاعاتٍ مثل الزراعة والرعاية الصحية والتصنيع مخاطرَ أمنية جديدة في إفريقيا، حيث يفتقر العديد من هذه الأجهزة إلى حمايةٍ قوية.

وبحسب مؤشر التهديدات العالمية، الصادر في يناير ٢٠٢٥م، عن شركة «تشيك بوينت سوفتوير تكنولوجيز» Check Point Software Technologies المتخصصة في حلول الأمن السيبراني، فإن هناك ٨ دول إفريقية على قائمة أكثر ٢٠ دولةً في العالم تعرّضاً للهجمات السيبرانية للعام ٢٠٢٤م، وهي: إثيوبيا وزيمبابوي وأنجولا وأوغندا ونيجيريا وكينيا وغانا وموزمبيق، وفقاً لما أكدته بيانات الكشف عن البرامج الضارة من مؤشر التهديدات السيبرانية العالمي للاتحاد الدولي للاتصالات، الأمر الذي يؤكد الحاجة الملحّة إلى تطوير أطر عمل أكثر فاعلية للأمن السيبراني لحماية التطورات الرقمية وضمان المرونة على المدى الطويل في إفريقيا.

وتناقش الدراسة تأثيرات الإرهاب السيبراني على الأمن القومي في قارة إفريقيا، من خلال أربعة محاور رئيسة:

يناقش أولها: العلاقة بين الأمن القومي والأمن السيبراني في إفريقيا، مع رصد مؤشرات الأمن السيبراني وفقاً للاتحاد الدولي للاتصالات.

فيما يتناول ثانيها: مخاطر الإرهاب السيبراني في قارة إفريقيا.

بينما يحلل ثالثها: إستراتيجيات مكافحة الإرهاب السيبراني في إفريقيا.

وأخيراً؛ يستشرف رابعها: مستقبل الأمن القومي الإفريقي في ضوء تهديدات الإرهاب السيبراني المتزايدة في القارة.

(١) Number of internet users in Africa from 2014 to 2029, Statista, accessible at: https://www.statista.com/forecasts/1146636/internet-users-in-africa

أولاً: الأمن القومي والأمن السيبراني في إفريقيا، مع رصد مؤشرات الأمن السيبراني وفقاً للاتحاد الدولي للاتصالات:

وفقاً لدليل وزارة العدل الأمريكية؛ يُعدّ «الأمن القومي» مصطلحاً جامعاً يشمل: «الدفاع الوطني، والاستخبارات ومكافحة التجسس، والأمن الدولي والداخلي، والعلاقات الخارجية». ويتضمن ذلك: مكافحة الإرهاب؛ ومكافحة التجسس والتجسس الاقتصادي الذي يُمارس لصالح أي حكومة أجنبية أو جهة أجنبية أو عميل أجنبي؛ وإنفاذ ضوابط التصدير والعقوبات؛ والتصدي لتهديدات الأمن السيبراني التي ترتكبها الدول، أو الإرهابيون، أو عملاؤهم، أو وكلاؤهم[١].

وعلى صعيد العلاقة بين الأمن السيبراني والأمن القومي؛ يُنظر إلى الفضاء السيبراني باعتباره المجال الرابع للدولة، إضافةً إلى المجالات الثلاثة الأخرى (الجو والبر والبحر)، وقد أصبحت مسألة حمايته والدفاع عنه مصدر قلق لدى العديد من صنّاع القرار في الدولة، نظراً لارتباطه الوثيق بالأمن القومي.

ويُمثّل التحدي الذي يفرضه الفضاء السيبراني هاجساً ملحّاً، يتمثل في المخاطر المحيطة باستخدامه على مؤسسات الدولة والأفراد، وذلك بسبب الزيادة الكبيرة في عدد مستخدمي الحاسوب، وتنوّع استخداماتهم وأماكن عملهم، واختلاف ثقافاتهم، وأهدافهم، وانتماءاتهم، إضافةً إلى التوسع في استخدام شبكة المعلومات الدولية على الإنترنت.

ويُعدّ انعدام الأمن السيبراني وهشاشته أمام عمليات الاختراق المستمرة أداةً فعّالة قادرة على المساهمة في تدمير الدولة سياسياً، وأمنياً، واجتماعياً، واقتصادياً. وفي ضوء تطور التقنيات، تتطور أساليب الاختراق باستمرار، وفي الوقت نفسه يتزايد تأثيرها السلبي بشكلٍ كبير، مما يُهدد الأمن القومي للدول. لذا؛ ينبغي للدول أن تُولي اهتماماً جاداً لإيجاد وسائل دفاعية للتحقق من الأمن السيبراني، إلى حين تحقيق الاستقرار على جميع المستويات[٢].

وفقاً للاتحاد الدولي للاتصالات ITU؛ يمكن تعريف «الأمن السيبراني» باعتباره: مجموعة الأدوات والسياسات والمفاهيم والضمانات الأمنية والمبادئ التوجيهية ونهج إدارة المخاطر والإجراءات والتدريب، وأفضل الممارسات والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المؤسسة والمستخدمين. وتشمل أصول المؤسسة والمستخدمين: أجهزة الحوسبة المتصلة، والموظفين، والبنية التحتية، والتطبيقات، والخدمات، وأنظمة الاتصالات، وإجمالي المعلومات المرسلة والمخزنة في البيئة السيبرانية.

ويسعى الأمن السيبراني إلى ضمان تحقيق خصائص الأمن للمؤسسة وأصول المستخدم والحفاظ عليها ضد المخاطر الأمنية ذات الصلة في البيئة السيبرانية. وتشمل أهداف الأمن العامة: التوافر، والسلامة، والتي قد تشمل الأصالة، وعدم الإنكار، والسرّية[٣].

وفي هذا الإطار؛ طرح الاتحاد الدولي للاتصالات مؤشر الأمن السيبراني العالمي GCI الذي يُستخدم من قِبَل الدول ومجموعات الاستثمار ومنظمات التنمية والشركات، والجهات الفاعلة الأخرى، كأداةٍ

(١) National Security, Legal Information Institute, accessible at: https://www.law.cornell.edu/wex/national_security

(٢) Asmaa Khalid Jarjees Al-Tae, Hameeda Abdul-Hussain Al-Dhalimi, Adnan Kadhum Jabbar Al-Shaibani, Relationship of Cybersecurity and the National Security of the Country: Iraq Case Study, Sys Rev Pharm, 2020;11(12), p.469.

(٣) Definition of cybersecurity, ITU, accessible at: https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx

مهمة لفهم التزامات الأمن السيبراني حول العالم. ويتبنّى مؤشر الأمن السيبراني العالمي نهجاً متعدد الأبعاد، يؤدي إلى رؤية أكثر موثوقية واعتمادية لالتزامات الأمن السيبراني. ونتيجةً لذلك؛ أصبحت الدول تعتمد على مؤشر الأمن السيبراني العالمي لتوجيه خططها الوطنية للأمن السيبراني. ويقيس مؤشر الأمن السيبراني العالمي GCI التزام الدول بالأمن السيبراني من خلال خمس ركائز أساسية، هي: التدابير القانونية، التدابير التقنية، التدابير التنظيمية، تنمية القدرات، والتعاون[١].

١- ضعف التدابير القانونية السيبرانية الإفريقية:

يُعدّ وجود أطر قانونية وتنظيمية شاملة في الدولة أحد أهم مرتكزات مؤشر الأمن السيبراني العالمي، ويشير هذا المحدد إلى جملة من السياقات القانونية والإجرائية تتمثل في: التشريعات الخاصة بمكافحة الجرائم الإلكترونية، وأدوات وقواعد حماية البيانات الشخصية، وهياكل تنظيم البنية التحتية الحيوية الرقمية. وعلى المستوى القاري؛ اعتمد الاتحاد الإفريقي، في يونيو ٢٠١٤م، اتفاقية الاتحاد بشأن الأمن السيبراني وحماية البيانات الشخصية، المعروفة باسم «اتفاقية مالابو»، كآلية لتقنين التعاون وحماية البيانات وتشجيع استجابة موحدة للتهديدات السيبرانية، مما يجعل مدى توقيع الدول وتصديقها وتطبيق نصوص الاتفاقية مؤشراً مركزياً في هذا السياق. ومع ذلك؛ فإن ضعف الإطار القانوني في الدول الإفريقية، وكذلك التباين القانوني الكبير بين بلدان القارة، يعرقل جهود التعاون عبر الحدود في مواجهة الجرائم السيبرانية ونقل الأدلة والتحقيقات الجنائية[٢].

٢- هشاشة التدابير التقنية رغم محاولات التطوير:

تُعتبر التدابير التقنية الناجمة عن تطور القطاعات التكنولوجية أبرز محددات مؤشر الأمن السيبراني العالمي. وفي الإطار الإفريقي؛ يشهد الطلب الرقمي في القارة ارتفاعاً كبيراً، لكن البنية التحتية والتدابير التقنية لا تزال نادرة، إذ تستحوذ إفريقيا على أقل من ١٪ من سعة مراكز البيانات العالمية، على الرغم من نمو استخدام بيانات الهاتف المحمول بنحو ٤٠٪ سنوياً، أي ما يقرب من ضعف المتوسط العالمي، وفقاً لمنظمة «مجتمع الإنترنت» الأمريكية، الأمر الذي دفع البنك الدولي، في أبريل ٢٠٢٥م، عبر مؤسسة التمويل الدولية IFC التابعة له إلى التوجه نحو البيانات الرقمية في إفريقيا باستثمار قدره ١٠٠ مليون دولار. ومع ذلك؛ لا يخلو بناء مراكز البيانات في الأسواق الناشئة كإفريقيا من المخاطر، فإمدادات الطاقة غير الموثوقة، واللوائح التنظيمية المعقدة، وعدم الاستقرار السياسي، كلها عوامل قد تردع الجهات الفاعلة التجارية عن المضي قُدماً في الاستثمار في البنية التحتية التقنية في القارة.

٣- غياب التدابير التنظيمية الإفريقية الحاكمة:

ثمّة غيابٌ لافت في مجال التدابير التنظيمية الشاملة لإدارة وحفظ قطاع الأمن السيبراني في قارة إفريقيا، إذ يبدو الأمن السيبراني في غالبية دول القارة غير مدرج على قائمة أولويات السياسات الوطنية، في حين تبدو الشركات والمؤسسات الخاصة عاجزةً عن إدماج مثل تلك الإستراتيجيات

(١) Global Cybersecurity Index 2024 5th Edition, International Telecommunication Union, 2025, p.2.

(٢) AFRICAN UNION CONVENTION ON CYBER SECURITY AND PERSONAL DATA PROTECTION, African Union, 27 June 2014, accessible at: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

في سياساتها وتدابيرها التنظيمية بالشكل الكافي.

ومن أبـــرز التدابير التنظيميـــة لإدارة الفضاء الســـيبراني: تمتع الـــدول بوجود فرق الاســـتجابة للحوادث الأمنية المعلوماتية والسيبرانية CSIRT، وهي فرق وطنية أو مؤسســـية تتولى رصد الهجمات والاختراقـــات، وتحليلها، والتعامل معها فوراً، وتعمل بشـــكلٍ عام على المراقبـــة والتحذيـــر المبكر من الهجمات السيبرانية، والاستجابة السريعة للحوادث وتقليل آثارهـــا، وتحليل الثغرات ونشـــر التوصيات الأمنية، والتنسيق الوطني أو القطاعي مع فرق أخرى كفرق الحكومة أو مزوّدي الخدمة.

وفي سياق الأمن الســـيبراني في إفريقيا، وفقاً لبيانات البنك الدولي، فـــإن حوالي ١٠ دول من ٢٦ دولة في شـــرق وجنوب إفريقيا تتمتـــع بوجود هذا النـــوع من الفرق، بينما ٥ دول فقط من ٢٢ دولة في غرب ووسط إفريقيا لديها تلك الفرق بحسب بيانات العـــام ٢٠٢٤م[١]. هذا يعني أن أقل من نصف الدول الإفريقية في هـــذه المجموعـــات المناطقية لديها قدرة وطنية منظّمة رســـمياً للاســـتجابة للحوادث السيبرانية.

٤- الافتقار إلى تنمية القدرات السيبرانية الإفريقية:

يجمع مرتكز تنمية القدرات، كمحدد مهم لمؤشر الأمن السيبراني العالمي، مؤشرات متعددة؛ أهمها: التدريب وتوافر الكفـــاءات المحلية المتخصصة في مجالات الأمن السيبراني، حيث يؤدي ضعف القدرات المحلية في هذا الإطار إلى تنامي اعتماد الدول على خبرات استشـــارية وإدارية وتقنيـــة خارجية، الأمر الذي يلقي بظلاله الســـلبية على الاستجابة الوطنية للتهديدات إلى جانب التكلفة الاقتصادية.

فالاســـتثمارات الوطنيـــة في مجـــالات التعليم والتدريب الســـيبراني، وامتلاك كوادر وطنية مؤهلة لإدارة ذلك القطاع الحساس، من شأنه زيادة القدرة التشـــغيلية وتحســـين مقياس الوقت اللازم للتعامل مع الهجمـــات. وتفتقر الدول الإفريقيـــة غالباً إلى بنـــاء وتنمية القـــدرات الوطنية الخاصـــة بالفضاء الســـيبراني؛ سواءً على صعيد التشـــغيل والإدارة أو على صعيد الحمايـــة والتأمين، ما يزيد من مخاطر وتحديات الأمن السيبراني في القارة، ومن الدلالات الفارقـــة في هذا الإطار أنه فـــي إفريقيا، التي يبلغ عدد ســـكانها ما يزيد عن ١,٤ مليار نســـمة، يوجد ما يقرب من ٢٠ ألف متخصص معتمد فقط بمجال الأمن السيبراني[٢].

٥- محدودية التعاون السيبراني الإفريقي البيني والخارجي:

يشير مفهوم التعاون في مجال الأمن السيبراني، بحسب مؤشر الأمن السيبراني العالمي، إلى جملة من المؤشرات الفرعية، والتي تشمل: الاتفاقيات الثنائية للأمن الســـيبراني، والاتفاقيات متعـــددة الأطراف مع الدول الأخرى، واتفاقيات المســـاعدة القانونية المتبادلة المتعلقة بالأمن السيبراني، والشراكات بين القطاعين العام والخاص، إضافةً إلى الشراكات بين الوكالات الحكومية المعنية بالفضاء السيبراني.

وفـــي الإطار القاري؛ ثمّة حالة من الضعف على صعيد التعاون بين الدول الإفريقية فيما يتعلق بالأمن الســـيبراني، ما يجعل ذلك الأمر من أبرز التحديات أمام تعظيم قدرة بلدان القارة على مواجهة التهديدات

(١) Enhancing Cyber Resilience in Developing Countries, World Bank, January 29, 2025, accessible at: Enhancing Cyber Resilience in Developing Countries

(٢) Michelle Meineke, The cybersecurity industry has an urgent talent shortage. Here's how to plug the gap, World Economic Forum, Apr 28, 2024, accessible at: https://www.weforum.org/stories/2024/04/cybersecurity-industry-talent-shortage-new-report/#:~:text=In%20Africa%2C%20there%20are%20approximately%2020%2C000%20certified,in%20a%20continent%20of%201.4%20billion%20people.

المتزايدة في الفضاء الرقمي، حيث تبقى مستويات التنسيق الإقليمي في حدودها الدنيا على الرغم من تزايد التهديدات والتحديات أمام البنية السيبرانية في الدول الإفريقية، وقد يرجع ذلك بشكلٍ أساسي إلى ما يمكن وصفه بغياب آليات تبادل المعلومات حول الحوادث والتهديدات السيبرانية، إضافةً إلى حالة التفاوت التشريعي والقانوني بين دول القارة بعضها وبعض، وصولاً إلى غياب أو ضعف الثقة فيما يتعلق بتبادل البيانات الحساسة بين الدول الإفريقية.

وعلى الرغم من تعدد المنظمات الإفريقية وتنوع مظلاتها من حيث التخصص والشمول، مثل الاتحاد الإفريقي والمجموعات الاقتصادية الإقليمية مثل إيكواس وسادك، إلا أن دول القارة ومنظماتها لم تنجح حتى الآن في تفعيل أطر ملزمة وجامعة للتعاون التقني الأمني والاستخباراتي بشكلٍ فعّال. في هذا الإطار؛ يشير مؤشر الأمن السيبراني العالمي ITU Global Cybersecurity Index ٢٠٢٤ إلى تسجيل غالبية معظم الدول الإفريقية درجات متدنية فيما يتعلق بالتعاون الدولي، ما يعكس محدودية الاتفاقيات الثنائية ومتعددة الأطراف الإفريقية الدولية المعنية بقطاع الأمن السيبراني. وهو ما يتعدى الجانب الحكومي ليمتد أيضاً إلى القطاعين العام والخاص في إفريقيا، وغياب المبادرات المشتركة بين القطاعات الحكومية، والخاصة، والأهلية، لدعم الأمن السيبراني[١]. الأمر الذي يجعل من تعزيز التعاون الإفريقي في هذا المجال ضرورةً إستراتيجية، لضمان استجابة جماعية فعّالة وموثوقة إزاء التحديات والتهديدات السيبرانية العابرة للحدود وحماية الأمن الرقمي للقارة.

ثانياً: مخاطر الإرهاب السيبراني في قارة إفريقيا:

في حين شهدت قارة إفريقيا خلال العقدين الماضيين توسعاً رقمياً متسارعاً، تمثلت مظاهره الأساسية في انتشار الإنترنت، وتزايد استخدامات الهواتف الذكية، والعناية المتزايدة بمشروعات البنى التحتية الرقمية، إلا أن ذلك التوسع خلق حالةً من التهديدات السيبرانية الجديدة على الواقع الأمني الإفريقي المحمّل أساساً بالأزمات والفجوات الهيكلية البارزة، والتي لم تقتصر على الجرائم التقليدية، بل امتدت لتشمل أبعاداً إرهابية ذات تأثيرات محلية وإقليمية ممتدة وذات ارتباطات وثيقة بظاهرة الإرهاب العالمي.

ويشير مصطلح «الإرهاب السيبراني» إلى: تلك التهديدات الأمنية الناجمة عن أعمال التخريب التي تُرتكب عبر أجهزة كمبيوتر متصلة بالشبكة، وهو مصطلح ظهر في أواخر القرن العشرين. يتميز هذا النوع من الإرهاب بإمكانية إخفاء الهوية، وقدرته على إلحاق أضرار جسيمة عبر مساحات شاسعة، بتكلفة منخفضة نسبياً في كثيرٍ من الأحيان. ومع ذلك؛ يُعدّ تعريف الإرهاب السيبراني موضع جدل بين الباحثين والسياسيين ووسائل الإعلام، حيث تختلف وجهات النظر حول ماهية هذا النوع من الهجمات.

وفي هذا الإطار؛ يمكن تعريف «الإرهاب السيبراني» Cyber-terrorism إجرائياً باعتباره: محاولات المنظمات أو الجماعات الإرهابية لاستغلال الفضاء السيبراني لشن هجمات أو تخريب البنى التحتية الحيوية، أو الترويج للأيديولوجيا، أو جمع الأموال، أو التجنيد الإلكتروني.

وفي القارة الإفريقية، حيث تتداخل القدرات الأمنية السيبرانية الضعيفة مع انتشار جماعات مسلحة وتنظيمات إرهابية، تبرز مخاطر مرتفعة ومتزايدة تهدد الأمن القومي، والاستقرار الاقتصادي،

(١) International Telecommunication Union (ITU). Global Cybersecurity Index 2024 Report. Geneva: ITU, 2024, pp.20-21.

وبنية الحوكمة الرقمية في القارة الإفريقية[١].

١- تزايد معدلات الجرائم السيبرانية بالفضاء الإفريقي:

وفقاً لتقديرات الإنتربول الدولي لعام ٢٠٢٥م؛ فإن نحو ثلثي الدول الإفريقية الأعضاء يعانون من تزايد الجرائم الإلكترونية التي باتت تتراوح نسبتها ما بين المتوسطة والعالية من إجمالي الجرائم، إذ تُمثل الجرائم الإلكترونية أكثر من ٣٠٪ من إجمالي الجرائم المُبلّغ عنها في غرب وشرق إفريقيا. وتُعتبر عمليات الاحتيال الإلكتروني، وبرامج الفدية[٢]، والتصيد الاحتيالي، واختراق البريد الإلكتروني للشركات، والابتزاز الجنسي الرقمي، من أكثر التهديدات الإلكترونية المُبلّغ عنها في القارة، ما جعل نحو ٩٠٪ من حكومات الدول الإفريقية تُقر بأنها بحاجةٍ إلى «تحسينات كبيرة» في قدرات إنفاذ القانون أو الملاحقة القضائية المتعلقة بتلك الجرائم السيبرانية.

ووفقاً للتقديرات الأمنية المعتبرة للإنتربول الدولي؛ فقد تجاوز الإرهاب السيبراني الإفريقي مسألة كونه قضيةً تقنية ليتحول إلى ركيزةٍ أساسية تمس الاستقرار والسلام والتنمية المستدامة في إفريقيا. وهو يتعلق مباشرةً بالسيادة الرقمية للدول، ومرونة المؤسسات، وثقة المواطنين، وحُسن سير الاقتصادات الوطنية. ففي العام ٢٠٢٤م، ارتفعت الإشعارات المشتبه بها بعمليات احتيال بنسبة تصل إلى ٣٠٠٠٪ في بعض الدول الإفريقية، وفقاً لبيانات كاسبرسكي Kaspersky، أحد شركاء القطاع الخاص البارزين الذين يعملون مع إدارة مكافحة الجرائم الإلكترونية في الإنتربول[٣].

كما ارتفعت حالات الكشف عن برامج الفدية في إفريقيا في عام ٢٠٢٤م، حيث سجلت جنوب إفريقيا أعلى عدد من تلك الجرائم، حيث بلغ عددها ١٧٨٤٩ حالة، تلتها اقتصادات أخرى عالية الرقمنة مثل نيجيريا ٣٤٥٩ حالة وكينيا ٣٠٣٠ حالة. وشملت الحوادث هجمات على البنية التحتية الحيوية، مثل اختراق هيئة الطرق الحضرية في كينيا KURA، وعلى قواعد البيانات الحكومية، مثل اختراقات المكتب الوطني للإحصاء في نيجيريا NBS.

فيما ارتفعت الحوادث المتعلقة بالاحتيال الإلكتروني للأعمال بشكلٍ كبير، حيث شكلت ١١ دولةً إفريقية غالبية نشاط الاحتيال الإلكتروني للأعمال الناشئة في القارة. وفي غرب إفريقيا؛ ساهم الاحتيال عبر البريد الإلكتروني في ظهور منظمات إجرامية مؤثرة للغاية، تُقدّر حصيلتها من تلك الجرائم بملايين الدولارات، مثل عصابة «بلاك آكس» العابرة للحدود[٤].

٢- استهداف الإرهاب السيبراني للبنية التحتية الحيوية:

تعمد التنظيمات الإرهابية في إفريقيا إلى تعطيل الخدمات الأساسية للبنية التحتية، مثل الكهرباء،

(١) Cyberterrorism, EBSCO Knowledge Advantage, accessible at: https://www.ebsco.com/research-starters/political-science/cyberterrorism

(٢) برامج الفدية: هي نوع من البرامج الخبيثة التي تمنع من الوصول إلى الأجهزة الإلكترونية والبيانات المخزنة عليها، وذلك عادةً عن طريق تشفير ملفاتك. ثم تطلب مجموعة إجرامية فديةً مقابل فك التشفير. في حالة هجوم برامج الفدية لن يتمكن المستخدمون من الوصول إلى الأجهزة والبيانات المخزنة عليها؛ لأن الملفات مشفرة. عادةً ما يُطلب من المستخدمين التواصل مع المهاجم عبر بريد إلكتروني مجهول، أو اتباع تعليمات على صفحة ويب مجهولة، لدفع الفدية بعملة رقمية. وقد يهدد المهاجمون أيضاً بنشر البيانات التي يسرقونها.

(٣) INTERPOL Warns of Sharp Increase in Cyber Attacks on Western and Eastern Africa, Cyber Press, June 25, 2025, accessible at: https://cyberpress.org/interpol-warns-of-sharp-increase-/in-cyber-attacks

(٤) INTERPOL AFRICA CYBERTHREAT ASSESSMENT REPORT 2025, INTERPOL, MAY 2025, pp.10-25.

والنقـــل، والاتصالات، والبنـــوك، من خلال هجمات ســـيبرانية مؤثرة، إذ يؤدي نجاح تلك التنظيمات في ذلك إلى تأثيراتٍ موازية للعمليات الإرهابية التقليدية من انهيارٍ للخدمات، وإحداث شـــلل اقتصادي، بما يقـــود في الأخير إلـــى زعزعة ثقـــة المواطنين في الحكومات وخلخلة النظم الحاكمة. وتُشكّل هجمات الفدية وعمليات الاحتيال عبر الإنترنت أبرز أشكال التهديدات السيبرانية في إفريقيا- كما سلف بيانه.

وتبـــرز أهميـــة هـــذه التهديدات فـــي تأثيرها المالـــي المرتفع، وقدرتها على تعطيل البنية التحتية والخدمات الأساســـية. وفي هذا الإطار؛ تشير بعض التقديرات إلى أن مؤسســـة من بين كل ١٥ مؤسسةً إفريقية قد تعرضت لمحاولة استهداف برنامج فدية كل أســـبوع خلال الربع الأول من عام ٢٠٢٣م، بنسبةٍ تتجاوز ضِعفَي المعدل العالمي. كما رصدت التقارير الأمنيـــة الدولية المعنيـــة تزايد اســـتهداف البنية التحتية الرقمية فـــي إفريقيا على وجه الخصوص، إذ كشـــفت نحو نصف دول القـــارة تقريباً أن بنيتها التحتية تعرضت لهجوم فدية خلال ٢٠٢٣م، ويشمل ذلك اســـتهداف البنوك ومزودي الإنترنت ومختلف الخدمـــات الحكومية. وقد اســـتهدفت إحدى هذه الهجمات الشبكة الداخلية لمنظمة الاتحاد الإفريقي؛ كبرى المنظمات الإقليمية في القارة[١].

وخلال الســـنوات الثلاث الأخيرة، حوّل مجرمو الإنترنت والإرهابيون الســـيبرانيون بعض اهتمامهم بعيداً عن ســـرقة المعلومات الشـــخصية من خلال عمليات احتيال مســـتهدفة مثل التصيد الاحتيالي، وركزوا عملياتهم الإرهابية والإجرامية على مهاجمة الوكالات الحكوميـــة والبنية التحتية الحيوية وكذلك الشركات. فعلى سبيل المثال: تعرضت وكالة الطرق الحضريـــة الكينية لهجوم ببرنامـــج فدية في يوليو ٢٠٢٤م، ســـرق خلاله المهاجمون معلومات شخصية وســـجلات مالية. فيمـــا أدى هجوم علـــى المكتب الوطني للإحصـــاء النيجيري أواخر عام ٢٠٢٤م إلى إغلاق موقع الوكالة الإلكتروني لمدة ثلاثة أســـابيع، ودفعها إلى الاستثمار في تحسين الأمن السيبراني.

وفـــي العـــام ٢٠٢٤م، اختـــرق قراصنـــة نظام المختبـــرات الصحية الوطنية في جنـــوب إفريقيا، ممـــا أدى إلى تعطيل نظام الصحة العامة في البلاد، ووضعـــت وزارة الصحـــة بجنوب إفريقيـــا خططاً لتدريب موظفيها على تدابير الأمن الســـيبراني. كما كانت شـــركة الطاقة الجنوب إفريقية «إسكوم» هدفاً لهجمات إلكترونية متكررة أيضاً، إلى جانب شـــركة الكهرباء في جوهانسبرج[٢].

٣- توظيف الإرهابيين الفضاء السيبراني للتجنيد والدعاية:

يمكن النظـــر إلى الفضاء الســـيبراني باعتباره أداةً إستراتيجية للتجنيد والدعاية الإرهابية الرقمية فـــي إفريقيا، وذلك عبر توظيـــف منصات التواصل الاجتماعي، وتطبيقات المراســـلة، والفضاء الرقمي بشـــكلٍ عام، إذ تُســـتخدم تلك الوســـائط من قِبَل التنظيمات الإرهابية بشكلٍ متزايد للترويج الفكري، والتجنيد التنظيمي، ونشـــر الأيديولوجيا المتشددة، وتنظيم العمليات في إفريقيا. ومع هشاشـــة الرقابة الرقميـــة، وضعف الوعي المجتمعـــي بخطورة تلك الأدوات، يصبح اســـتغلال هذه القنوات وسيلةً فعّالة للتنظيمات الإرهابية العابرة للحدود في إفريقيا.

ووفقاً لمكتب الأمم المتحدة المعني بالمخدرات والجريمة؛ فإنه على مـــدى العقد الماضي، نجحت

(١) إفريقيا ومحلها في خارطة الأمـن السيبراني العالمي، الجزيرة، ٢٢ يوليو ٢٠٢٥، متاح على الرابط الآتي: https://www.ajnet.me/tech/2025/7/22/%D8%A7-

(٢) Cyberattacks Take Aim at Government, Infrastructure, Companies, ADF, August 26, 2025, accessible at: https://adf-magazine.com/2025/08/cyberattacks-take-aim-at-govern-/ment-infrastructure-companies

المنظمات الإرهابية بإفريقيا في التكيف والانتشار من خلال استغلال الثغرات الأمنية ونقاط الضعف. وقد سهّل التقدم في تكنولوجيا المعلومات والاتصالات، بالإضافة إلى التوسع في استخدام الأجهزة المحمولة، الوصول إلى الإنترنت وشبكات التواصل الاجتماعي. وقد جعل هذا الواقع الفضاء الإلكتروني أداةً شائعة للمنظمات الإرهابية لنشر دعايتها، وتطبيق إستراتيجيات التجنيد، وتمويل عملياتها، واستهداف أفراد محددين، وتوسيع أنشطتها[١].

وفي الحالة الإفريقية؛ تُستخدم المنصات الإلكترونية، مثل منصات التواصل الاجتماعي، بشكلٍ متزايد لنشر محتوى إرهابي لأغراض التجنيد والدعاية وتنسيق الأنشطة. إذ تؤكد منظمة «تكنولوجيا ضد الإرهاب» Tech Against Terrorism، وهي منظمة رائدة في مجال مكافحة النشاط الإرهابي عبر الإنترنت، أن حركة الشباب الصومالية التي تنشط في منطقة القرن الإفريقي، هي «أكبر منتج للمواد الإرهابية على الإنترنت»، وهي مسؤولة عن حوالي ٢٠-٢٥٪ من المحتوى الإرهابي على الإنترنت في إفريقيا[٢]. فيما تستخدم الجماعات الإرهابية، مثل حركة الشباب، وبوكو حرام، والجماعات التابعة لتنظيم «داعش»، وغيرها من الجماعات المتطرفة العنيفة، وسائل التواصل الاجتماعي بشكلٍ متزايد لأغراض مختلفة، في مقدمتها: إلهام وتجنيد المتابعين، وبث رسائل تؤكد قوتها وتهدف إلى ترهيب سلطات إنفاذ القانون في دول القارة[٣].

٤- استخدام الإرهابيين الفضاء السيبراني كوسيلة للتمويل:

بدلاً من الهجمات التقليدية فقط؛ تستخدم التنظيمات الإرهابية في إفريقيا الفضاء السيبراني لتنفيذ هجمات مالية تشمل: برامج الفدية، واختراق الحسابات البنكية، وابتزاز وسرقة البيانات، ما يوفر لتلك التنظيمات تدفقات مالية ضخمة يمكن توظيفها في تمويل ودعم الأنشطة الإرهابية العسكرية واللوجستية والدعائية والتجنيدية على حدٍّ سواء.

على الصعيد الإفريقي؛ لطالما اعتمد تنظيم القاعدة، على سبيل المثال، اعتماداً كبيراً على التبرعات، إذ تعتمد شبكته العالمية لجمع التبرعات على قاعدة من الجمعيات الخيرية والمنظمات غير الحكومية، والمؤسسات المالية الأخرى التي تستخدم مواقع إلكترونية وغرف دردشة ومنتديات على الإنترنت لجمع الأموال للتنظيم بطرقٍ ملتوية بعيداً عن رقابة الأجهزة المالية والأمنية بالدول الإفريقية[٤].

وفي أحدث حلقات توظيف الفضاء السيبراني لتمويل الإرهاب في إفريقيا، كشف الإنتربول، في ٢٢ أكتوبر ٢٠٢٥م، بالتعاون مع أفريبول، عن عملية كاتاليست Catalyst النوعية لتفكيك شبكات سيبرانية لتمويل الإرهاب، التي جرت وقائعها على

(١) Counterterrorism, UNODC, accessible at: https://www.un.org/en/unpdf/countering-use-of-internet-social-networks-for-terrorist-purposed-in-morocco

(٢) Harun Maruf, Inside Somalia's war on al-Shabab disinformation, VOA, 2024, March 21, accessible at: https://www.voanews.com/a/inside-somalia-s-war-on-al-shabab-disinformation/7528211.html

(٣) Brenda Mwale, The regulation of terrorist online content in Africa: an overview of the applicable regional instruments and the legal frameworks of South Africa, Kenya and Nigeria, JOURNAL OF POLICING, INTELLIGENCE AND COUNTER TERRORISM, 06 Apr 2025, accessible at: https://www.tandfonline.com/doi/epdf/10.1080/18335330.2025.2486659?needAccess=true

(٤) Gabriel Weimann, How Modern Terrorism Uses the Internet, UNITED STATES INSTITUTE OF PEACE, MARCH 2004, accessible at: https://www.usip.org/sites/default/files/sr116.pdf

مدار شهرين، وأسفرت عن اعتقال ٨٣ شخصاً في ٦ دول إفريقية، وتحديد هوية ١٦٠ شخصاً مشتبهاً بهم في عمليات تمويل مرتبطة بالإرهاب، وكشـفت عن حوالي ٢٦٠ مليون دولار أمريكي من العملات الورقية والافتراضية، يحتمل ارتباطها بأنشطة إرهابية. وقد تمت مصادرة حوالي ٦٠٠ ألف دولار أمريكي بالفعل، مع إجراء تحقيقات إضافية لتتبع واسـتعادة المزيد مـن الأصول في كلٍّ من: أنجـولا، ونيجيريا، وكينيا، وتنزانيا، والكاميرون[١].

٥- الاتجاه نحو شبكات الاتصالات البديلة والتحكم عن بعد:

أصبح نظـام الإنترنت عبر الأقمـار الصناعية Starlink، الذي ابتكـره الملياردير الأمريكي إيلون ماسـك، أداةً شائعة بشـكلٍ متزايد لدى الجماعات الإرهابية المسلحة للتواصل في المناطق التي تفتقر إلى البنية التحتية التقليدية للاتصالات الأرضية.

وفي الحالة الإفريقية؛ تزايد اسـتخدام الأقمار الصناعيـة، والشـبكات الافتراضيـة والمحمولة، لتنسيق العمليات الإرهابية بعيداً عن الرصد الأمني والاستخباراتي، من خلال استغلال شبكة Starlink، إذ أصبحت تقنيات الاتصـال عبر Starlink جزءاً متزايداً من الإستراتيجيات الاتصالية التي تستخدمها الجماعات الإرهابية والمتمردة في إفريقيا.

وعلى مدار العامين الماضيين، انتشـرت العديد من مقاطـع الفيديو والصور على وسـائل التواصل الاجتماعي، تُظهر الجماعات الإرهابية المسلحة في إفريقيا وهي تسـتخدم نظام الإنترنت عبر الأقمار الصناعية، فقد ظهر هذا الجهاز، الذي يمكن تمييزه من خلال طبق اسـتقبال أبيض مثبّـت على حامل ثلاثي القوائم، في يونيـو ٢٠٢٤م، في مقطع فيديو نشرته جماعة نصرة الإسـلام والمسلمين JNIM التابعـة لتنظيم القاعدة، خـلال عملية في منطقة جاو شـرق مالي ضد تنظيم «داعش» غرب إفريقيا ISWA[٢].

ويوفر ستارلينك للمستخدمين تغطية شبه كاملة للقارة الإفريقية، مقارنةً بما يزيد قليلاً عن ثلث تغطية تقنية الإنترنت الأرضية. وتتيح شـبكة سـتارلينك، التي تضـم آلاف الأقمـار الصناعيـة، للجماعات الإرهابية، من منطقة الساحل إلى بحيرة تشاد، نشر الدعاية وتنسـيق عملياتها. وتقلل الاتصالات الآمنة التي توفرها هذه التقنيـة من قدرة الحكومات على اعتراض اتصالات الإرهابيين، وحالياً تنشط أنظمة سـتارلينك في ٢٠ دولةً إفريقية من أصل ٥٤ دولة، وقد كشـفت الغارات التي شـنها الجيش النيجيري على جماعة بوكو حرام، خلال عام ٢٠٢٥م، عن تقنية الربـط الاتصالي الصاعد عبـر الأقمار الصناعية، مما يشـير إلى أن الجماعة الإرهابية تستخدم نظام سـتارلينك للتواصل مع العالـم الخارجي لمجابهة عمليـات الرصد والاختراق الأمني والاسـتخباراتي لتلك الاتصالات[٣].

ثالثاً: إستراتيجيات مكافحة الإرهاب السيبراني في إفريقيا:

مع تسـارع عمليات التحـول الرقمي في جميع أنحاء إفريقيا؛ أصبحت تحديات الأمن السـيبراني

(١) 83 arrests in landmark African operation against terrorism financing, INTERPOL, 22 October 2025, accessible at: https://www.interpol.int/News-and-Events/News/2025/83-arrests-in-landmark-African-operation-against-terrorism-financing

(٢) Célia Cuordifede, Starlink: The newest asset for rebel and jihadist groups in West Africa, Le Monde, July 5, 2025, accessible at: https://www.lemonde.fr/en/international/article/2025/07/05/starlink-the-newest-asset-for-rebel-and-jihadist-groups-in-west-africa_6743055_4.html

(٣) Starlink Becomes Communication Tool of Choice for Sahel Terrorists, ADF, August 12, 2025, accessible at: https://adf-magazine.com/2025/08/starlink-becomes-communication-tool-of-choice-for-sahel-terrorists/

أكثر إلحاحاً، ما جعل الحكومات الإفريقية تتجه نحو تبنّي إستراتيجيات للأمن السيبراني وقوانين للجرائم الإلكترونية تركز على قضايا مثل: بناء القدرات الفردية والمؤسسية ووضع أطر حوكمة شاملة. كما تتضمن بعض هذه الإستراتيجيات أهدافاً تتعلق بالسياسة الخارجية، بدءاً من تعزيز التعاون الدولي، ووصولاً إلى المشاركة في المنتديات الإقليمية والدولية ذات الصلة. ومع ذلك؛ يُعدّ الأمن السيبراني من بين التحديات الرقمية التي يتعين على الدول الإفريقية معالجتها، فمنذ عام ٢٠٢٠م، صُنّفت إفريقيا كأكثر المناطق تعرّضاً للهجمات الإلكترونية لكل دولة، وفقاً لمؤشر التعرض للأمن السيبراني[١] (Cybersecurity Exposure Index (CEI)، الأمر الذي يوجب على دول القارة الدفع باتجاه تبنّي المزيد من الإستراتيجيات الفعّالة لمجابهة تحديات الإرهاب السيبراني المتزايدة.

١- تزايد الإدراك إفريقي بمخاطر الإرهاب السيبراني:

أُولى خطوات بناء إستراتيجيات فعّالة لمجابهة التهديدات السيبرانية في إفريقيا بشكلٍ عام، والإرهاب السيبراني بشكلٍ خاص، هو إدراك الحكومات الإفريقية لما تعانيه سياساتها الأمنية السيبرانية من هشاشة وضعف.

وفي هذا الإطار؛ ثمة اعتراف إفريقي متزايد بمخاطر الإرهاب السيبراني، ومن ثَمّ بحاجة القارة لتدشين إستراتيجيات أمنية سيبرانية محكمة لمجابهة تهديدات الإرهاب في الفضاء الرقمي، وهو ما كشف عنه استطلاع الإنتربول الخاص لعام ٢٠٢٥م، حول مستويات المخاطر المتصوَّرة للجريمة السيبرانية عبر المناطق الفرعية في إفريقيا كما أبلغت عنها الدول الأعضاء في الإنتربول، وسبقت الإشارة إليه.

إذ أوضح ما يزيد عن ثلثي الدول الإفريقية الأعضاء في الإنتربول، ممن شملها الاستطلاع، أن الجرائم الإلكترونية والجرائم المرتبطة بها تُمثّل نسبةً تتراوح بين المتوسطة والعالية من إجمالي الجرائم، حيث مثلت الجرائم الإلكترونية أكثر من ٣٠٪ من إجمالي الجرائم المُبلّغ عنها في كلٍّ من غرب وشرق إفريقيا، مما يجعلها مصدر قلق كبير في هذه المناطق الفرعية[٢].

٢- تحسين البنية القانونية لمجابهة الإرهاب السيبراني:

مع إدراك الدول الإفريقية لارتفاع مستويات الإرهاب السيبراني؛ عمدت الكثير من تلك الدول إلى تحسين الأطر القانونية القوية والمتسقة مع المعايير الدولية؛ لمعالجة الأمن السيبراني وحماية البيانات من الاختراقات الإرهابية الإلكترونية. شملت تلك التحسينات: حماية البنى التحتية الرقمية، مكافحة التمويل الإرهابي الرقمي. فوفقاً للإنتربول؛ فقد أفاد نحو ٧٥٪ من الدول الإفريقية بأن أطرها القانونية أو قدراتها القضائية بحاجة لتحسين كبير، عبر تبنّي قوانين محدثة تجيز الحجز والتحليل الرقمي للأدلة، وتعمل على تعزيز حماية البنى التحتية الحيوية، ومعالجة التمويل السيبراني للإرهاب[٣].

ومن أمثلة ذلك: إستراتيجية كوت ديفوار للأمن السيبراني (٢٠٢١-٢٠٢٥م)، وخطة ناميبيا الوطنية للأمن السيبراني (٢٠٢٢-٢٠٢٧م)، وإقرار برلمان غانا قانون الأمن السيبراني عام ٢٠٢٠م، وإعلان السنغال أولوية إستراتيجيتها الوطنية لحماية الأمن السيبراني، ورؤية رواندا الإستراتيجية التي

(١) Cybersecurity Exposure Index (CEI) 2020, July 17, 2024.

(٢) INTERPOL AFRICA CYBERTHREAT ASSESSMENT REPORT 2025, INTERPOL, Op.Cit, pp.10-11.

(٣) Ibid.

تركز على الاستجابة للطوارئ الحاسوبية الإقليمية والدولية، وتعزيز التعاون في مكافحة الجرائم الإلكترونية، إضافةً إلى بناء شراكات مع المنظمات المعنية لتعزيز القدرات الوطنية في مجال الأمن السيبراني[١].

٣- تعزيز التعاون الخارجي لمكافحة الإرهاب السيبراني:

بالنظر إلى معاناة دول القارة الإفريقية من الطابع العابر للحدود للهجمات السيبرانية والإرهاب الرقمي؛ فقد اتجهت دول القارة إلى تعزيز التعاون الإقليمي والدولي المرن لمجابهة تلك التحديات، من خلال تضمين إستراتيجيات مكافحة الإرهاب السيبراني في القارة آليات لإنشاء شبكات تبادل المعلومات، وتنسيق تعاملات مع القطاع الخاص والشركاء الدوليين، وإبرام اتفاقيات ثنائية ومتعددة الأطراف في مجال الأمن السيبراني، ولاسيما أن نحو ٨٦٪ من الدول الإفريقية ترى أنها بحاجة لتحسين كبير في قدراتها على التعاون الدولي. ومن أمثلة آليات التعاون الإفريقية المهمة لمجابهة مخاطر الإرهاب السيبراني: مبادرة منصة التعاون ضمن Global Forum on Cyber Expertise GFCE ، التي تعمل على تجميع بيانات فنية وسياسات من الدول الإفريقية لتعزيز القدرات المشتركة، وبناء العلاقات وتعزيزها بين الجهات المعنية، بما يتيح لها تبادل المعلومات الإجمالية والمحددة حول تهديدات الإرهاب السيبراني، بما يُمكّن الحكومات والأطراف المهتمة الأخرى من توظيف تلك المعلومات لتحديد الثغرات، وتعزيز آليات الوقاية والاستجابة لمواجهة مجموعة متنوعة من التهديدات السيبرانية[٢].

ومن الفعاليات المهمة في هذا الإطار: إطلاق قوة شرق إفريقيا الاحتياطية EASF، في سبتمبر ٢٠٢٥م، ورشة عمل إقليمية حول التوعية بالأمن السيبراني والإرهاب السيبراني، بالتعاون مع الهيكل الإفريقي للسلام والأمن APSA، لجمع خبراء الأمن السيبراني والمؤثرين الرقميين وممثلي الشباب من جميع أنحاء شرق إفريقيا، للتباحث حول مواضيع رئيسية، من أبرزها: استخدام الجماعات الإرهابية لتكنولوجيا المعلومات والاتصالات، وتقنيات مكافحة الإرهاب، والتطرف الإلكتروني، والتحليل الجنائي الرقمي، والأطر القانونية والسياسية للأمن السيبراني، لتعزيز الاستجابة الواقعية للحوادث السيبرانية، والمشاركة الفعّالة، وتبادل المعرفة، والعمل على تحقيق نتائج عملية تعزز المرونة السيبرانية الإقليمية في إفريقيا[٣].

٤- بناء الوعي المجتمعي والمؤسسي بمخاطر الإرهاب السيبراني:

يمكن النظر إلى الوعي المجتمعي والمؤسسي إزاء المخاطر والتهديدات الأمنية السيبرانية؛ باعتباره ركيزةً وقائية لمجابهة الإرهاب السيبراني في إفريقيا، حيث كشفت دراسة بحثية إفريقية أن جماعات الإرهاب السيبراني تستفيد بشكلٍ كبير من ضعف الوعي التكنولوجي ونقص الثقافة الأمنية الرقمية لدى الجماهير والمؤسسات على حدٍّ سواء، لتنفيذ عملياتها التي تضر بالدول الإفريقية على كل المستويات؛ سياسياً، وأمنياً، واقتصادياً، واجتماعياً.

وفي السياق الإفريقي؛ أكدت الدراسة أن الوعي لدى الأفراد والمؤسسات بشأن مخاطر

---

(١) محمود سامح همام، الهجمات السيبرانية في إفريقيا.. قراءة في التحديات والاستجابات، السياسة الدولية، ٢٦ فبراير ٢٠٢٥م، متاح على الرابط الآتي: https://www.siyassa.org.eg/News/21972.aspx

(٢) Cybersecurity and Cybercrime Trends in Africa, The GFCE, November 2016, accessible at: CybersecuritytrendsreportAfrica-en-2.pdf

(٣) EASF Launches Cybersecurity and Cyber Terrorism Workshop in Kigali, Eastern Africa Standby Force, September 8, 2025, accessible at: EASF Launches Cybersecurity and Cyber Terrorism Workshop in Kigali

وتحديات وطرق مجابهة الإرهاب السيبراني لا يزال محدوداً بشكلٍ كبير، ما يجعل من الأهمية بمكان تضمين الإستراتيجيات الإفريقية لمكافحة الإرهاب السيبراني حملات توعية وطنية، وإدراج مناهج تعليمية للأمن السيبراني في المدارس والجامعات الإفريقية، مع تشجيع مشاركة القطاع الخاص والمجتمع المدني مع المؤسسات والجهات الحكومية، الأمنية والإدارية والمالية، في مبادرات الأمن الرقمي، مع تطوير منصات رقمية تُمكّن المستخدمين على اختلاف أنواعهم وخلفياتهم المهنية من الإبلاغ عن الحوادث والهجمات المحتملة، وتُعلّم أساسيات الأمن الإلكتروني، وتقديم الدول الإفريقية برامج تدريبية موجهة للشباب؛ بهدف تأهيلهم كمجندين رقميين للوقاية من توظيف الجماعات المتطرفة للفضاء الرقمي لشن هجمات إرهابية سيبرانية[1].

٥- توظيف الذكاء الاصطناعي لمكافحة الإرهاب السيبراني بإفريقيا:

أحدث الذكاء الاصطناعي تحولات جذرية في المجتمعات من خلال دفع عجلة الابتكار في مختلف القطاعات، بما في ذلك قطاع الأمن. فمع استخدام الذكاء الاصطناعي كوسيلة لتعزيز الابتكار في مجال الأمن؛ فإنه أصبح أداةً مهمة فيما يتعلق بمنع ومكافحة التطرف العنيف والإرهاب السيبراني، في ظل استغلاله من قِبَل الجماعات الإرهابية لأغراض خبيثة، بما في ذلك تعزيز القدرات السيبرانية، وتمكين الهجمات المادية، وتسهيل تمويل الإرهاب، ونشر الدعاية والمعلومات المضللة، وغيرها من التكتيكات العملياتية.

وفي إفريقيا؛ تتزايد المخاوف من تزايد إمكانية الوصول إلى أدوات الذكاء الاصطناعي التي تستخدمها الجماعات الإرهابية. ورغم محدودية البيانات حول استخدام الذكاء الاصطناعي من قِبَل هذه الجماعات في المنطقة؛ فإن الحالات الأخيرة، مثل تلك التي استخدم فيها تنظيم داعش في غرب إفريقيا ISWAP الذكاء الاصطناعي في «تحرير مقاطع الفيديو وتحرير الرسائل الإلكترونية المكتوبة»، تُظهر كيف تُستغل هذه التقنية.

في الوقت ذاته؛ يتيح هذا المشهد المتطور للتهديدات فرصةً لاستخدام أدوات الذكاء الاصطناعي لمكافحة الإرهاب في إفريقيا. ومع ذلك؛ فإن هذه الإمكانات محدودة بأطر مكافحة الإرهاب الحالية، والتي تفتقر إلى حدٍّ كبير للتجهيز لمواجهة المخاطر التي يشكلها استخدام الإرهابيين للذكاء الاصطناعي. في ظل هذه الخلفية؛ جاءت إستراتيجية الاتحاد الإفريقي القارية للذكاء الاصطناعي لعام ٢٠٢٤م- التي أقرها المجلس التنفيذي للاتحاد الإفريقي، الذي يضم ممثلين من جميع الدول الأعضاء في الاتحاد- لمجابهة المخاطر التي يشكلها الذكاء الاصطناعي على الأمن والسلم في القارة. إذ تركز تلك الإستراتيجية الحديثة بشكلٍ رئيسي على الابتكار، وحوكمة الذكاء الاصطناعي، وتعظيم فوائده في إفريقيا، كما أنها تضع الأمن السيبراني أيضاً كمجال ذي أولوية أمنية كبرى لحفظ الدول والمجتمعات الإفريقية من مخاطر الإرهاب.

في هذا الإطار؛ سلطت رئاسة مفوضية الاتحاد الإفريقي الضوء على إمكانات الذكاء الاصطناعي في إحداث ثورة في مكافحة الإرهاب، وأشارت إلى أن أدوات المراقبة المدعومة بالذكاء الاصطناعي يمكنها تتبع تحركات الإرهابيين، وتحليل المعاملات المالية المشبوهة، واكتشاف أنماط التطرف على منصات التواصل الاجتماعي. كما ألقت الضوء على إمكانات التحليل الجنائي القائم على الذكاء الاصطناعي في تعطيل العمليات المالية للإرهابيين، من خلال تحديد التدفقات النقدية غير المشروعة

(١) Moses Adah Agana, Bassey I.Ele, A Strategic Cyber Crime and Security Awareness Information System using a Dedicated Portal, arXiv, 3 Oct 2019, accessible at: IST-Africa Template

والسلوك المالي غير الطبيعي.

ويمكن لإمكانات الذكاء الاصطناعي في مكافحة الإرهاب في القارة الإفريقية أن تذهب إلى أبعد من ذلك، ففي تقرير مشترك؛ حدد معهد الأمم المتحدة لبحوث الجريمة والعدالة UNICRI، ومركز الأمم المتحدة لمكافحة الإرهاب UNCCT، عدة طرق تُستخدم فيها التكنولوجيا المدعومة بالذكاء الاصطناعي في مكافحة الإرهاب، بما في ذلك: التحليلات التنبؤية للأنشطة الإرهابية، وتحديد مؤشرات التطرف، والكشف عن المعلومات المضللة والمضللة التي ينشرها الإرهابيون لأغراض إستراتيجية، وإدارة المحتوى وإزالته آلياً، ومكافحة الخطابات الإرهابية والتطرف العنيف، وإدارة متطلبات تحليل البيانات الأمنية السيبرانية المكثفة[١].

رابعاً: مستقبل الأمن القومي الإفريقي في ضوء تهديدات الإرهاب السيبراني المتزايدة في القارة:

مع تزايد تهديدات الإرهاب السيبراني في قارة إفريقيا، وتفاوت الدول الإفريقية فيما يتعلق بإستراتيجيات المجابهة وتفعيل آليات مبادرات أمن التحول الرقمي، أصبحت القارة مرتعاً خصباً لمجرمي الإنترنت والإرهابيين السيبرانيين من ذوي التقنيات المتطورة. ومع توقع وصول عدد مستخدمي الإنترنت في إفريقيا إلى ١,١ مليار بحلول عام ٢٠٢٩م؛ فقد تزايدت أهمية مجابهة تهديدات الإرهاب السيبراني في إفريقيا أكثر من أي وقتٍ مضى[٢].

وللتخفيف من حدة التهديدات الإرهابية السيبرانية في المستقبل؛ من المتوقع أن تتجه الحكومات الإفريقية، بالشراكة مع الشركات التكنولوجية والمؤسسات الإقليمية والدولية المعنية، نحو «أتمتة» المهام المتعلقة بالأمن السيبراني التي كان يقوم بها المحللون البشريون تقليدياً، من قبيل: مراقبة الشبكات، وتحديد نقاط الضعف، والاستجابة للحوادث السيبرانية، من خلال استخدام البرامج والتقنيات المتقدمة للقيام بهدف زيادة الكفاءة، وتقليل حالات الخطأ البشري، وتسريع وتيرة الاستجابة. وصولاً إلى تبنّي أدوات أكثر تقدّماً يمكن من خلالها تحسين عملية التنبؤ بالتهديدات المحتملة، والتخفيف من حدتها قبل وقوعها. وتوفر هذه الأنظمة الآلية، المدعومة بخوارزميات التعلم الآلي، المراقبة المستمرة والتحليل الفوري الذي لا توفره الأنظمة اليدوية، مما يوفر للدول الإفريقية حمايةً مُحسّنة لبنيتها الرقمية بشكلٍ كبير من التهديدات السيبرانية، ويحمي الأصول الرقمية.

وفي هذا الإطار؛ ستتجه الحكومات الإفريقية إلى تفعيل أنظمة الذكاء الاصطناعي الأمنية بشكلٍ أكبر، لتراقب تلك الأنظمة المدعمة بالذكاء الاصطناعي الشبكات بحثاً عن التهديدات الإرهابية السيبرانية، وتعمل تلقائياً على حظر حركة البيانات المُريبة أو تعزل الأجهزة التي تُخالف السياسات أو تُظهر علاماتٍ على نشاطٍ ضار، وتجمع منصات أخرى وتحلل السجلات من أجهزة مختلفة، باستخدام حلولٍ آلية للكشف عن أي شذوذ. كما تعالج ميزات الأتمتة مهامّ الأمن المُتكررة، مثل تحليل رسائل البريد الإلكتروني المريبة. كما ترشد ميزات Chatbot الفرق في الاستجابة لسيناريوهاتٍ أمنية

(١) Brenda Mwale, AI and Counter-Terrorism in Africa: Assessing the Role of the African Union's Continental AI Strategy, The Global Network on Extremism and Technology (GNET), 26th June 2025, accessible at: AI and Counter-Terrorism in Africa: Assessing the Role of the African Union's Continental AI Strategy – GNET

(٢) Ignus De Villiers, The future of cyber security in Africa: Automating and predicting threats, Liquid Intelligent Technologies, October 24, 2024, accessible at: https://liquid.tech/the-future-of-/cyber-security-in-africa

معيّنة، وتُقيّم أدوات التعلم الآلي المخاطر وتقترح حلولاً للثغرات الأمنية[١].

إلى جانب ما سبق؛ من الضروري أن تنحى الدول الإفريقية مستقبلاً نحو اعتماد مبدأ «المرونة السيبرانية» Cyber Resilience كإطارٍ إستراتيجيي لمجابهة تهديدات الإرهاب السيبراني بالفضاء الرقمي، ويشير مفهوم «المرونة السيبرانية» إلى قدرة النظام التقني الرقمي على التعافي من الصدمة أو الهجوم أو الاختراق بطريقةٍ مثلى، سواءً في ذلك العودة إلى حالته الأصلية قبل الصدمة، أو خلق حالة معدلة جديدة أقل تأثّراً بتلك الصدمة وأكثر قدرةً على امتصاص تبعاتها وتأثيراتها الضارة.

وفي الواقع الإفريقي؛ فإنه من مقتضيات المرونة السيبرانية افتراض الحتمية، بمعنى التأكيد على أن الاضطرابات والمخاطر الإرهابية السيبرانية أمرٌ لا مفر منه، إذ أن الأمن السيبراني المطلق ربما يكون أمراً بعيد المنال في الواقع الراهن، حتى في أكثر النظم الرقمية تقدّماً. ومن ثَمّ فإنه من المرونة السيبرانية وجود ما يمكن وصفه بـ«الخطة ب» للتعافي في حالة حدوث خطأ ما. ويمكن تعزيز المرونة السيبرانية عن طريق تطوير وتأطير الحلول المستقبلية، وتعزيز الممارسات الفعّالة عبر النظم الرقمية[٢].

كما تتطلب إستراتيجيات المجابهة المستقبلية للإرهاب السيبراني، اللازمة لحفظ الأمن القومي لدول قارة إفريقيا، إدماج الأبعاد الخارجية في تلك المعادلة الأمنية، من خلال تسليط الضوء على تعزيز التعاون الإقليمي والدولي في مجالات سيبرانية أمنية أساسية، مثل التعاون بين فرق الاستجابة للطوارئ الحاسوبية CERTs، وتعزيز بناء القدرات وتبادل المعارف في مجال مكافحة الجرائم الإلكترونية، والتمسك بمعايير الأمن السيبراني الدولية، وتعزيز تطبيق القانون الدولي. كما يُعدّ تعزيز التعاون الإقليمي والدولي هدفاً مشتركاً للعديد من الإستراتيجيات، أو السياسات، أو القوانين النموذجية المتعلقة بالأمن السيبراني وحماية البنية التحتية الحيوية والجرائم الإلكترونية، التي اعتمدتها المجموعات الاقتصادية الإقليمية في قارة إفريقيا[٣].

ونظراً لأن المبادئ التوجيهية والسياسات والقواعد الموضوعة على المستوى الدولي لها آثارٌ على المستويين الوطني والإقليمي؛ فإنه من المهم على الصعيد الإفريقي ضمان صياغة هذه الأطر بطريقة تعكس أكبر قدرٍ ممكن من الحقائق الوطنية والإقليمية. علاوةً على ذلك؛ فإن المشاركة الفعّالة للجهات الإفريقية الفاعلة في السياسة الرقمية العالمية لا تقتصر على تعزيز مصالحها فحسب، بل تُعدّ أيضاً مفتاحاً لبناء مستقبل رقمي شامل وآمن ومستدام للبشرية.

ولتحقيق هذه الغاية؛ ينبغي أن تركز الإجراءات التي يُمكن للحكومات الإفريقية والمنظمات الإقليمية والقارية اتخاذها على عددٍ من المرتكزات؛ أبرزها: ضمان انعكاس الأولويات الرقمية بوضوح في السياسات الخارجية والعلاقات الدولية، مع إعطاء الأولوية للمشاركة في عمليات حوكمة رقمية دولية محددة تعكس الأولويات الوطنية والإقليمية والقارية، وتعزيز المشاركة في المؤتمرات الدولية ذات الصلة،

(١) Ibid.

(٢) Myriam-Dunn Caveltry, “Cyber-Security,” In Alan Collins (ed.), Contemporary Security Studies, 5th edition (Oxford: New York: Oxford University Press, 2019), pp.374-75.

(٣) Sorina Teleanu, Jovan Kurbalija, Stronger digital voices from Africa Building African digital foreign policy and diplomacy, DiploFoundation, November 2022, pp.10-11.

حيث تعالج العديد من قضايا السياسة الرقمية ذات الصلة بإفريقيا (مثل قضايا البنية التحتية في الاتحاد الدولي للاتصالات، وقضايا التجارة الإلكترونية في منظمة التجارة العالمية).

إضافةً إلى مواصلة إعطاء الأولوية للاعتبارات الاقتصادية والتنموية المتعلقة بالقضايا الرقمية- على الاعتبارات الجيوسياسية- في العلاقات الثنائية ومتعددة الأطراف، بما يتماشى مع الأولويات والمصالح الوطنية، وكذلك تعزيز النهج الشامل للحكومة والمجتمع في الحوكمة الرقمية والسياسة الخارجية الرقمية، وتعزيز المواقف المنسقة للدول الإفريقية في الحوكمة الرقمية الدولية، على سبيل المثال: من خلال الاتحاد الإفريقي أو المجموعات الاقتصادية الإقليمية، بجانب العمل على وضع مناهج طويلة الأجل لبناء القدرات الأكاديمية والبحثية والسياسات الرقمية للجيل القادم من الدبلوماسيين وصانعي السياسات الأفارقة[1].

خاتمة:

وختاماً؛ فإنه في ضوء التهديدات الإرهابية الراهنة والمتوقعة للأمن السيبراني الإفريقي، وانعكاساتها القائمة والمحتملة على الأمن القومي لدول القارة، فإن هناك ثلاثة سيناريوهات مستقبلية محتملة؛ تتمثل في: التحول الفردي المتقدم، والاستمرار الهش، و«أقلمة» الدفاع السيبراني الإفريقي.

فالأول: هو سيناريو تحوّلي منفرد خاص بكل دولة:

من خلال البناء المتقدم الذي تقوم من خلاله الدول الإفريقية بإسراع وتيرة بناء بنى تحتية رقمية قوية، تستوعب إستراتيجيات الأمن السيبراني، وتنشئ فرق استجابة قوية لمجابهة المخاطر، وتُوقّع اتفاقيات إقليمية لدعم تلك الإستراتيجيات بما يؤدي إلى تعزيز الأمن القومي لكل دولة، وجذب استثمارات رقمية، وهو ما يحقق في صورته الكلية بروز إفريقيا كمركز سيبراني آمن.

في حين أن الثاني: هو سيناريو الهشاشة واستمرارية التخلف:

في حال إذا بقيت الدول الإفريقية متأخرةً في القدرات التقنية والتعاون الخارجي، وهو ما يجعل دول القارة ساحةً لعمليات الإرهاب السيبراني الواسعة، ما يُضعف الاستقرار، ويقوّض الاقتصاد الرقمي ويعرّضه لأضرار ومخاطر كبرى، بما يلقي بظلاله السلبية على الأمن القومي لدول القارة بشكلٍ عام.

وأخيراً يأتي السيناريو الثالث: وهو السيناريو الجامع القائم على «أقلمة» الدفاع السيبراني الإفريقي:

وهو السيناريو الأكثر ترجيحاً، وفقاً للسياقات الأمنية الراهنة في القارة، والموجه نحو الأطر المؤسسية التكاملية بالقارة، لقيادة مشروع إستراتيجي إفريقي شامل موجه نحو التكتلات الإقليمية الشاملة والجزئية، وفي مقدمتها الاتحاد الإفريقي، والمجموعات الإقليمية مثل مجموعة تنمية الجنوب الإفريقي SADC، والمجموعة الاقتصادية لدول غرب إفريقيا ECOWAS، والجماعة الاقتصادية لشرق إفريقيا EAC، تضطلع ببناء إستراتيجيات أمنية سيبرانية إقليمية، مع تبادل البيانات وقيادة العمل المشترك، ما يخفف من حدة المخاطر الإرهابية السيبرانية على الدول الضعيفة في القارة، ويعزز من قدرات الأمن الإفريقي المجتمعي، ويدمج دول القارة في خط دفاعي وقائي موحد ومتكامل لمجابهة التهديدات الأمنية السيبرانية على كل المستويات ■

(١) Ibid, p.p. 12-13.