ورقة تحليلية

الأمن السيبراني في إفريقيا بين التحديات المحلية والرهانات الإستراتيجية

مصطفى جالي*

20 يوليو / تموز 2025

مركز الجزيرة للدراسات
ALJAZEERA CENTRE FOR STUDIES

Tel: +974-44663454
jcforstudies@aljazeera.net
studies.aljazeera.net

تشهد القارة الإفريقية تزايداً ملحوظًا في وتيرة وحجم التهديدات السيبرانية (ادوبي ستوك)

مقدمة

تشهد القارة الإفريقية تحولاً رقميًّا متسارعًا، رغم التحديات المستمرة المرتبطة بالبنية التحتية الرقمية من حيث التغطية والجودة وسهولة الوصول. فقد ارتفع عدد مستخدمي الإنترنت بشكل ملحوظ؛ إذ انضم أكثر من 160 مليون مستخدم جديد إلى الفضاء السيبراني بين عامي 2019 و2022 وفق معطيات الإنتربول. هذا التحول الرقمي ترك أثره العميق في مختلف القطاعات، من البنية التحتية الحيوية إلى الخدمات المصرفية والتجارة الإلكترونية، كما انعكس على الحياة اليومية للأفراد من خلال الانتشار الواسع للمدفوعات الرقمية والاستخدام المتزايد لمنصات التواصل الاجتماعي. وتُعد الهواتف المحمولة الوسيلة الرئيسية للولوج إلى الإنترنت في إفريقيا؛ إذ يستخدمها أكثر من 650 مليون شخص لهذا الغرض. ويبرز تأثير هذا التحول بشكل خاص لدى الشباب، الذين يشكّلون أكثر من 60% من سكان القارة؛ إذ يعتمدون على الإنترنت لأغراض متعددة تشمل العمل والتواصل والتسوق والتعبير عن الذات؛ ما يسهم في نشوء مجتمع شبابي متصل رقميًّا.

ومع هذا الانخراط المتزايد في العالم الرقمي، تتزايد في المقابل التحديات المرتبطة بالأمن السيبراني؛ إذ إن تنامي الاعتماد على التكنولوجيا وظهور ما يُعرف بـ"الجيل الرقمي" وسَّع من نطاق الهجمات السيبرانية التي تستغلها الجهات الإجرامية. وقدَّرت تقارير الإنتربول، في عام 2021، الخسائر المالية الناجمة عن الجرائم السيبرانية في إفريقيا بأكثر من

4 مليارات دولار أميركي، ما يعادل نحو 10% من الناتج المحلي الإجمالي للقارة. ومنذ ذلك الحين، تفاقمت التهديدات من حيث الحجم والتعقيد والتأثير.

أمام هذا الواقع، أصبحت معالجة ضعف الثقافة الرقمية، ومحدودية الاستعداد السيبراني، وغياب ممارسات الأمن الرقمي من الأولويات الملحَّة. وعلى الرغم من الجهود المبذولة من قبل الدول الإفريقية لتعزيز أمنها الرقمي، فإن الفضاء السيبراني لا يزال يمثل تهديدًا أمنيًّا حقيقيًّا، يفرض تحديات متعددة الأبعاد تتطلب استجابة شاملة، كما يضع القارة أمام رهانات على المستوى الدولي يجب كسبها من أجل حماية سيادتها الرقمية واستقرارها المستقبلي.

تطرح هذه الورقة تساؤلات متعددة تخص، أولاً، الاتجاهات الكبرى للتهديدات السيبرانية في القارة. ثانيًا: حجم ومظاهر الالتزام بالتدابير التي من شأنها تعزيز الأمن السيبراني لدى الدول. وثالثًا: التحديات التي تواجهها بغية تحقيق هذا المسعى. وأخيرًا، الرهانات الدولية المطروحة أمامها في هذا المجال.

موجة متصاعدة من التهديدات

تشهد القارة الإفريقية تزايدًا ملحوظًا في وتيرة وحجم التهديدات السيبرانية، مدفوعةً بضعف البنية التحتية الرقمية والتشريعات، واتساع رقعة المستخدمين للإنترنت. تتعدد أشكال هذه التهديدات من حيث الوسائل والدوافع والجهات الفاعلة؛ مما يجعلها أكثر تعقيدًا وأشدَّ خطورة. لذلك، من المهم تسليط الضوء على الأنماط الأساسية لهذه التهديدات مع تحليل أساليبها وتأثيرها.

خلال عام 2023، عرفت التهديدات السيبرانية في إفريقيا ديناميكية متسارعة؛ إذ تطورت الهجمات من حيث الحجم والتعقيد بشكل ملحوظ. واستنادًا إلى بيانات منظمة الإنتربول الإقليمية، تتمثل هذه التهديدات في الاتجاهات التالية(1):

أولاً: تصاعد مستمر في حجم وتأثير الجرائم السيبرانية عبر القارة

تشير الدول الأعضاء في الإنتربول إلى ارتفاع متواصل في عدد الهجمات السيبرانية على مستوى القارة الإفريقية. فأكثر من ثلثي الدول قيَّمت الجرائم السيبرانية -سواء تلك المعتمِدة كليًّا أو جزئيًّا على الفضاء السيبراني- على أنها تمثل مخاطر متوسطة إلى عالية ضمن نطاقها القضائي. كما لاحظت زيادة في الأثر المالي والاجتماعي لهذه الجرائم على المجتمعات والمؤسسات. وفي مؤشر آخر على نمو الجريمة السيبرانية، يُقدَّر أنه خلال عام 2023، شهدت إفريقيا زيادة

بنسبة 23% في متوسط عدد الهجمات الأسبوعية لكل مؤسسة مقارنة بالعام السابق، وقد كان أعلى معدل في العالم.

وتم تسليط الضوء على برامج الفدية باعتبارها واحدة من أخطر التهديدات الناشئة في القارة، وغالبًا ما تستهدف البنية التحتية الحيوية، بينما لا تزال عمليات الاحتيال عبر الإنترنت هي الشكل الرئيسي للجريمة الرقمية التي تؤثر على الأفراد والمؤسسات، من حيث الحجم والتأثير المالي.

ثانيًا: برمجيات الفدية والاحتيال الإلكتروني أبرز التهديدات المتنامية

لقد كانت التهديدات البارزة في تقارير الإنتربول تشمل:

- البرمجيات الخبيثة مثل برامج الفدية وأحصنة طروادة المصرفية وبرمجيات سرقة البيانات.
- هجمات التصيد والاحتيال الإلكتروني، لاسيما الاحتيال عبر البريد الإلكتروني للأعمال (BEC).
- خدمات الجريمة السيبرانية، بما في ذلك أدوات التجسس وبرامج التصيد الإلكتروني، وأشكال أخرى من الاحتيال عبر الإنترنت.

في عام 2023، تم تصنيف برمجيات الفدية كواحدة من أكثر التهديدات خطورة، نظرًا لاستهدافها البنى التحتية الحيوية في حين لا تزال الاحتيالات الإلكترونية هي الشكل الأكثر شيوعًا للجريمة السيبرانية سواء من حيث العدد أو الخسائر المالية.

واعتبرت البلدان الأعضاء في الإنتربول برامج الفدية والابتزاز الرقمي من أخطر التهديدات السيبرانية التي تواجهها القارة الإفريقية. وتثير هذه الهجمات قلقًا خاصًا نظرًا لتأثيرها المالي المرتفع، وقدرتها على تعطيل البنية التحتية الحيوية والخدمات الأساسية بشدة، والضرر الذي يمكن أن تسببه للمنظمات والأفراد المتضررين. تشير الأبحاث التي أجرتها شركة الأمن السيبراني Check Point إلى أنه في المتوسط، تعرضت 1 من كل 15 مؤسسة في إفريقيا لمحاولة برامج الفدية كل أسبوع خلال الربع الأول من عام 2023. هذا أعلى من المتوسط الأسبوعي العالمي، الذي بلغ حوالي 1 من كل 31 منظمة. كما يبدو أن التأثير المالي للهجمات آخذ في الازدياد أيضًا؛ فوفقًا لشركة IBM، بلغ متوسط تكلفة هجوم برامج الفدية في عام 2023 حوالي 5.13 ملايين دولار أميركي، بزيادة قدرها 13 في المئة عن عام 2022.

ثالثًا: استهداف البنية التحتية الحيوية الإفريقية

ومن المثير للقلق أن ما يقرب من نصف البلدان الإفريقية التي شملها الاستطلاع الذي قام به الإنتربول، أبلغت عن هجمات برامج الفدية ضد بنيتها التحتية الحيوية، بين يناير/كانون الثاني 2023 وديسمبر/كانون الأول 2023، التي تهدف إلى تعطيل أو تدمير أو تخريب هذه البنيات. ويشمل ذلك الهجمات التي تستهدف المؤسسات الحكومية والمستشفيات والمؤسسات المالية ومقدمي خدمات الإنترنت. على سبيل المثال، في السنوات الأخيرة، تعرضت أكبر شركة للكهرباء في غانا (ECG)، والبنوك الوطنية في زامبيا وجنوب السودان، والمؤسسات الحكومية في إثيوبيا والسنغال وزيمبابوي، ومزوِّد خدمة الإنترنت في جنوب إفريقيا لهجمات برامج الفدية. حتى الاتحاد الإفريقي واجه هجومًا معوقًا من مجموعة BlackCat (المعروفة أيضًا باسم ALPHV) ضد شبكتها الداخلية، في عام 2023. إلى جانب ذلك، أبلغت الدول الأعضاء أيضًا عن هجمات برامج الفدية عبر مختلف القطاعات. ووفقًا للبيانات المجمَّعة التي قدَّمها شركاء الإنتربول من القطاع الخاص، فإنه في حين أن قطاعات البنوك وتجارة التجزئة والتكنولوجيا والرعاية الصحية هي الأكثر استهدافًا على الصعيد العالمي، فإنه لا يوجد قطاع أو مؤسسة أو منظمة محصنة ضد هجمات برامج الفدية. إن استهداف البنية التحتية الحيوية أمر مثير للقلق بشكل خاص؛ إذ يستمر التحول الرقمي في التسارع في جميع أنحاء القارة وأصبحت الأنظمة الرقمية الأساسية متصلة بشكل متزايد.

رابعًا: تطور كبير في أساليب المهاجمين مع دمج التقنيات الجديدة

إلى جانب طريق العمل المتطورة، يمكن أن يعزى التأثير المتزايد لبرامج الفدية جزئيًّا إلى ظهور نماذج سيبرانية جديدة للجريمة المنظمة يستخدمها مجرمو الإنترنت. اكتشف الإنتربول وشركاؤه أن العديد من مجموعات برامج الفدية تدير الآن برامج تابعة مفصلة، تنطوي على تطوير منصات تقدم برامج الفدية خدمةً لمجرمي الأطراف الثالثة، والمعروفة باسم "affiliate programs"؛ حيث يمكن للشركات المتعاونة استخدام المنصات التي توفرها مجموعة برامج الفدية الأساسية لنشر البرامج الضارة، ونشر البيانات المسربة، وغسل عائدات جرائمهم. في مقابل استخدام النظام الأساسي، تدفع الشركات التابعة رسومًا لمجموعة برامج الفدية الأساسية، والتي يمكن أن تكون اشتراكًا شهريًّا أو نسبة مئوية من مدفوعات الفدية المستلمة من خلال النظام الأساسي. عندما تصبح أكثر نضجًا، تمكِّن عمليات برامج الفدية كخدمة مجرمي الإنترنت من تبسيط العمليات والارتقاء بأنشطتهم، كما أنها تسهم في ظهور متغيرات جديدة وأكثر تطورًا وعدوانية.

كما يواصل المهاجمون داخل القارة الإفريقية ومن خارجها استغلال الثغرات البشرية أساسًا لشنِّ هجماتهم؛ حيث لوحظ استخدام أساليب هندسة اجتماعية متطورة لاستهداف الأفراد والمؤسسات؛ مما يزيد من صعوبة اكتشاف الهجمات في مراحلها الأولى. لا يزال التصيد عبر البريد الإلكتروني من أكثر الوسائل شيوعًا لبدء الهجمات السيبرانية، مثل برمجيات الفدية والاحتيالات المختلفة. إلى جانب البريد الإلكتروني، بدأ المجرمون باستغلال قنوات اتصال جديدة، مثل وسائل التواصل الاجتماعي وتطبيقات المراسلة الفورية، بما يتماشى مع الاتجاهات التكنولوجية والاجتماعية في المنطقة. كما أن هناك اعتمادًا متزايدًا على التكنولوجيا الحديثة في تنفيذ الهجمات، مثل: سرقة البيانات كوسيلة للابتزاز، وسوء استخدام الذكاء الاصطناعي في عمليات التصيد، وتزوير المحتوى، والتضليل الرقمي.

على المستوى الجيوسياسي والعسكري، يلاحَظ بروز، أولاً، الهجمات برعاية الدول حيث قامت بعض الدول الأجنبية باستخدام الفضاء السيبراني للتجسس أو زرع الفوضى في دول إفريقية عبر أدوات متطورة جدًّا يصعب تتبع مصدرها، وقد تكون موجهة ضد خصوم جيوسياسيين أو لضمان النفوذ الاقتصادي. ثانيًا: الحروب السيبرانية الهجينة التي تستخدم فيها الهجمات الإلكترونية جزءًا من إستراتيجيات حرب غير تقليدية إلى جانب الحملات الإعلامية والدبلوماسية، كما في حالات الصراع على النفوذ بين الصين، والولايات المتحدة، وروسيا في إفريقيا. كما كان التأثير المباشر لانتشار الفضاء الرقمي في المجال العسكري هو إحداث تحول في وسائل العمل السري والضغط السياسي دون استخدام العنف. كما بدأت تقنيات المراقبة المحسَّنة والتكنولوجيات الناشئة مثل المسيرات تُحدث أثرًا ملموسًا في ساحات القتال الإفريقية(2).

والتالي، فإن هذه التهديدات لا تقتصر على الجانب التقني فحسب، بل تمتد آثارها إلى ما هو إستراتيجي يمس الأمن القومي، الاستقرار السياسي والاجتماعي، والنمو الاقتصادي للدول الإفريقية؛ حيث أصبحت تؤدي -على المستوى الاقتصادي- لخسائر مالية ضخمة نتيجة اختراق الأنظمة وسرقة البيانات، وتعطُّل عمليات التجارة والخدمات الرقمية، وتلحق أضرارًا مباشرة بالبنية التحتية الحيوية كالمطارات، والطاقة، والاتصالات. أما على المستوى الاجتماعي، فإنها تتسبب في تعطيل الخدمات العامة الأساسية مثل الصحة والتعليم، كما تسهم في فقدان الثقة العامة في الأنظمة الرقمية والمؤسسات الحكومية، بالإضافة لزيادة الفجوة الرقمية وتأثيرها على الفئات الضعيفة. أما على المستوى السياسي والحقوقي فإنها تؤدي لتدخلات سيبرانية في الانتخابات والعمليات الديمقراطية، واستغلال الفضاء السيبراني في نشر معلومات مضلِّلة وتقويض مؤسسات الدولة؛ مما يشكِّل تهديدًا لسيادة الدول واستقرارها الداخلي، من جهة. من جهة ثانية، فإنها تتسبب في انتهاكات واسعة لحقوق الخصوصية وحريات التعبير، علاوة على أن استخدام تقنيات المراقبة والاستهداف الرقمي يهدد الحقوق الأساسية للمواطنين(3).

مستويات متفاوتة من الالتزام

كشف المؤشر العالمي للأمن السيبراني (GCI) الصادر عن الاتحاد الدولي للاتصالات (ITU) لعام 2024(4)، أن أكثر من نصف الدول الإفريقية لا يزال أقل من المتوسط العالمي. هذا على الرغم من التقدم الكبير في تدابير وأنشطة الأمن السيبراني التي تقودها الحكومات في العديد من البلدان.

أولاً: على المستوى الوطني

وفقًا للمؤشر، فإن إفريقيا تتميز بمستويات متفاوتة من الالتزام بالأمن السيبراني، 7 دول إفريقية فقط -موريشيوس ومصر وتنزانيا وغانا وتونس ونيجيريا والمغرب- هي من بين أفضل 50 دولة لديها أعلى مؤشرات للأمن السيبراني. المغرب هو البلد الإفريقي الوحيد الذي وصل إلى قائمة أفضل 50 دولة في المؤشر الوطني للأمن السيبراني (أكتوبر/تشرين الأول 2022) -الذي يقيس استعداد البلدان لمنع التهديدات السيبرانية وإدارة الحوادث السيبرانية.

وقد قسَّم المؤشر الدول الإفريقية لأربعة أصناف:

(أدوار نموذجية): تقود سبع دول، تمثل 13%، عبر ثلاث مناطق (شمال وشرق وغرب إفريقيا) القارة في إظهار التزام قوي بالأمن السيبراني بالإجراءات المنسقة والمدفوعة من الحكومة عبر جميع الركائز الخمس وغالبية مؤشراتها. هذه البلدان هي المغرب ومصر وموريشيوس وغانا وتنزانيا وكينيا ورواندا.

(مستوى متقدم): تُظهر أربعة بلدان، هي زامبيا وبنين وتوغو وجنوب إفريقيا، تمثل 7.4%، مستويات متقدمة من الالتزام بالأمن السيبراني من خلال إظهار التزامات قوية بالإجراءات المنسقة والمدفوعة بالحكومة عبر غالبية الركائز.

(قيد التأسيس): 18 بلدًا، تمثل 33.3%، على مستوى التأسيس من جميع المناطق، من خلال إظهار التزام أساسي بالأمن السيبراني بالإجراءات التي تقودها الحكومة عبر عدد معتدل من الركائز أو المؤشرات. وتشمل هذه البلدان أوغندا وتونس ونيجيريا ومالاوي.

(في مرحلة التطور): 21 بلدًا، تمثل 38.9% في مرحلة التطور من جميع المناطق؛ مما يدل على التزام الأمن السيبراني الأساسي بالإجراءات التي تقودها الحكومة عبر ركيزة واحدة على الأقل، أو عدة مؤشرات فرعية، وتشمل هذه الرأس الأخضر وسيشل وتشاد والسودان.

(في المرحلة الأولى من البناء): أربعة بلدان، هي بوروندي وغينيا بيساو وجمهورية إفريقيا الوسطى وإريتريا، تمثل 7.4%، في المرحلة الأولى من تطوير الأمن السيبراني من خلال إظهار التزام الأمن السيبراني الأساسي بالإجراءات التي تقودها الحكومة عبر مؤشر أو مؤشر فرعي واحد على الأقل. وتحتل إريتريا أدنى مرتبة. ويمكن تفسير الترتيب في هذه الفئة بعوامل مثل محدودية إمكانية الوصول إلى البيانات ذات الصلة في حالة إريتريا أو أنها تشوبها حروب أهلية وعدم استقرار سياسي في حالتي جمهورية إفريقيا الوسطى وبوروندي(5).

منذ الإصدار السابق، شهدت إفريقيا تحولاً كبيرًا في التزام بالأمن السيبراني. في جميع أنحاء القارة، قطع العديد من البلدان خطوات كبيرة في تنفيذ تدابير ومبادرات الأمن السيبراني. على سبيل المثال، شهدت جمهورية الكونغو الديمقراطية وجنوب إفريقيا أكبر تحسينات في التدابير التنظيمية. أحرزت الغابون والرأس الأخضر وجزر القمر تقدمًا في التدابير القانونية. وعززت إثيوبيا تدابير التعاون التي تتبعها، بينما أحرزت توغو تقدمًا ملحوظًا في تدابير تنمية القدرات. كما تسجل إسواتيني وتوغو وجمهورية الكونغو الديمقراطية أعلى معدلات النمو في القارة.

أما البلدان التي تظهر أهم التحسينات في المستويين، التأسيسي والتطوري، تشمل مالاوي وإسواتيني وإثيوبيا وليبيا وموزمبيق والجزائر وغامبيا والجمهورية الديمقراطية الكونغو وسيراليون وغينيا وتوغو. حيث حققت نسبة عالية من التقدم من أصحاب الفئة الثالثة الحاليين (أكثر من 70%) منذ التقرير السابق. تشمل البلدان الجزائر وجمهورية ألمانيا الديمقراطية الكونغو وإسواتيني وإثيوبيا. أما البلدان التي أحرزت تقدمًا ضئيلاً أو لم تحرز أي تقدم أو ظلت منخفضة الأداء منذ عام 2021 فتشمل زيمبابوي وتشاد والسودان وساوتومي وبرينسيبي وجمهورية إفريقيا الوسطى وإريتريا. كما شهد العديد من البلدان تدهورًا طفيفًا في درجاتها، وهي تونس وغينيا بيساو ونيجيريا. وعلى الرغم من أن بعض التقدم يمكن تفسيره بالتغيير في المنهجية التي اعتمدها التقرير، إلا أن جزءًا كبيرًا من التقدم الذي أحرزه كل بلد يمكن إرجاعه إلى التدابير والتدخلات المنسقة التي تبذلها الحكومات الوطنية لتحسين القدرات الوطنية للأمن السيبراني(6).

ثانيًا: على المستوى الإقليمي والقاري

تكشف التوقعات الإقليمية للأمن السيبراني عن مستويات متنوعة من تطوير الأمن السيبراني عبر مناطق إفريقية مختلفة. ويتصدر شمال إفريقيا الالتزام بالأمن السيبراني، بينما تتخلف إفريقيا الوسطى عن جميع المناطق الأخرى. والجدير بالذكر أن أنماطًا مماثلة من أنشطة الأمن السيبراني التي تقودها الحكومات واضحة في شرق وجنوب وغرب إفريقيا. وتسلط البيانات الإقليمية الضوء على أنه على الرغم من وجود ثغرات في جميع ركائز الأمن السيبراني، فإن

التدابير التقنية وتدابير تنمية القدرات تتطلب مزيدًا من الأولوية. يمكن أن يؤدي تعزيز التعاون وتبادل أفضل الممارسات داخل المناطق وعبرها إلى رفع تحديات الأمن السيبراني الوطنية والإقليمية في جميع أنحاء القارة(7).

من جهة أخرى، يتميز الأمن السيبراني باعتباره برنامجًا رائدًا في إطار أجندة الاتحاد الإفريقي لعام 2063، باعتباره "مؤشرًا واضحًا على أن إفريقيا بحاجة ليس فقط إلى تضمين التغيرات السريعة التي أحدثتها التقنيات الناشئة في خططها التنموية، ولكن أيضًا لضمان استخدام هذه التقنيات لصالح الأفراد أو المؤسسات أو الدول القومية الإفريقية من خلال ضمان حماية البيانات وسلامتها عبر الإنترنت"(8).

كما يحظى الأمن السيبراني والجرائم الإلكترونية بمكانة بارزة في إستراتيجية التحول الرقمي للاتحاد الإفريقي، والتي تتضمن العديد من توصيات السياسات والإجراءات المقترحة في هذين المجالين. في حين أن معظمها مرتبط بتعزيز الأمن السيبراني على المستويين الوطني والقاري، إلا أن هناك أيضًا بعض العناصر المتعلقة بالعمليات الدولية. تتمثل إحدى التوصيات في أن يقوم الاتحاد الإفريقي ودوله الأعضاء "بدعم العملية التي تقودها الأمم المتحدة لإنشاء الإطار العالمي للأمن السيبراني في إطار الأمم المتحدة"(9). وفي عام 2018، قرر الاتحاد الإفريقي إنشاء مجموعة خبراء الأمن السيبراني (AUCSEG) مكلفة بتقديم المشورة للمفوضية وصانعي السياسات بشأن القضايا المتعلقة بالأمن السيبراني. ومن المتوقع أيضًا أن تدعم المجموعة، التي بدأت العمل في عام 2019، مفوضية الاتحاد الإفريقي والدول الأعضاء في مسائل التعاون الدولي فيما يتعلق بالأمن السيبراني وحماية البيانات الشخصية ومكافحة الجرائم الإلكترونية(10).

في صميم مبادرات الاتحاد الإفريقي للأمن السيبراني تكمن اتفاقية الأمن السيبراني وحماية البيانات الشخصية لعام 2014 (اتفاقية مالابو)، وتغطي هذه الاتفاقية أكثر من الأمن السيبراني والجرائم السيبرانية وتتضمن أحكامًا بشأن المعاملات الإلكترونية وحماية البيانات الشخصية. كل هذا يعطي الاتفاقية طابعًا فريدًا ومبتكرًا بين اللوائح والسياسات المتعلقة بالأمن السيبراني، كما تتضمن الاتفاقية عدة أحكام تتعلق بالتعاون الدولي. وتشجع الدول الأطراف على إبرام اتفاقات بشأن المساعدة القانونية المتبادلة في التصدي للجرائم السيبرانية وتمكين تبادل المعلومات بشأن التهديدات السيبرانية وتقييمات الضعف من خلال مؤسسات مثل مراكز الاستجابة لطوارئ الحاسوب الآلي. كما أن البلدان مكلفة باستخدام آليات التعاون الدولي -سواء كانت قائمة على شراكات خاصة أو عامة- عندما يتعلق الأمر بالاستجابة للتهديدات السيبرانية، وتحسين الأمن السيبراني، وتحفيز الحوار بين أصحاب المصلحة المتعددين(11)، غير أنها لم تدخل حيز التنفيذ إلا في الثامن من يونيو/حزيران من عام 2023، أي بعد 8 سنوات من خروجها لحيز الوجود؛ إذ وقَّعت عليها 15 دولة من أعضاء الاتحاد الإفريقي الـ15 وهو العدد المطلوب لدخول الاتفاقية حيز النفاذ(12).

من جهة أخرى، يوجد هناك تداخل في العضوية بين اتفاقيتي مالابو وبودابست. اتفاقية بودابست هي اتفاقية بشأن الجرائم السيبرانية لمجلس أوروبا، وتركز على تعريف الجريمة السيبرانية والأحكام القانونية ذات الصلة والتعاون عبر الحدود. واثنا عشر بلدًا إفريقيًّا أطرافًا أو موقِّعة أو تمت دعوتها للانضمام إلى الاتفاقية، هي: الرأس الأخضر والسنغال وغانا وموريشيوس والمغرب ونيجيريا أطراف في الاتفاقية. ووقَّعت جنوب إفريقيا على الاتفاقية، بينما دُعيت بنين وبوركينا فاسو وتونس وكوت ديفوار والنيجر إلى الانضمام إليها. من بين هذه البلدان، وقَّعت أو صدَّقت الرأس الأخضر وغانا وموريشيوس والسنغال على اتفاقيتي مالابو وبودابست.

في أغسطس/آب 2022، أعلنت اللجنة الاقتصادية لإفريقيا التابعة للأمم المتحدة وجمهورية توغو عن اتفاقية لإنشاء المركز الإفريقي للتنسيق والبحوث في مجال الأمن السيبراني بشكل مشترك. ويهدف المركز، الذي سيكون مقره في لومي، لأن يصبح مركزًا إقليميًّا للمعلومات والاستخبارات المتعلقة بالأمن السيبراني، وأن يسهم في بناء القدرات والأطر على المستويين، الوطني والإقليمي، لتقييم التهديدات السيبرانية والتخفيف من حدتها. كما يعالج مجلس السلم والأمن التابع للاتحاد الإفريقي قضايا الأمن السيبراني. على سبيل المثال، في مايو/أيار 2019، في اجتماع حول التخفيف من تهديدات الأمن السيبراني للسلام والأمن في إفريقيا، شجَّع المجلس الدول الأعضاء على "تعزيز التنسيق الوطني والإقليمي والقاري، من بين أمور أخرى، من خلال تنسيق وتحديث إستراتيجيات الأمن السيبراني الوطنية واستجابات وسياسات الطوارئ للأمن السيبراني". وفي أغسطس/آب 2022، في اجتماع حول التقنيات الناشئة ووسائل الإعلام الجديدة، أشار المجلس إلى أهمية قيام "مفوضية الاتحاد الإفريقي والدول الأعضاء بتطوير نهج إستراتيجي لتنفيذ معايير الأمم المتحدة بشأن السلوك المسؤول للدول في الفضاء السيبراني على المستويين الإقليمي والقاري"(13).

كما شرعت المجموعات الاقتصادية الإقليمية أيضًا في تنفيذ سياسات وبرامج مختلفة تتعلق بالأمن السيبراني. في عام 2021، اعتمدت الجماعة الاقتصادية لدول غرب إفريقيا (ECOWAS) إستراتيجيتها الإقليمية للأمن السيبراني والجرائم السيبرانية، والتي تحدد الإجراءات التي يجب اتخاذها على المستوى الوطني على وجه الخصوص لتعزيز الأمن السيبراني ومكافحة الجريمة السيبرانية. كما وضعت السوق المشتركة لشرق وجنوب إفريقيا (COMESA) مشروع قانون نموذجي للجريمة السيبرانية (2011)، بالإضافة إلى سياسة نموذجية، وخارطة طريق للتنفيذ في مجال الأمن السيبراني. كما أن الجماعة الاقتصادية لدول وسط إفريقيا (ECCAS) لديها قانون نموذجي بشأن الأمن السيبراني، في حين وضعت مجموعة تنمية إفريقيا الجنوبية (SADC) قانونًا نموذجيًّا بشأن جرائم الحاسوب والجريمة السيبرانية (2012). كما تتعدد الأطر الإقليمية الإفريقية المعنية بالأمن السيبراني، وتشمل: منتدىAfricaCERT الذي يهدف إلى تعزيز الجاهزية السيبرانية ومرونة البنى التحتية الرقمية عبر التعاون الإقليمي والدولي، ويضم 26 دولة إفريقية؛

وآليةAFRIPOL التابعة للاتحاد الإفريقي، التي تسعى إلى تطوير نهج موحد لمكافحة الجرائم الإلكترونية من خلال إستراتيجية 2020-2024 التي تركز على بناء القدرات، وتوحيد التشريعات، وتقييم التهديدات، والتعاون مع كيانات دولية كالاتحاد الدولي للاتصالات وهيئة ICANN والإنتربول. كما تلعب مؤسسة بناء القدرات الإفريقية (ACBF) دورًا في تنمية المهارات والسياسات السيبرانية؛ بالإضافة إلى دور منظمات المجتمع المدني في رفع الوعي وبناء القدرات في قضايا مثل الجريمة السيبرانية وحماية الأطفال عبر الإنترنت(14).

تحديات مركبة

على مدى السنوات الماضية، اعتمد أكثر من اثنتي عشرة دولة إفريقية أو شارك في عملية اعتماد تشريعات جديدة تتعلق بالجرائم السيبرانية. ويمثل ذلك خطوة استباقية نحو تعزيز الأطر القانونية لمكافحة الجرائم الإلكترونية. كما حدث أيضًا نمو كبير في الاستثمار في مكافحة الجريمة السيبرانية في القارة، بما في ذلك من البلدان الإفريقية الأعضاء وأصحاب المصلحة خارج المنطقة. وفي عام 2023، أنشأ المزيد من البلدان وحدات مخصصة للجرائم الإلكترونية، وزاد ما يقرب من النصف من مستويات التوظيف، وأفاد أكثر من 60% بمشاركتها في مبادرات بناء القدرات. وعلاوة على ذلك، هناك أكثر من 130 مبادرة تدريبية، فضلاً عن أكثر من 40 حملة توعية عامة في القارة(15).

على الرغم من هذه الخطوات المهمة، لا تزال البلدان الإفريقية تواجه تحديات مستمرة في مجال الأمن السيبراني، لاسيما في ظل الثورة التي يشهدها ميدان الذكاء الاصطناعي، يمكن إيجاز أبرزها في:

تحديات ثقافية

لا يزال الوعي بالأمن السيبراني نقطة ضعف؛ إذ يقلِّل العديد من المؤسسات والشركات والأفراد من المخاطر المرتبطة بالأمن السيبراني؛ مما يجعلهم أكثر عرضة للوقوع في فخاخ مثل التصيد الاحتيالي أو عمليات الاحتيال عبر الإنترنت.

كما تسود الفكرة القائلة بأن الأمن السيبراني والذكاء الاصطناعي يؤثران فقط على الشركات متعددة الجنسيات في الشمال أو الشركات الكبيرة، لكن في الحقيقة فهي تتعلق بأي منظمة سواء عامة أو خاصة، وبشكل أعم المجتمع ككل. وفقًا للجنة الاقتصادية الإفريقية التابعة للأمم المتحدة، فإن المستوى المنخفض للتأهب للأمن السيبراني في القارة يكلف الدول ما معدله 10% من ناتجها المحلي الإجمالي؛ إذ تخسر القارة ما يقرب من 4 مليارات دولار كل عام بسبب الجرائم الإلكترونية وحدها، وما تشكِّله من مخاطر كبيرة للمؤسسات من الخسائر المالية، وتسرب البيانات

الحساسة، والسمعة وفقدان الميزة التنافسية، بالإضافة لاستخدام الفضاء الرقمي والذكاء الاصطناعي لنشر الشائعات والمحتوى الزائف والمضلل؛ مما يؤدي إلى زعزعة الاستقرار السياسي والمجتمعي(16).

الأمن السيبراني ليس بعدُ من الأولويات

يلاحَظ غياب الأمن السيبراني عن السياسات العامة الشاملة حيث لا يُنْظَر إليه كأولوية إستراتيجية في خطط التنمية الوطنية، كما أن الشركات لا تدمجه بعمق في إستراتيجياتها. يجب أن يكون الأمن السيبراني في صميم إستراتيجية المؤسسات والشركات. تتمثل مسؤولية الحكومات في تنفيذ إستراتيجيات متماسكة وشاملة وطويلة الأجل. على مستوى اللاعبين الاقتصاديين، يجب أن يصبح الأمن السيبراني مجالاً دائمًا للاهتمام، وهو ما لا يحدث حاليًّا. وفقًا لاستطلاع أجرته شركة PricewaterhouseCoopers، عام 2021، بين ما يقرب من 300 فاعل في مختلف القطاعات في إفريقيا الناطقة بالفرنسية، فإن أكثر من نصف الشركات التي تمت استشارتها تدرك أهمية الأمن السيبراني، ولكنه لا يحظى لديها بالأولوية، على المستوى المؤسسي. وعدَّ أقل من ثلث الجهات الفاعلة التي شملها الاستطلاع أن الأمن السيبراني موضوع ذي أولوية(17).

نقص الكفاءات والمهارات

يعاني أغلب الدول الإفريقية من نقص كبير في خبراء الأمن السيبراني، وضعف برامج التدريب والتأهيل التكنولوجي، بالإضافة أنه لم يتم بعد دمج الأمن السيبراني والذكاء الاصطناعي في المناهج الدراسية بالشكل الكافي. يحد هذا النقص من قدرة الشركات والمؤسسات على تأمين أنظمتها بشكل فعَّال.

على الرغم من الجهود المبذولة للاستثمار في الموظفين والمهارات من أجل مكافحة التهديدات السيبرانية بشكل أفضل، بما يؤكد التزام الدول الإفريقية الأعضاء بتعزيز المرونة السيبرانية في جميع أنحاء القارة. فعلى سبيل المثال، أبلغ ما يقرب من نصف أجهزة إنفاذ القانون في البلدان الأعضاء في الإنتربول، في عام 2023، عن زيادة في عدد الموظفين المكلفين بمكافحة الجريمة السيبرانية. وبالإضافة إلى ذلك، سلَّطت أربعة بلدان على الأقل الضوء على أنها أنشأت مؤخرًا وحدة للجرائم السيبرانية أو أنها بصدد القيام بذلك. إلا أن الإنتربول لا يزال يعتبر أن الموارد البشرية المخصصة لمكافحة الجريمة السيبرانية في القارة لا تزال غير كافية، على الرغم من أن البلدان تتخذ خطوات استباقية لتحسين الحالة(18).

من ناحية أخرى، رغم سَنِّ العديد من القوانين الجديدة، إلا أن التطبيق لا يزال ضعيفًا في كثير من الدول، ويتمثل ذلك في نقص القدرات في إنفاذ القانون؛ إذ إن العدد الضئيل من الموظفين والموارد المخصصة للجرائم السيبرانية يحول دون تحقيق ذلك؛ حيث تعد الأطر التشريعية الفعالة معيارًا رئيسيًّا لأنشطة إنفاذ القانون ومكوِّنًا أساسيًّا لتحقيق الأمن السيبراني، كما تسهم في تعزيز قدرات قوات الشرطة ومهاراتها التشغيلية من خلال تحسين كفاءتهم في التحقيق في الجرائم السيبرانية وتعزيز التعاون الدولي.

تحديات مالية

كل من الحكومات والشركات ما زالت لا تستثمر بشكل كافٍ في الأمن السيبراني، وخاصة الشركات الصغيرة والمتوسطة، التي لا توفر الموارد اللازمة للاستثمار في حلول الأمن السيبراني القوية. إن نقص الإنفاق المخصص لأمن تكنولوجيا المعلومات يجعل هذه الكيانات عرضة للهجمات باستمرار. على سبيل المثال، ينفق ثلثا الشركات الإفريقية الكبيرة، التي شملها أحد الاستطلاعات، أقل من 20 ألف يورو سنويًّا على هذا المجال(19). كما أن غياب الحوافز لتعزيز الابتكار المحلي لحلول تتناسب مع التحديات الإفريقية، وضعف الاستثمار في البحث والابتكار في التكنولوجيا الرقمية المحلية، يعوق الابتكار وبناء شركات ناشئة قوية. بالتالي، هناك المزيد مما يتعين القيام به، سواء في الشركات أو في المؤسسات العامة. لذلك من الضروري زيادة الوعي حول أهمية الأمن السيبراني وتشجيعها على زيادة الاستثمار في هذا المجال، الشيء نفسه ينطبق على الذكاء الاصطناعي.

غياب التنسيق والجهود المشتركة

على المستوى القاري، يوجد تباين كبير في التشريعات بين الدول مما ينتج عنه قصور في التعاون الأمني والمعلوماتي في مجال تبادل المعلومات والتنسيق بين أجهزة الأمن والشرطة في مختلف الدول. هذا بالإضافة لتأخر انضمام بعض الدول إلى الاتفاقيات الدولية والإقليمية ذات الصلة مثل اتفاقية بودابست ومالابو؛ إذ يمثل الوضع العام فرصة كبيرة للقارة لتسخير فرص التعاون متعدد الأطراف في مجال الأمن السيبراني بشكل أفضل[20]. في حين أن الاتفاقية القارية مهمة بالنظر إلى نطاقها، فإن هذا الافتقار إلى التصديق ينتقص من أثرها المحتمل. يمكن تفسير هذه الوتيرة البطيئة للتصديق بأسباب متعددة: من الأسباب السياسية (المتجذرة في التنوع السياسي والثقافي والتاريخي للمنطقة)، إلى العمليات المطولة داخل البلدان، والوعي المحدود بين صانعي السياسات بأهمية الأمن السيبراني وأهميته للأمن القومي، والقدرة المحدودة داخل البلدان على تولي واختتام العمليات اللازمة(20).

من جهة ثانية، هناك تحديات تواجه إقامة شراكات ومنصات رسمية بين القطاعين العام والخاص لمساعدة الشركات في مكافحة الجريمة السيبرانية. يعد إنشاء وتعزيز الشراكات المفتوحة والشاملة أمرًا أساسيًّا لتعزيز التعاون الفعال في مكافحة الجريمة الإلكترونية. ومع ذلك، أبلغت البلدان الإفريقية الأعضاء عن وجود صعوبات في تعزيز التعاون بين أجهزة إنفاذ القانون وأصحاب المصلحة المعنيين في منظومة الأمن السيبراني لاسيما فيما يخص التحقيقات في الجرائم الإلكترونية(22).

لقد أصبح من الأهمية بمكان تعزيز التعاون الإقليمي فيما بين البلدان الإفريقية لمواءمة الأطر التنظيمية وتبادل أفضل الممارسات. سيؤدي ذلك بشكل جماعي إلى تعزيز قدرة إفريقيا على مواجهة التهديدات السيبرانية وتطوير الذكاء الاصطناعي الذي يتناغم حقًّا مع إفريقيا. ويمكن أن تشمل هذه المبادرة اعتماد معايير مشتركة، وتيسير التعاون وتبادل المعلومات فيما بين البلدان الإفريقية، فضلاً عن برامج بناء القدرات(23).

بالتالي، فإن الأمن السيبراني في إفريقيا يواجه تحديات مركبة تشمل الأبعاد البشرية والمؤسساتية، والمالية والتقنية، والتشريعية والسياسية. معالجة هذه التحديات تتطلب إرادة سياسية واضحة، واستثمارات مالية، وتعاونًا إقليميًّا، وبناء قدرات بشرية قوية.

رهانات إستراتيجية

تشمل الرهانات المطروحة أمام البلدان الإفريقية عدة مستويات إستراتيجية وسياسية وتقنية وتنموية، وترتكز على تحقيق التوازن بين الدفاع عن السيادة الرقمية وسط التدخلات الخارجية والمنافسة الجيوسياسية العالمية، والمساهمة في صنع القواعد ذات الصلة بالأمن السيبراني على المستوى الدولي.

أولاً: مواجهة الدعاية التي تقودها الجهات الخارجية

لقد أسهم التدافع الدولي الذي تشهده إفريقيا في السنوات الأخيرة، في تصاعد الدعاية الرقمية والتلاعب بالمعلومات بشكل خطير. التضليل الإعلامي في إفريقيا ليس جديداً، فوسائل الإعلام التي تسيطر عليها الدولة تمارس البروباغاندا وتشوه المعارضة وتتجاهل مصالح الأحزاب والجهات التي لا تتماشى مع مواقفها. الجديد هو الانتشار الواسع النطاق للمعلومات المضللة من قبل الجهات الفاعلة الخارجية. الهدف هو التأثير على الجمهور ونتائج الانتخابات والسياسات الحكومية بهدف تحقيق مصالح بعينها كالحصول على حقوق استغلال موارد الطاقة والمعادن أو عقود البناء لشركات

عامة أو خاصة دون امتثال للقوانين المعمول بها، أو تهدف إلى توقيع صفقات عسكرية غير شفافة ومبيعات الأسلحة، وتسهيل الوصول إلى الموانئ والأراضي الزراعية الغنية وغيرها.

كانت روسيا أول من تبنَّى إستراتيجية الهندسة الاجتماعية هذه، على مدى السنوات الماضية، قامت Meta الشركة الأم لفيسبوك، بتفكيك العديد من الشبكات الموالية لروسيا التي روَّجت للأحزاب الحاكمة المتحالفة وغذَّت القومية المتطرفة في ثماني دول إفريقية على الأقل. تؤثر هذه التلاعبات واسعة النطاق على ملايين المستخدمين من بين السكان المستهدفين لاسيما من خلال وسائل التواصل الاجتماعي. يعد إنتاج وتنسيق الدعاية الرقمية جزءًا أساسيًّا مما يسميه الخبراء "برنامج بقاء النظام" الذي تقدمه موسكو للأنظمة الاستبدادية الهشة في إفريقيا، مثل بوركينا فاسو وجمهورية إفريقيا الوسطى ومالي والسودان. وبالإضافة إلى ذلك، هناك دعم للمرتزقة، وتمويل الحملات الانتخابية، والغطاء السياسي في المحافل الدولية، والمساعدة في استغلال الموارد المدرَّة للربح. بفضل استخدام إستراتيجية بارعة، تمر تعاملات روسيا دون أن يلاحظها أحد؛ إذ لا يدير الكرملين ما يسمى "الذباب الإلكتروني"، لكنه يدفع للسكان المحليين والمؤثرين مقابل إنشاء محتوى مضلل على منصات الفيسبوك، وإكس (تويتر سابقًا)، وواتساب، وإنستغرام، بما يجعل الرسائل تبدو صادقة ويصعب على السلطات والمستخدمين اكتشافها. فبعد بضعة أشهر من الغزو الروسي لأوكرانيا، في فبراير/شباط 2022، مثلاً، حدَّد اتحاد التحقيقات للمجتمع المدني "Code for Africa" ما لا يقل عن 175 صفحة على الفيسبوك في 21 دولة إفريقية، وهي مسؤولة عن ارتفاع المحتوى الموالي لروسيا في القارة. كانت الأخبار المزيفة تهدف إلى إقناع الأفارقة بأن الغرب دبَّر هذه الحرب بالوكالة(24).

على الجانب الآخر، قامت بكين بتضخيم روايات الحزب الشيوعي الصيني من خلال وسائل الإعلام الذي تملكها الدولة مثل "سي جي تي أن" (CGTN) و"تشاينا ديلي" (China Daily)، و"شينخوا" (Xinhua) التي لديها مكاتب في إفريقيا؛ إذ ينشرون على نطاق واسع خطاب الجبهة المتحدة في الحزب الشيوعي الصيني، وهي وكالة حكومية مسؤولة عن عمليات التأثير محليًّا ودوليًّا. كما قامت "ميتا" (Meta) بتفكيك نظام تضليل مرتبط بالجيش الفرنسي، تم إنشاؤه لزعزعة استقرار الشبكات الروسية المنافسة في جمهورية إفريقيا الوسطى قبل انتخابات 2020 في ذلك البلد. قبل ذلك تدخلت شركة الاستشارات البريطانية "كمبريدج أنالتيكا" (Cambridge Analytica) في الانتخابات في كينيا ونيجيريا لصالح جهات خاصة. كما قدمت تركيا التدريب للصحفيين ووسائل الإعلام الإفريقية. كما لم تفلت مصر والمغرب ونيجيريا والسنغال من شبكات الدعاية الإيرانية. من جهة أخرى، تغذِّي هذه الحملات المعلومات المضللة بين الأفارقة بشكل متزايد؛ إذ إن الأنظمة الأجنبية التي ليست ليبرالية تشوه سمعة الديمقراطية من خلال مزج المعلومات الكاذبة والمثيرة مع الانتقادات المشروعة للسياسة الغربية(25).

في المستقبل، من المتوقع أن يصبح الفضاء السيبراني في إفريقيا بشكل متزايد، مجالاً جديدًا للصراع الجيوسياسي بين مختلف القوى؛ إذ تتزامن الأهمية الجيوسياسية المتزايدة للقارة مع الانفجار المتوقع في عدد مستخدمي الإنترنت.

ثانيًا: تعزيز القدرات السيبرانية الدفاعية

تسهم الهجمات المتكررة وحوادث التخريب والتجسس وغيرها في تسريع وتيرة التسلح السيبراني. لقد أعلنت بعض الدول بالفعل أن "الفضاء السيبراني" أصبح يشكل المجال العسكري الخامس (بعد البر والبحر والجو والفضاء). وقد وضع العديد من البلدان في مختلف أنحاء العالم ميزانيات كبيرة لبناء القدرات السيبرانية العسكرية الهجومية والدفاعية على حدٍّ سواء، لكنها لم تشمل حتى الآن سوى أربع دول إفريقية، هي: كينيا ونيجيريا وجنوب إفريقيا وسيراليون. في جنوب إفريقيا، تركز وزارة الدفاع على إنشاء قدرة شاملة لحرب المعلومات تغطي مجالات، منها الحرب السيبرانية والإلكترونية والنفسية. كما أعلنت كينيا، في عام 2016، عن التزامها بتطوير قدرات إلكترونية هجومية. وفي عام 2018، أنشأت نيجيريا قيادة للحرب الإلكترونية ضمن الجيش لتعزيز الحماية من التهديدات السيبرانية. كذلك، أوضحت سيراليون في إستراتيجيتها الوطنية 2017–2022 ضرورة امتلاك وسائل للرد على الهجمات السيبرانية، بما في ذلك قدرات هجومية عند الحاجة(26).

ثالثًا: حماية السيادة الرقمية وسط المنافسة الجيوسياسية الدولية

أصبحت الموضوعات الرقمية بارزة بشكل متزايد في علاقات إفريقيا مع شركائها. فيما يتعلق بقضايا الحوكمة الواسعة، يهدف الاتحاد الأوروبي والولايات المتحدة الأميركية والصين إلى جذب دعم الدول الإفريقية لمبادرات مثل إعلان مستقبل الإنترنت بقيادة الولايات المتحدة الأميركية والاتحاد الأوروبي والمبادرة الصينية حول البناء المشترك لمجتمع ذي مستقبل مشترك في الفضاء السيبراني. وتشارك الجهات الفاعلة الثلاث في مبادرات مختلفة لدعم تطوير البنى التحتية الرقمية في جميع أنحاء القارة، بما في ذلك مبادرة الحزام والطريق الصينية ومبادرة التنمية العالمية الجديدة، وشراكة مجموعة السبع للبنية التحتية العالمية والاستثمار، بقيادة الولايات المتحدة الأميركية؛ والبوابة العالمية للاتحاد الأوروبي.

تولي هذه الجهات الفاعلة أيضًا مزيدًا من الاهتمام للموضوعات الرقمية الأخرى في علاقاتها مع البلدان الإفريقية. يتطور نهج الصين تجاه إفريقيا من نهج يركز على البنية التحتية إلى نهج أكثر شمولاً يغطي أيضًا قضايا الحوكمة الرقمية الأخرى، بما في ذلك التجارة الإلكترونية والاقتصاد الرقمي والأمن السيبراني وتنمية القدرات. يتطلع الاتحاد

الأوروبي إلى دعم نمو الاقتصاد الرقمي في جميع أنحاء القارة، فضلاً عن تطوير سياسات وبيئات تنظيمية مواتية للاقتصادات والمجتمعات الرقمية الشاملة. كما تنظر الولايات المتحدة بشكل متزايد إلى إفريقيا على أنها المكان المناسب لتنفيذ منافستها الرقمية مع الصين. كما وضعت الهند الرقمنة أولوية لتعاونها مع إفريقيا، لاسيما في مجالات مثل الصحة الرقمية والحكومة الإلكترونية والمعرِّفات الرقمية(27).

في خضم هذا المشهد الجيوسياسي الرقمي سريع التغير، تهدف الدول الإفريقية إلى اتباع أولوياتها الخاصة وتجنب الانحياز إلى أي طرف. على سبيل المثال، في المنافسة الرقمية بين الولايات المتحدة والصين بدلاً من التطلع إلى التوافق إستراتيجيًّا مع القوى السياسية الرقمية الكبرى، يبقى الرهان أن تكون الدول الإفريقية أكثر اهتمامًا بتنويع قاعدتها التكنولوجية وتعزيز الحوكمة الرقمية من خلال اتخاذ قرارات تسهم في تحقيق الأمن والنمو الاقتصادي وحماية سيادتها في المجال الرقمي.

رابعًا: تعزيز المشاركة الدولية

يتمثل الرهان الأول في تعزيز الحضور الإفريقي ضمن فضاءات الحوكمة الرقمية العالمية، خاصة داخل المنظمات والهيئات متعددة الأطراف مثل الاتحاد الدولي للاتصالات، ومنظمة التجارة العالمية، وهيئة الإنترنت للأرقام والأسماء المُخصصة أو "آيكان" (ICANN)، ومنتدى إدارة الإنترنت. وتسعى الدول الإفريقية من خلال هذا الحضور إلى عدم تهميش مصالحها وضمان تمثيل عادل لقضاياها الرقمية ضمن صياغة القواعد والمعايير الدولية. إذ تواجه إفريقيا تحديًا كبيرًا يتمثل في تهميشها ضمن بعض المنصات الدولية؛ إذ إن تمثيلها غالبًا ما يكون ضعيفًا أو شكليًّا، وهو ما يدفعها إلى السعي نحو ضمان مشاركة فعلية ومنصفة في صنع السياسات الدولية حتى لا تُفرَض عليها قواعد لا تأخذ في الاعتبار أولوياتها وظروفها الخاصة.

كما يشكِّل الدفاع عن السيادة الرقمية هاجسًا حقيقيًّا للدول الإفريقية في ظل تصاعد التوترات الجيوسياسية العالمية. وتسعى هذه الدول إلى ضمان احترام القانون الدولي داخل الفضاء السيبراني، وتطالب بصوت موحد يدافع عن مصالح القارة ضمن المفاوضات متعددة الأطراف.

وفي خضم هذا التفاعل الدولي، تحرص الدول الإفريقية على تحقيق توازن دقيق بين مصالحها التنموية من جهة، والانخراط في النقاشات الأمنية الجيوسياسية من جهة أخرى؛ إذ يؤكد العديد من الحكومات الإفريقية على ضرورة جعل الأمن السيبراني رافعة للتنمية وليس أداة لصراع النفوذ بين القوى الكبرى.

كما تراهن إفريقيا على لعب دور فاعل في المشاورات الأممية الرامية إلى صياغة اتفاقية دولية حول الجرائم السيبرانية، من خلال مشاركتها في اللجنة الخاصة التابعة للجمعية العامة للأمم المتحدة. وتسعى من خلال ذلك إلى ضمان أن تعكس الاتفاقية المرتقبة خصوصياتها القانونية والتقنية، وأن تحمي مجتمعاتها من التهديدات الإلكترونية المتزايدة.

أخيرًا، يتطلب هذا الطموح الإفريقي نحو التموقع في النظام السيبراني العالمي تكوين جيل جديد من الدبلوماسيين الرقميين والخبراء السيبرانيين القادرين على تمثيل مصالح القارة بكفاءة داخل المنصات الدولية، وعلى التأثير في السياسات الرقمية العالمية انطلاقًا من رؤية إفريقية منسجمة وشاملة.

خاتمة

في مواجهة مستوى متصاعد من التهديدات السيبرانية، تقف إفريقيا اليوم على مفترق طرق حاسم بين تحديات مركبة يجب العمل على تجاوزها ورهانات على المستوى الدولي يجب كسبها، ولكن أيضًا فرص هائلة يجب اغتنامها.

فرغم التحديات البنيوية والمؤسساتية التي تواجهها، تملك إفريقيا فرصًا واعدة وآفاقًا إستراتيجية يمكن استثمارها لتأمين موقع فاعل لها ضمن النظام السيبراني العالمي. فتنامي الوعي السياسي بأهمية الفضاء الرقمي، وازدياد مشاركة الدول الإفريقية في المنصات الدولية المعنية بالأمن السيبراني، يفتح الباب أمام القارة لتعزيز قدراتها الذاتية والتأثير في صياغة القواعد الحاكمة للفضاء الرقمي.

من أبرز الفرص المتاحة، يمكن الإشارة إلى التوجه المتصاعد نحو التعاون جنوب-جنوب، وتنامي المبادرات الإقليمية داخل القارة كتلك التي يقودها الاتحاد الإفريقي لتعزيز التنسيق الأمني الرقمي، إضافة إلى تزايد الدعم الدولي لبناء القدرات التقنية والمؤسساتية للدول الإفريقية. كما يمثل تفاعل دول القارة مع إستراتيجيات القوى الكبرى والأجندة الرقمية الأممية، سواء من خلال الشراكات أو مجموعات الخبراء أو مفاوضات الاتفاقيات الدولية، فرصة لتعزيز حضورها، شريطة تبني رؤية موحدة تعكس أولويات التنمية والسيادة الرقمية الإفريقية.

كما أن التوسع السريع في البنية التحتية الرقمية، والاهتمام المتزايد من قبل القطاع الخاص والاستثمار الأجنبي في الأسواق الرقمية الإفريقية، يتيحان فرصًا لتطوير أنظمة حماية متقدمة، وتحفيز الابتكار في مجال الأمن السيبراني، خاصة إذا تم ربط هذه الجهود بإصلاحات مؤسساتية وتشريعية داخلية تضمن الشفافية وحماية المعطيات.

إن مستقبل الأمن السيبراني في إفريقيا لا يتوقف فقط على مواجهة التهديدات وسد الفجوات الحالية، بل يتطلب أيضًا بناء نموذج إفريقي مستقل للأمن الرقمي، يقوم على مبدأ الشمولية، ويوازن بين الأمن وحقوق الإنسان، وبين التنمية والحماية. وبذلك، يمكن للقارة أن تتحول من كونها ساحة هشَّة للهجمات ومتلقيةً للسياسات الرقمية إلى فاعل مؤثر في صياغتها، بما يخدم مصالح شعوبها ويعزز مكانتها في الساحة الدولية.

*** مصطفى جالي، باحث متخصص في القضايا السياسية والجيوسياسية والأمن الدولي، مهتم بالشؤون الإفريقية.**

مراجع

[1] Interpol, African Cyberthreat Assessment Report 2024, outlook by the african cybercrime operations desk – 3rd edition. https://tinyurl.com/3ajjar6d

[2] "Understanding Africa's Emerging Cyber Threats" Africa Center for strategic studies, Apr. 10, 2025. (accessed May 24, 2025). https://tinyurl.com/4yeccmd5

[3] Abraham, "Major Cyber Attack on Africa's Top organizations in 2024," A&D Forensics, Feb. 02, 2025. (accessed May 24, 2025). https://tinyurl.com/ya7vbsjw

[4] مؤشر يقيِّم مستوى تأهب البلدان للأمن السيبراني، أي قدرة الدول على حماية بنيتها التحتية الحيوية وبياناتها الحساسة والاستجابة بفاعلية للتهديدات والحوادث السيبرانية، والذي يقيس التزامات البلدان في مجال الأمن السيبراني عبر 5 ركائز أساسية: التدابير القانونية (قوانين ولوائح الأمن السيبراني والجرائم السيبرانية)، والتدابير الفنية، والتدابير التنظيمية (الإستراتيجيات والمنظمات الوطنية)، وتدابير تنمية القدرات (التوعية والتدريب والتثقيف والحوافز)، وتدابير التعاون (الشراكات بين الوكالات والشركات والبلدان)، وتشمل هذه الركائز الخمسة 20 مؤشرًا فرعيًّا.

Interpol, African Cyberthreat Assessment Report 2024. Ibid.

[5] Ibidem.

[6] Lenah Chacha and Corlane Barclay, "Mapping Africa's Cybersecurity Development: Insights from the Global Cybersecurity Index 2024 ", 2024. (accessed May 24, 2025). https://tinyurl.com/mtc6ufrb

[7] Ibidem.

[8] "Flagship Projects of Agenda 2063, African Union," Au.int, 2024. (accessed May 24, 2025). https://tinyurl.com/yky4whhk

[9]The Digital Transformation Strategy For Africa (2020–2030), African Union, 2020. (accessed May 24, 2025). https://tinyurl.com/ybpajnur

[10] African Union Cyber Security Expert Group - Terms of Reference, African Union, (n.d.). (accessed May 24, 2025). https://tinyurl.com/5cyc7skf

[11] Sorina Teleanu and Jovan Kurbalija, "Stronger digital voices from Africa: Building African digital foreign policy and diplomacy," DiploFoundation, Nov. 16, 2022. https://tinyurl.com/352xsczw (accessed May 24, 2025).

[12] "Africa: AU's Malabo Convention set to enter force after nine years," Data Protection Africa, May 19, 2023. https://tinyurl.com/yc5am6bx (accessed May 24, 2025).

[13] "Stronger digital voices from Africa..",Ibid.

[14] Ibidem.

[15] Interpol, African Cyberthreat Assessment Report 2024.Ibid.

[16] Franck Kié, "Cyber Africanum est ! Les enjeux de l'intelligence artificielle et de la cybersécurité en Afrique", Fondation Jean-Jaurès, September 10, 2024. https://tinyurl.com/5n8b7b9c (accessed May 24, 2025).

[17] Ibidem.

[18] Interpol, African Cyberthreat Assessment Report 2024.Ibid.

[19] "Les enjeux de l'intelligence artificielle et de la cybersécurité en Afrique",Ibid.

[20] "Mapping Africa's Cybersecurity Development...Ibid.

[21] "Stronger digital voices from Africa..",Ibid.

[22] Interpol, African Cyberthreat Assessment Report 2024.Ibid.

[23] "Les enjeux de l'intelligence artificielle et de la cybersécurité en Afrique", Ibid.

[24] Kyle Hiebert, "Disinformation tactics in Africa," Issafrica.org, February 04, 2025. https://tinyurl.com/34k6kbx9 (accessed May 24, 2025).

[25] Ibidem.

[26] "Stronger digital voices from Africa..", Ibid.

[27] Ibidem.

انتهى