الإنتربول

تقرير الإنتربول لتقييم التهديدات السيبرانية في أفريقيا لعام 2025

الإصدار الرابع

أيار/مايو 2025

إخلاء المسؤولية القانونية

المحتويات

الكلمة التمهيدية من الإنتربول

نيل جيتون
مدير مكافحة الجريمة السيبرانية
الإنتربول

تقف القارة الأفريقية اليوم عند منعطف حاسم في تطورها الرقمي. وفيما يتّسع نطاق الاتصال وتتسارع وتيرة الابتكار الرقمي، يتفاقم أيضاً تعقيد التهديدات السيبرانية التي تواجه المنطقة. فهذه التهديدات لا تعرف حدوداً- بل هي عابرة للأوطان تتنقل بسرعة وتزداد تطورا. كما أنها تستهدف البنية التحتية التي يقوم عليها التقدم، كالنظم المالية والخدمات العامة والبنية التحتية الحرجة والأهم، ثقة المواطنين في المستقبل الرقمي.

ويوفر الإصدار الرابع لتقرير الإنتربول عن تقييم التهديدات السيبرانية في أفريقيا لمحة أساسية عن الوضع الحالي. وإذ يسترشد بالاستخبارات الميدانية والمشاركة الكثيفة لأجهزة إنفاذ القانون والتعاون بين القطاعين العام والخاص، يرسم صورة واضحة لمشهد التهديدات المتغير باستمرار الذي ما زالت تطغى عليه البرمجيات الخبيثة، وبخاصة برمجية انتزاع الفديةوالاحتيال عبر الإنترنت، بما في ذلك التصيد الاحتيالي، والاحتيال بالبريد الإلكتروني المهني، في حين أن المخاطر الناشئة، مثل الاحتيال المدعوم بالذكاء الاصطناعي، والاعتداء الجنسي القائم على الصور عبر الإنترنت، والجرائم الجنسية الرقمية، والجرائم السيبرانية كخدمة، تتطلب اهتمامًا عاجلاً.

ونقرّ في الإنتربول أنه لا يمكن لأي جهاز أو بلد أن يتصدّى لهذه التحديات بمفرده. بالفعل، يستوجب نطاق الجريمة السيبرانية وسرعتها استجابة موحدة ومنسّقة مستندة إلى المعلومات الاستخباراتية. ومن خلال العملية المشتركة لمكافحة الجريمة السيبرانية في أفريقيا (AFJOC) وبالشراكة الوثيقة مع أفريبول، نعزز قدراتنا الميدانية ونعمّق الثقة بين الوحدات الوطنية لمكافحة الجريمة السيبرانية، ونوطد التعاون عبر الحدود الوطنية بما يسمح بتعطيل شبكات الجريمة السيبرانية.

كذلك، يعكس التقرير تنامي القدرة على الصمود والإمكانيات في أجهزة إنفاذ القانون الأفريقية. ويُحرَز التقدم على مستوى العمليات الإقليمية والإصلاحات التشريعية الجديدة وجهود بناء القدرات. بيد أن الطريق أمامنا ما زال طويلاً. فالفجوات في المعرفة الرقمية والمواءمة بين التشريعات وموارد التحقيق والوصول إلى الأدلة الرقمية ما زالت تعيق الإنفاذ الفعال.

وبالنسبة إلى جميع شركائنا – إن في أجهزة إنفاذ القانون أو الحكومات أو الصناعة أو المجتمع المدني- يمثل هذا التقرير دعوة إلى العمل وأساسا للتعاون في الوقت ذاته. فمن خلال العمل معا وتبادل المعرفة وبناء الثقة عبر الحدود والقطاعات، يمكننا تحقيق مستقبل أفريقيا الرقمي.

وأودّ أن أعرب عن خالص تقديري للمكتبُ المعني بعمليات مكافحة الجريمة السيبرانية في أفريقيا وجميع الذين ساهموا في هذا التقرير. فجهودنا توطّد عزيمتنا الجماعية على بناء بيئة رقمية أكثر أمانا وقدرة على الصمود. وأخيرا، أودّ أن أشكر مجتمع إنفاذ القانون في البلدان الأعضاء الأفريقية على تفانيه في مكافحة الجريمة السيبرانية ليصبح العالم أكثر أمانا.

الكلمة التمهيدية من أفريبول

السفير جلال شلبا
المدير التنفيذي بالوكالة،
أفريبول

تدخل القارة الأفريقية عصر التحوّل الرقمي السريع الذي يوفر فرصا غير مسبوقة للتنمية الاقتصادية والاجتماعية والمؤسسية لدولها الأعضاء. ويعكس هذا الزخم التزاما جماعيا بتسريع وتيرة الشمول الرقمي، وتحسين الخدمات العامة وتحفيز الابتكار المحلي. إنما يترافق هذا التقدم الكبير أيضا بتهديدات متزايدة ومتطورة في الفضاء السيبري، الأمر الذي يعرّض إلى الخطر أمن الدول والبنية التحتية الحرجة ومؤسسات الأعمال والمواطنين الأفريقيين.

وفي وجه هذه التحديات المعقدة، تُعتبر أفريبول منظمة رائدة في القارة الأفريقية في مجال وضع الاستجابات المنسقة والطموحة والمحددة السياق المتكيفة مع الواقع الأفريقي. والتزامنا واضح: تعزيز السيادة الرقمية القوية القادرة على حماية مجتمعاتنا بفعالية من التهديدات السيبرانية التي لا تنفك تزداد براعة، والتي غالبا ما تكون عبر وطنية في طبيعتها وسريعة التطور بقدر التكنولوجيات بحدّ ذاتها.

وفي عام 2024، كثف أفريبول جهوده عبر التعاون الوثيق مع الإنتربول والهياكل الإقليمية المتخصصة وأجهزة الأمن الوطني والشركاء الاستراتيجيين في القطاع الخاص. وقد أفضت العمليات المشتركة الكبيرة، مثل عملية Serengeti، إلى تفكيك الشبكات الإجرامية المتطورة والمتخصصة في برمجيات انتزاع الفدية والاحتيال المالي والتصيد الاحتيالي المحدد الهدف والهجمات على نظم المعلومات الحكومية. وألقت هذه النجاحات الميدانية الضوء على أهمية التعاون بين الأجهزة وتشارك المعلومات وتجميع القدرات والاستجابة المنسقة في القارة.

وبموازاة ذلك، واصل أفريبول تعزيز مهارات العاملين في أجهزة إنفاذ القانون من خلال برامج تدريب متخصصة ومستهدفة، تغطي مجالات رئيسية مثل تحليل الاستخبارات الإجرامية وتعقّب التدفقات المالية غير المشروعة والمراقبة السيبرانية وحماية البنية التحتية الحرجة. كما شكّلت الاتفاقات الاستراتيجية الموقّعة مع كل من شركة Kaspersky و Group-IB عام 2024 خطوة حاسمة في التزامنا بتزويد الدول الأعضاء بالموارد الضرورية لمنع الحوادث الكبيرة والتصدي لها، من خلال تعزيز الوصول إلى الأدوات التكنولوجية والبيانات الاستخباراتية المتصلة بالتهديدات والخبرة الدولية.

وفي عام 2025 وبعده، سيركز أفريبول جهوده على هذه الأولويات الاستراتيجية الثلاثة: (1) تعزيز التعاون الدولي وبين البلدان الأفريقية لبناء استجابة موحدة في وجه التهديدات العابرة للحدود الوطنية؛ (2) دعم الدول الأعضاء بشكل وثيق في توسيع نطاق قدراتها الميدانية والبشرية والتكنولوجية؛ و(3) الدمج المنهجي للابتكارات الناشئة، وبخاصة الذكاء الاصطناعي وتكنولوجيات blockchain، لاستباق المخاطر وتكييف استراتيجياتنا في الوقت الفعلي.

فالأمن السيبري ليس مجرد مسألة فنية، بل أصبح ركيزة أساسية للاستقرار والسلام والتنمية المستدامة في أفريقيا، كما تنص عليه خطة عام 2063. وهو يتعلق مباشرة بالسيادة الرقمية للدول، وقدرة مؤسساتنا على الصمود، وثقة المواطنين وحسن سير اقتصاداتنا. وفي هذه الروح من المسؤولية المشتركة والتضامن القاري والابتكار المستمر يجدّد أفريبول التزامه ببناء فضاء سيبري أفريقي مأمون وشامل وسيادي وقادر على الصمود يحقق السلام والأمن والتقدم الجماعي.

شكر وتقدير

أعدّ هذا التقرير المكتبُ المعني بعمليات مكافحة الجريمة السيبرانية في أفريقيا، بدعم من مكتب العمليات المشتركة لمكافحة الجريمة السيبرانية في أفريقيا الذي تموله وزارة الخارجية والكومنولث والتنمية في المملكة المتحدة. ولطرح الأسئلة عن التقرير، يُرجى الاتصال بنا على الموقع Africadesk@interpol.int.

ويمثل هذا التقرير تتويجا لتحليل شامل للمعلومات التي جُمعت من مجموعة من المصادر، بما في ذلك البلدان الأعضاء الأفريقية وشركاء الإنتربول في القطاع الخاص مثل Bi.Zone و Group-IB وشركة Kaspersky و Trend Micro. إضافةً إلى ذلك، تمت الاستفادة من وحدات الإنتربول المعنية بالاستخبارات والعمليات لتوفير المعلومات للتقرير وإثرائه، بما يضمن فهما شاملا ودقيقا للمسائل.

ونعرب عن امتناننا لمساهمة 43 من أصل 54 بلدا عضوا أفريقيا استكمل الاستبيان لتقييم التهديدات السيبرانية وقدّم أفكارا قيّمة استرشد بها هذا التقرير.

الإنتربول

AFJOC

Foreign & Commonwealth Office

AFRIPOL

BI.ZONE Cybersecurity

GROUP-IB

kaspersky

TREND MICRO

موجز

تتسارع وتيرة الجريمة السيبرانية في أفريقيا مهددةً السلامة العامة والنظم المالية والثقة الرقمية. وفي حين تتصدّى لها معظم البلدان، ما زال عديد منها يواجه تحديات هيكلية تحدّ من قدرتها على كشف التهديدات السيبرانية والتحقيق فيها وتعطيلها.

وتبقى قدرات أجهزة إنفاذ القانون غير متكافئة. بالفعل، تفيد أغلبية البلدان عن نقص في مهارات التحقيق في الجرائم السيبرانية، وإمكانية محدودة في الوصول إلى أدوات الأدلة الجنائية الرقمية والبنية التحتية غير الكافية. ورغم أن بلدان عديدة أطلقت وحدات مخصصة لمكافحة الجريمة السيبرانية، غالبا ما تعمل هذه الوحدات في ظل محدودية الموارد وعدد الموظفين.

تتحسّن الأطر القانونية غير أن التقدم مجزأ. فقد حدّثت بعض البلدان الأعضاء التشريعات المتصلة بمكافحة الجريمة السيبرانية إنما في حالات عدة، أشارت البلدان المشمولة في الدراسة الاستقصائية إلى أن أطرها القانونية وقدراتها في مجال الملاحقة القانونية بحاجة إلى تحسين. ويمكن أيضا مواءمة هذه القوانين مع المعايير الإقليمية والدولية بشكل أفضل. وما زالت هذه الثغرات تعيق الملاحقات القضائية ومقبولية الأدلة الرقمية.

ويبقى التنسيق عبر الحدود عائقا كبيرا. ففي حين حققت العمليات التي يسّرها الإنتربول نتائج ملحوظة، تشير البلدان في تقاريرها إلى أن قنوات التعاون الرسمية مثل عمليات المساعدة القانونية المتبادلة ما زالت بطيئة وغير مستخدمة على نحو كاف. كما أن المسائل القضائية وغياب الثقة والوصول المحدود إلى المنصات الرقمية العالمية هي عوامل تزيد من تعقيد جهود الإنفاذ الإقليمية.

كذلك، تتطور التهديدات الناشئة بسرعة. فالاستخدام الجنائي للذكاء الاصطناعي، ووسائط الإعلام الاصطناعية ومخططات الاحتيال المدعومة بالهواتف الخلوية يفوق قدرة عدة أجهزة على الاستجابة. وغالبا ما تستغل هذه التهديدات النقاط الخفية القانونية والميدانية، وتتطلّب أشكالا جديدة من التعاون بين الأجهزة والتعاون الدولي.

ورغم هذه التحديات، تظهر علامات تقدم مشجّعة. بالفعل، قد عززت بلدان أعضاء عديدة الشراكات بين القطاعين العام والخاص، وحدّثت التشريعات بما يتيح فعالية أكبر في الملاحقة القانونية للجرائم السيبرانية وشاركت في العمليات الإقليمية الناجحة. ويتزايد الوعي لمخاطر الجرائم السيبرانية كما أن المزيد من خدمات الشرطة الوطنية تمنح الأولوية لقدرات التحقيق الرقمي.

ويشير هذا التقرير إلى التحديات الرئيسية في مجال الجريمة السيبرانية التي تواجه أفريقيا، واتجاهات التهديدات الناشئة والأمثلة المستمدة من العالم الحقيقي على الحواجز المنهجية والنجاحات الميدانية. ويختتم بتوصيات لتعزيز القدرات الوطنية وتوطيد الأطر القانونية والإجرائية وتعميق التعاون الدولي- وجميعها أساسية لبناء القدرة على الصمود في الأجل الطويل.

1. مقدمة

يعيد التحوّل الرقمي المتسارع في أفريقيا تحديد ملامح الاقتصادات والحوكمة والمجتمع. ورغم الاستفادة من التكنولوجيات الأخيرة والابتكار،كما وسّع أيضا بشكل ملحوظ مجال التعرض للهجمات السيبرانية. وفيما يزداد الاعتماد على الفضاء الرقمي، تتفاقم التهديدات التي تستهدف النظم المالية والخدمات العامة ومؤسسات الأعمال والمستخدمين النهائيين.

وبهدف فهم مشهد المخاطر المتطور والتصدي له بشكل أفضل، أجرى الإنتربول تقييما للتهديدات السيبرانية على مستوى القارة. ويستند التقرير إلى دراسة استقصائية مفصّلة لأجهزة إنفاذ القانون الأفريقية والبيانات الاستخباراتية الميدانية وأفكار شركاء الإنتربول في القطاع الخاص ومعلومات مفتوحة المصدر. ويضمن هذا النهج المتعدد المصادر وجود نظرة واقعية وشاملة للاتجاهات الإقليمية.

ويتبع هذا التقييم التقرير عن تقييم التهديدات السيبرانية في أفريقيا لعام 2024، ويبني على الاستنتاجات التي خلص إليها تقرير العام الماضي. كما يهدف إلى توفير منظور محدّث لمشهد الجريمة السيبرانية وتعقّب التقدم المحرز في التصدي للتحديات المشار إليها سابقا.

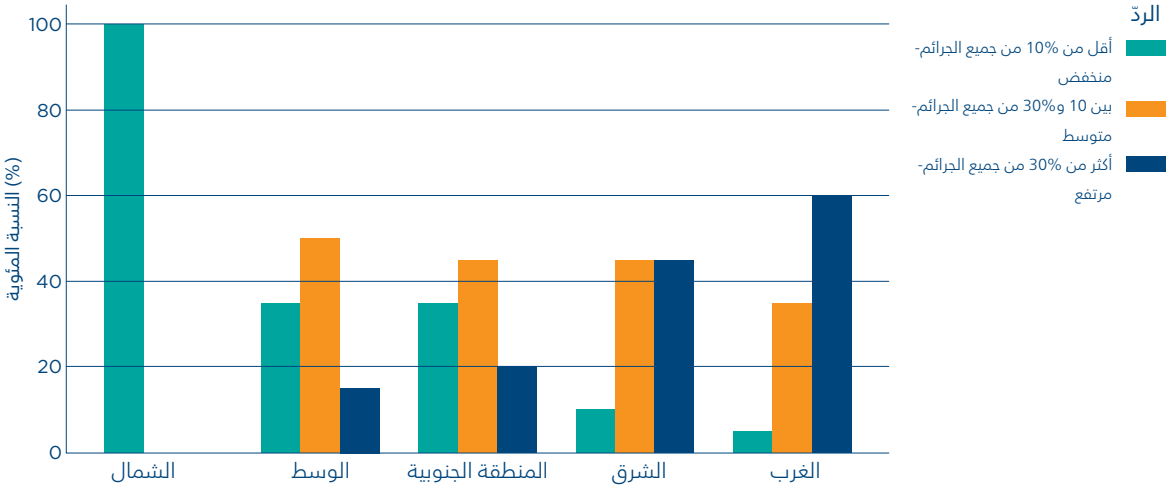
ويتمثل هدف هذا التقرير في دعم إنفاذ القانون وصانعي السياسات وأصحاب المصلحة في الأمن السيبري في تحديد التهديدات لناشئة، ومعالجة الثغرات في القدرات وتعزيز التعاون على المستويين الوطني والإقليمي. كما أن التحقيق في الجرائم السيبرانية على أي مستوى كان له تأثيرٌ مباشر على الضحايا الفعليين والمحتملين الموجودين حول العالم. لذا، وبفضل الجهود الجماعية، سيكون مستقبل أفريقيا الرقمي أكثر أمانا.

2. مشهد التهديدات السيبرانية المتطور في أفريقيا

سمح التحول الرقمي السريع في أفريقيا بزيادة التواصل إلى حد كبير ودفع إلى اعتماد التكنولوجيات على نطاق واسع مثل الخدمات المصرفية عبر الهواتف المحمولة والتجارة الإلكترونية والحوسبة السحابية، بما يحفّز النمو الاقتصادي والابتكار[1]. بيد أن هذا التوسّع طرح أيضا تحدياتٍ في مجال الأمن السيبري، سيما أن البنى التحتية الرقمية أصبحت تشكل أهدافا جذابة للجهات الفاعلة في الجريمة السيبرانية. وفي ظل وجود أكثر من 500 مليون مستخدم للإنترنت في المنطقة، ما زالت عدة بلدان تفتقر إلى التدابير الملائمة في مجال الأمن السيبري، الأمر الذي يعرّض مؤسسات الأعمال والأفراد إلى الهجمات[2]. كما تواجه عدة بلدان في القارة تحديات مثل الأطر القانونية التي لا تزال في طور التشكل، والاستثمار المحدود في الأمن السيبري والثغرات في المعرفة الرقمية، الأمر الذي يفاقم هذه المخاطر.

كذلك، نظرا للاستخدام الواسع النطاق للهواتف الذكية، أصبحت المنصات الجوالة هدفا أوليا لمرتكبي الجرائم السيبرانية، وبخاصة في المناطق التي تعتمد مستوى مرتفعا من الخدمات المصرفية بواسطة الهواتف المحمولة. إضافة إلى ذلك، تنشأ مخاطر أمنية جديدة عن الدمج المتزايد لأجهزة إنترنت الأشياء في قطاعات مثل الزراعة والرعاية الصحية والتصنيع، حيث أن العديد من هذه الأجهزة لا تحظى بحماية متينة.[3] وقد كانت دول أفريقية عديدة، بما في ذلك إثيوبيا وزمبابوي وأنغولا وأوغندا ونيجيريا وكينيا وغانا وموزامبيق، من بين الأكثر استهدافا على المستوى العالمي عام 2024، وفقا للبيانات بشأن الكشف عن برمجيات خبيثة الصادرة عن المؤشر العالمي للتهديدات السيبرانية للاتحاد الدولي للاتصالات اللاسلكية.[4] ويؤكد هذا الأمر على الحاجة إلى أطر أكثر متانة في مجال الأمن السيبري من أجل حماية التطورات الرقمية وضمان قدرة المنطقة على الصمود في الأجل الطويل.[5,6]

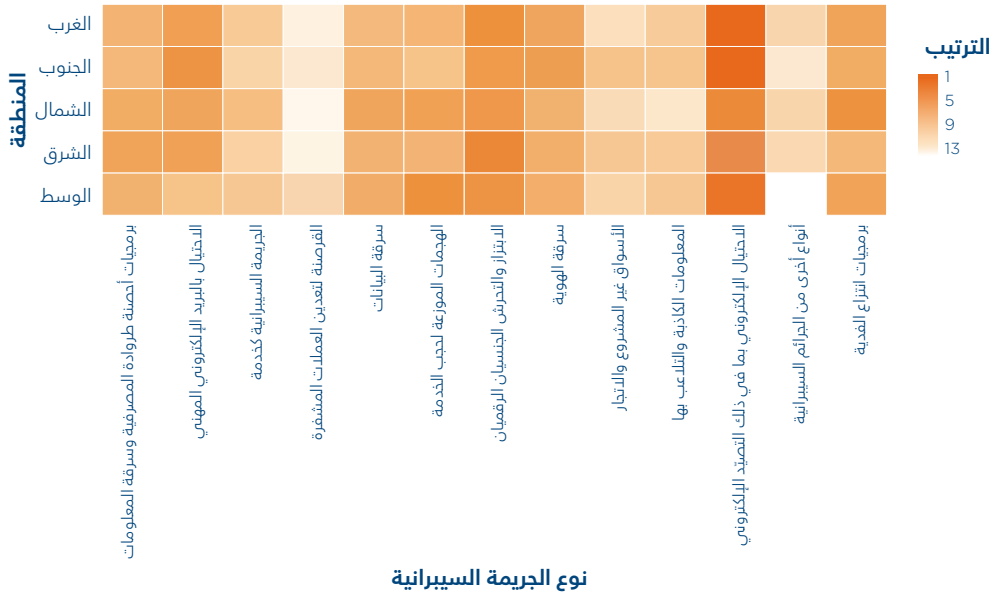
وأما تقرير الإنتربول عن تقييم التهديدات السيبرانية في أفريقيا لعام 2025، فيلقي الضوء على الزيادة الحادة في حوادث الجرائم السيبرانية في أفريقيا. وأشار أكثر من ثلثي البلدان الأفريقية الأعضاء في الإنتربول المشمولة بالدراسة الاستقصائية إلى أن الجرائم التي تعتمد على الفضاء السيبري والمرتكبة بواسطة هذا الفضاء تمثل نسبة متوسطة إلى مرتفعة من جميع الجرائم. وبصورة خاصة، تشكل الجرائم السيبرانية أكثر من 30 في المائة من جميع الجرائم المبلّغ عنها في أفريقيا الغربية والشرقية معا، ما يحوّل الأمر إلى مصدر قلق كبير في هذه المناطق الفرعية.



الرسم1: المستويات الملحوظة لمخاطر الجرائم السيبرانية في جميع المناطق الفرعية في أفريقيا وفقا لما أفادت عنه البلدان الأفريقية الأعضاء في الإنتربول في استبيان عام 2025.

1 GSMA, The Mobile Economy of the Sub-Saharan Africa: https://event-assets.gsma.com/pdf/GSMA_ME_SSA_2024_Web.pdf
2 https://innovation-village.com/cybersecurity-in-africa-emerging-threats-and-solutions
3 GSMA, The Mobile Economy of the Sub-Saharan Africa: https://event-assets.gsma.com/pdf/GSMA_ME_SSA_2024_Web.pdf
4 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf
5 Check Point, The State of Cyber Security 2025: https://www.checkpoint.com/security-report
6 https://it-online.co.za/2024/09/13/africa-faces-urgent-cybersecurity-challenges

وقد حدّدت إصدارات سابقة للتقرير الهجمات المتصلة ببرمجيات انتزاع الفدية وبرمجيات أحصنة طروادة المصرفية وسرقة المعلومات، والاحتيال الإلكتروني، والتصيد الاحتيالي، والاحتيال بالبريد الإلكتروني المهني، والبرمجيات الخبيثة كخدمة، مثل برمجيات التجسس وأدوات التصيد الاحتيالي، على أنها التهديدات السيبرانية الأكثر انتشارا[7]. ولا يزال الاحتيال الإلكتروني، وبخاصة التصيد الاحتيالي، من بين الجرائم السيبرانية الأكثر شيوعا في البلدان الأعضاء في الإنتربول، في حين تبقى برمجيات انتزاع الفدية والاحتيال بالبريد الإلكتروني المهني واسعة الانتشار. إضافة إلى ذلك، تشير البلدان الأعضاء الأفريقية في تقاريرها إلى أن الابتزاز الجنسي الرقمي وسرقة الهوية هما من التهديدات السيبرانية الكبيرة.



الرسم 2: أكثر التهديدات السيبرانية التي تم الإبلاغ عنها في البلدان الأفريقية الأعضاء في الإنتربول في عام 2024، استنادًا إلى بيانات استبيان جهات إنفاذ القانون.

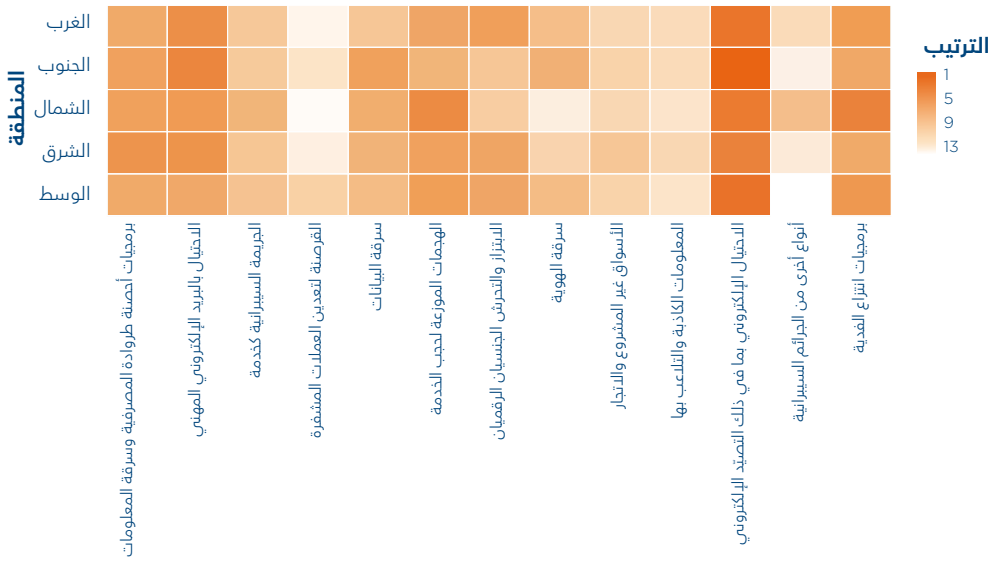
وقد شهدت برمجيات أحصنة طروادة المصرفية وسرقة المعلومات والجريمة السيبرانية كخدمة تراجعا في الحوادث المبلّغ عنها مقارنة بالأعوام الماضية. ويمكن أن يشير هذا الاتجاه إلى تحسّن الجهود في مجال إنفاذ القانون، وزيادة الوعي للأمن السيبري أو إلى تحوّل في تكتيكات مرتكبي الجرائم السيبرانية باتجاه أساليب أكثر فعالية مثل الهندسة الاجتماعية وعمليات الاحتيال عن طريق الذكاء الإلكتروني.

كما أفادت عدة بلدان أعضاء في الإنتربول في منطقة أفريقيا عن تزايد الأثر المالي والميداني للجريمة السيبرانية، حيث حُدّدت عمليات الاحتيال الإلكتروني والاحتيال بالبريد الإلكتروني المهني وبرمجيات انتزاع الفدية والهجمات الموزعة لحجب الخدمة (DDoS) كالتهديدات الأكثر ضررا من الناحية المالية في جميع المناطق الفرعية. وبين عامي 2019 و2025، أفضت الحوادث السيبرانية في القارة إلى خسائر مالية مقدرة بأكثر من 3 مليارات دولار أمريكي[8]، حيث أن قطاعات المالية والرعاية الصحية والطاقة والقطاع الحكومي هي الأكثر تضررا.[9] وتشكل هذه الصناعات الحاسمة الأهمية أهدافا أولية لمرتكبي الجرائم السيبرانية الذين يقومون بتعطيل العمليات وانتهاك البيانات بما يفضي إلى عواقب مالية كبيرة.

7 تقرير الإنتربول عن تقييم التهديدات السيبرانية في أفريقيا لعام 2024: https://www.interpol.int/en/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf

8 https://african.business/2025/02/apo-newsfeed/over-half-of-africans-fear-financial-losses-from-cybercrime-survey-finds

9 Group-IB, Hi-Tech Crime Trends Report 2023/2024; Middle East & Africa Cyberthreat Landscape: https://www.group-ib.com/resources/research-hub/hi-tech-crime-trends-2023-mea/



الرسم 3: متوسط ترتيب أنواع الجريمة السيبرانية حسب الأثر المالي المبلّغ عنه في المناطق الفرعية الأفريقية، بالاستناد إلى البيانات المقدمة من البلدان الأعضاء في الإنتربول.

وفقا لما تبلّغ عنه البلدان الأفريقية الأعضاء في الإنتربول، يعمد مرتكبو الجرائم السيبرانية باستمرار إلى تنقيح تكتيكاتهم، باستخدام الهندسة الاجتماعية والذكاء الاصطناعي ومنصات المراسلة الآنية لإطلاق هجمات متزايدة التطور. كذلك، تستغل الشبكات المحلية والدولية لمرتكبي الجرائم السيبرانية مواطن الضعف البشرية كوسيلة أولية، عبر اللجوء إلى تقنيات خداع متقدمة لاستهداف المنظمات والأفراد.

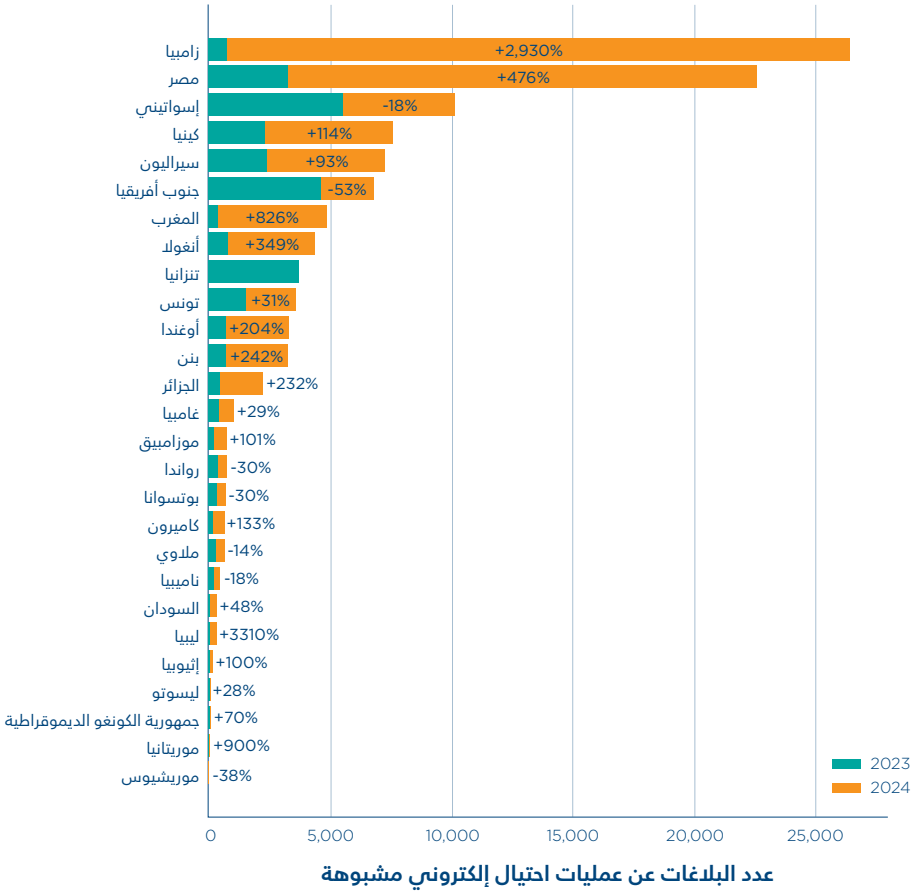
1.2 التهديدات السيبرانية الأكثر انتشارا في أفريقيا في عام 2024

كشفت الاستنتاجات التي خلصت إليها الدراسة الاستقصائية الأخيرة للبلدان الأفريقية الأعضاء في الإنتربول والشركاء في القطاع الخاص،[10] مقرونة بالتقارير الإقليمية عن الأمن السيبري، أن عمليات الاحتيال الإلكتروني وبرمجيات انتزاع الفدية والاحتيال بالبريد الإلكتروني المهني والابتزاز الجنسي الرقمي هي أبرز التهديدات السيبرانية. ويوفّر هذا القسم تحليلا مفصلا لمشهد التهديدات السيبرانية المتطور، حيث يلقي الضوء على التهديدات الأكثر انتشارا في أفريقيا في عام 2024.

1.1.2. عمليات الاحتيال الإلكتروني

تشهد عمليات الاحتيال الإلكتروني زيادة حادة في بلدان عديدة سيما أن مرتكبي الجرائم السيبرانية يكيّفون باستمرار أساليبهم لاستغلال مواطن الضعف والاحتيال على الأفراد ومؤسسات الأعمال معا. بالفعل، أصبحت الأنشطة الاحتيالية، بما في ذلك التصيد الاحتيالي والجيل الرومانسية، أكثر تطورا من خلال الاستخدام الاستراتيجي للهندسة الاجتماعية والذكاء الاصطناعي والتلاعب عبر منصات التواصل الاجتماعي. واعتبرت البلدان الأعضاء في الإنتربول أن عمليات الاحتيال الإلكتروني هذه هي من بين أبرز التهديدات السيبرانية التي واجهت أفريقيا في عام 2024، وأشارت إلى ارتفاع تواترها وتداعياتها الشديدة. وهذا ما تؤكد عليه مصادر إضافية، بما في ذلك البيانات الواردة من شركاء الإنتربول في القطاع الخاص.

10 البيانات الواردة من أربعة شركاء للإنتربول من القطاع الخاص: Group-IB و Trend Micro وشركة Kaspersky و Bi.Zone



الرسم 4: الزيادة في التبليغات عن عمليات الاحتيال الإلكتروني في جميع المناطق في أفريقيا بين عامي 2023 و2024، بالاستناد إلى بيانات قدمتها شركة Kaspersky.

وترتبط هذه الزيادة في عمليات الاحتيال الإلكتروني بشكل وثيق بالتحول الرقمي السريع في أفريقيا.[11] بالفعل، يستفيد المجرمون من النشاط الإلكتروني المتنامي، وبخاصة في مجال استخدام وسائل التواصل الاجتماعي والتجارة الرقمية والخدمات المصرفية عن طريق الهواتف المحمولة لارتكاب عمليات الاحتيال. كما تشير البيانات الواردة من البلدان الأفريقية الأعضاء في الإنتربول إلى أن ضحايا هذه الجرائم متنوعون إذ تؤثر على الأفراد من مختلف الفئات العُمرية والأجناس والمهن. وفي حين تظهر البيانات في الدراسة الاستقصائية الواردة من البلدان الأعضاء أن بعض المجموعات أكثر هشاشة، من الواضح أن جميع الفئات السكانية معرضة للخطر.

ولا تزال عمليات الاحتيال الإلكتروني، عن طريق التصيد الاحتيالي، تمثل التهديد السيبري الأكثر انتشارا في أفريقيا في عام 2024، وتؤثر على الأفراد والمنظمات في القارة. وقد حدّدت البلدان الأعضاء في الإنتربول التصيد الاحتيالي كمصدر القلق الأول للأمن السيبري، مشيرةً إلى تواتره المرتفع وأثره الواسع. ووفقا للتقارير عن الأمن الرقمي، يشكل التصيد الاحتيالي نسبة 34 في المائة من جميع الحوادث السيبرانية التي تم كشفها في أفريقيا.[12] ويستفيد مرتكبو الجرائم السيبرانية من التصيد الاحتيالي من خلال انتحال هوية كيانات موثوق بها عن طريق رسائل البريد الإلكتروني ومنصات المراسلة الآنية أو مواقع الإنترنت الزائفة، وحث الأشخاص على توفير معلومات حساسة مثل بيانات تسجيل الدخول، وبيانات مالية أو تفاصيل شخصية عن الهوية.[13] وعند الحصول على هذه المعلومات، يصبح من السهل الدخول غير المشروع إلى حسابات الأشخاص وسرقة هويتهم وارتكاب الاحتيال المالي. كما أن التطور المتزايد لمخططات التصيد الاحتيالي يزيد بشكل كبير من مواطن الضعف في القطاعات المهمة، بما في ذلك المصارف والمؤسسات الحكومية والاتصالات اللاسلكية.

11 GSMA, The Mobile Economy of the Sub-Saharan Africa: https://event-assets.gsma.com/pdf/GSMA_ME_SSA_2024_Web.pdf
12 ESET Threat Report: https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-threat-report-h22024.pdf
13 _INTERPOL Africa Cyberthreat Assessment Report 2024: https://www.interpol.int/en/content/download/21048/file/24COM005030-AJFOC Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf

وتشير البيانات الواردة في الدراسة الاستقصائية للإنتربول إلى تطور ملحوظ في تكتيكات التصيد الاحتيالي، التي أصبحت أكثر تحديدا من حيث تصميمها ومحليةً بشكل متزايد ومتطورة من الناحية التكنولوجية، إذ انتقلت من عمليات الاحتيال الإلكتروني التقليدية إلى الهجمات المستهدفة في مجال الهندسة الاجتماعية. وبات الجناة الآن ينتحلون هوية سلطات معترف بها وشركات بارزة، ويستغلون البطالة المستشرية عن طريق عروض عمل ملفقة، ويستخدمون منصات الهواتف المحمولة للقيام بعمليات احتيال متصلة بعرض الجوائز أو الاحتجاج بحالة طوارئ. إضافة إلى ذلك، إن التصيد الاحتيالي عن طريق الهواتف المحمولة والتصيد الاحتيالي عن طريق الصوت وحملات التصيد الاحتيالي عبر وسائل التواصل الاجتماعي تستغل ثقة الضحايا ومحفزاتهم العاطفية، الأمر الذي يوسع نطاق مشهد التهديد بشكل أكبر.[14] كما أن إمكانية الوصول إلى أدوات التصيد الاحتيالي المعقولة الكلفة على مواقع التسوق الإلكترونية غير المشروعة تساهم إلى حدّ كبير في انتشار هذه المخططات. ويستعين الجناة أيضا بالنصوص والتسجيلات الصوتية والمصورة التي يتم إنشاؤها عن طريق الذكاء الاصطناعي لتعزيز موثوقية حملات التصيد الاحتيالي وقدرتها على الإقناع، عبر تكييف ما تنقله من رسائل لتتماشى مع اللغات المحلية والفروقات الثقافية.[15]

كذلك، أشارت البيانات التي قدمتها البلدان الأفريقية الأعضاء في الإنتربول إلى أن أثر التصيد الاحتيالي يمتد إلى قطاعات متعددة في أفريقيا، ينطوي كل منها على مواطن ضعف وتداعيات متمايزة. فالمؤسسات المالية تتكبد خسائر كبيرة نتيجة سرقة الحسابات والمعاملات غير المصرح بها، ما يقوّض ثقة المستهلك ويعيق الشمول المالي الرقمي. كما تواجه شركات الاتصالات تحديات على مستوى استغلال العلامة التجارية، والاحتيال المتصل باستبدال شرائح SIM وعمليات الاحتيال الجماعية عن طريق المراسلة الآنية، الأمر الذي يؤثر سلبا على سمعتها وكفاءتها العملياتية. إضافة إلى ذلك، تتصدى الحكومات ومؤسسات الرعاية الصحية والمنشآت التعليمية لبيانات المواطنين التي تمّ اختراقها، وتعطّل العمليات وتراجع ثقة عموم الناس، ما يؤكد على ضرورة وضع استراتيجيات متينة وخاصة بكل قطاع للتخفيف من الآثار.

وفي عام 2024، ازدادت عمليات الاحتيال الرومانسي في جميع أنحاء أفريقيا وأصبحت إحدى عمليات الاحتيال الإلكتروني الأوسع انتشارا في القارة. ويستخدم مرتكبو هذه العمليات تكتيكات أكثر تقدما وإضرارا، مدفوعين بازدياد استخدام الإنترنت والوصول الواسع النطاق إلى وسائل التواصل الاجتماعي. وتشير البيانات المقدمة من البلدان الأعضاء في الإنتربول إلى أن الجناة يبدأون بالاتصال بالضحايا عن طريق وسائل التواصل الاجتماعي، وخدمة المراسلات الإلكترونية، وتطبيقات المواعدة الإلكترونية. ويسعون إلى إقامة علاقات شخصية معهم من خلال استغلال مواطن ضعفهم وهشاشتهم، وقد تكون هذه التفاعلات قصيرة جدا أو تتحول إلى علاقة عميقة تدوم عدة سنوات. وبعد أن يتمكن الجناة من ترسيخ علاقة الثقة الموهومة، يشرعون في التحايل على الضحية لدفعها إلى التنازل عن الأموال أو عن أصول أخرى.

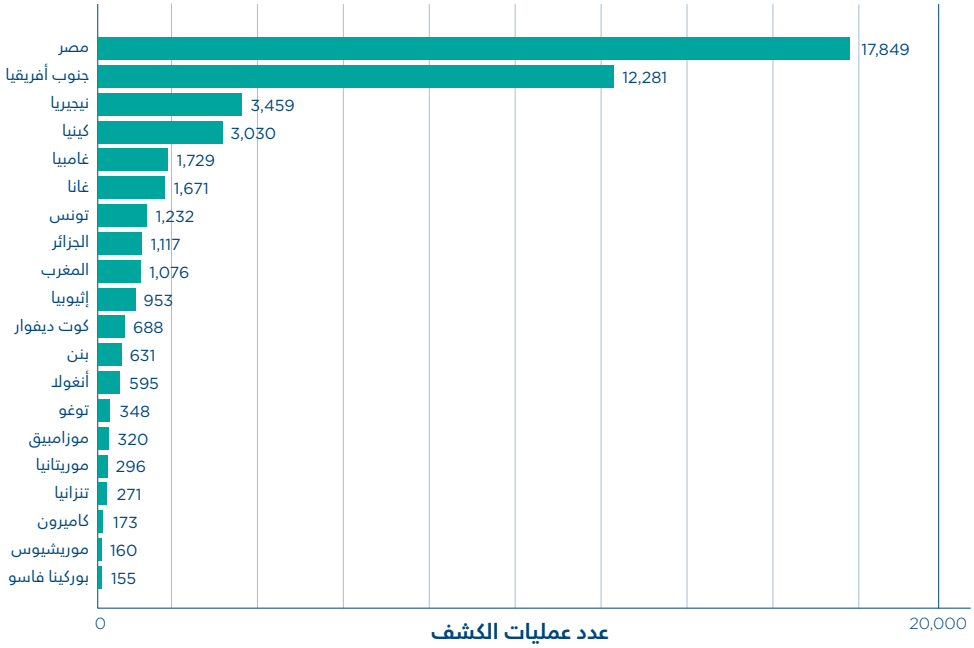
تُعتبر عمليات الاحتيال الرومانسية مصدر قلق واسع الانتشار في جميع أنحاء أفريقيا، حيث تفيد بعض المناطق عن مستويات أعلى منها. وبصورة خاصة، حُدّدت بلدان أفريقيا الغربية، بما في ذلك نيجيريا وغانا وكوت ديفوار وبنن، كالمناطق التي تنشط فيها شبكات الاحتيال الرومانسي بصورة خاصة.[16] ويتمثل أحد أبرز الاتجاهات الأخيرة في قيام الجناة بخداع الضحايا بوعود رومانسية، وإرغامهم بعد ذلك على استثمار الأموال في مخططات احتيالية متصلة بالعملات المشفرة.[17]

وأصبحت عمليات الاحتيال الرومانسي من بين أشكال الجرائم السيبرانية الأكثر ربحيةً، وتُلحق أضرارا عاطفية ومالية كبيرة. ففي إحدى أبرز القضايا في نيجيريا، قام أحد الجناة بتجميع 1.9 مليون دولار أمريكي من ضحايا مختلفين قبل أن يُصار إلى توقيفه.[18] وتكشف بيانات الإنتربول عن حالات عديدة حيث قام ضحايا أفريقيون متعددون بدفع الأموال للجناة، فيستنفدون أحيانا أموال معاشاتهم التقاعدية أو يراكمون الديون. وتبقى حالات عديدة غير مبلغ عنها بسبب شعور الضحية بالخجل والذنب والوصمة الاجتماعية، الأمر الذي يبيّن أن الأثر المالي الفعلي أكبر بكثير ممّا تشير إليه الوثائق الرسمية.[19] ونظرا إلى تزايد تعقيد وحجم هذه العمليات، تحتاج أجهزة إنفاذ القانون الأفريقية بشكل ملحّ إلى تدريب متخصص وتعزيز قدرات الأدلة الجنائية للتصدي بفعالية لهذا التهديد المتنامي والتحقيق فيه.

14 https://www.kaspersky.com/about/press-releases/kaspersky-reports-nearly-900-million-phishing-attempts-in-2024-as-cyber-threats-increase
15 https://cltc.berkeley.edu/2025/01/16/beyond-phishing-exploring-the-rise-of-ai-enabled-cybercrime
16 https://theconversation.com/online-romance-scams-who-nigeria-and-ghanas-fraudsters-are-how-they-operate-and-why-they-do-it-247916
17 https://www.reuters.com/world/africa/almost-800-arrested-over-nigerian-crypto-romance-scam-2024-12-16/
18 https://www.interpol.int/en/News-and-Events/News/2024/Arrests-in-international-operation-targeting-cybercriminals-in-West-Africa
19 https://www.knowbe4.com/hubfs/Online-Scams+Victims-Africa-report-2024.pdf

2.1.2. برمجيات انتزاع الفدية

في عام 2024، حدّدت البلدان الأعضاء في الإنتربول برمجيات انتزاع الفدية كأحد التهديدات السيبرانية الأكثر انتشارا في القارة الأفريقية، حيث تطرح خطرا متزايدا بالنسبة إلى الحكومات ومؤسسات الأعمال ومرافق الخدمات المهمة. وتشير البيانات الواردة من شركاء الإنتربول في القطاعين العام والخاص إلى أن عمليات كشف برمجيات انتزاع الفدية على أساس شهري ارتفعت عام 2024 مقارنة بالعام الماضي.[20] وهذه الهجمات مقلقة بصورة خاصة نظرا لتداعياتها المالية الكبيرة، وقدرتها على تعطيل البنية التحتية الحرجة بشكل شديد وللضرر الذي تلحقه بالمنظمات والأفراد المعرّضين لها. وتبيّن التقارير الواردة من شركات الأمن السيبري[21] ومن شركاء الإنتربول في القطاع الخاص أن جنوب أفريقيا ومصر واجها العدد الأكبر من الحوادث المتصلة ببرمجيات انتزاع الفدية، تليها اقتصاديات أخرى ذات مستوى مرتفع جدا من الرقمنة مثل نيجيريا وكينيا وغامبيا وتونس والمغرب والجزائر وإثيوبيا، وحتى أن دول أصغر حجما مثل بنن أفادت أيضا عن هجمات كبيرة، بما يؤكد على أن برمجيات انتزاع الفدية تشكل تحدٍّ على نطاق القارة، وبخاصة في البلدان التي تتمتع ببنية تحتية رقمية أكثر تطورا.



الرسم 5: أبرز 20 دولة أفريقية من حيث عدد اكتشافات تهديدات برامج الفدية خلال عام 2024، وفقًا لبيانات شركة ترند مايكرو.

وقد كانت التداعيات المالية لبرمجيات انتزاع الفدية في أفريقيا ملحوظة في عام 2024. فقد كانت بعض الحوادث متصلة بالسرقة الصريحة، مثل السرقة السيبرانية في شركة التكنولوجية المالية النيجيرية Flutterwave في نيسان/أبريل، التي أفادت عن تحويل مبلغ 7 مليون دولار أمريكي تقريبا.[22] وفي حالات أخرى، تراوحت مبالغ طلب الفدية بين عشرات الآلاف وملايين الدولارات، غالباً ما تُطلب بالعملات المشفرة، بما يؤدي إلى أعباء مالية كبيرة. علاوة على ذلك، أفضت عمليات تعطيل برمجيات انتزاع الفدية إلى خسارة الإيرادات وخفض الإنتاجية ووقف التجارة وتكاليف التعافي الكبيرة.

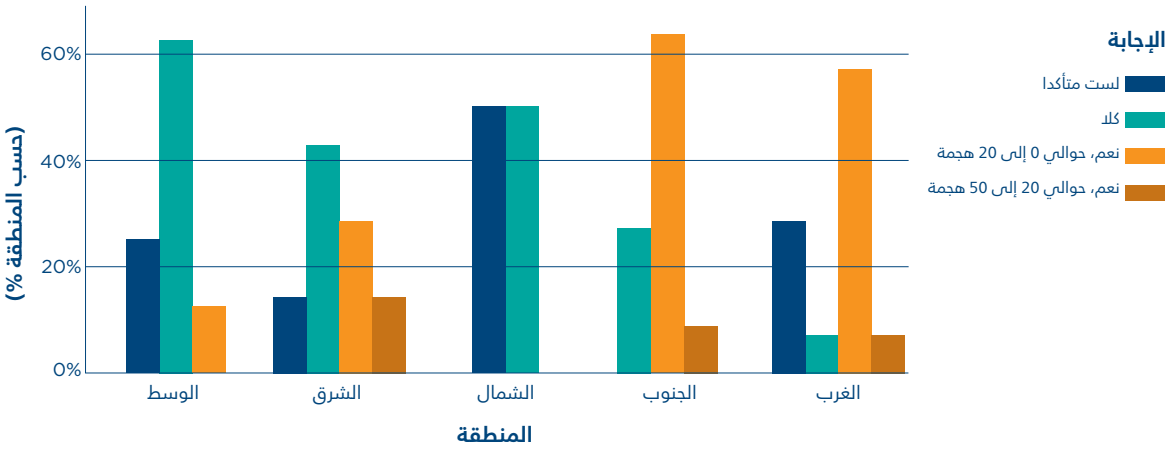
20 According to data provided by Trend Micro, 2024.

21 https://falconfeeds.io/blogs/cyber-attacks-in-africa-a-comprehensive-analysis-of-trends-from-january-to-august-2024-206317

22 https://africa.businessinsider.com/local/markets/fintech-giant-flutterwave-loses-naira11-billion-to-security-breach

وقد عطّلت المنشأة الكهربائية في كاميرون (ENEO) عمليات إدارة الطاقة في حين أن الخرق الذي حصل في هيئة الطرقات الحضرية في كينيا عرّض إلى الخطر البيانات الحيوية المتصلة بالبنية التحتية للطرقات.[23] وتضرّرت أيضا قواعد البيانات الحكومية، بما في ذلك عمليات القرصنة في كانون الأول/ديسمبر 2024 التي طالت هيئة المؤسسات المتناهية الصغر والصغيرة في كينيا والمكتب الوطني للإحصاءات في نيجيريا.[24] وفي جنوب أفريقيا، وقعت وزارة الدفاع ضحية مجموعة Snatch لبرمجيات انتزاع الفدية في أواخر عام 2024، حيث خسرت 1.6 تيرابايت من البيانات، بما في ذلك اتصالات رئيس البلاد.[25] وواجه قطاع الاتصالات اللاسلكية تهديدات مماثلة، مثل الخرق الذي استهدف شركة الاتصالات اللاسلكية في ناميبيا في أواخر عام 2024، حيث تعرّض إلى الخطر 626.3 جيغابايت من البيانات، بما في ذلك أكثر 492.000 ملف، مما أثّر على أكثر من 619.000 زبون.[26] وكشف هذا الاختراق عن معلومات حسّاسة خاصة بأفراد ومؤسسات أعمال وكيانات حكومية، الأمر الذي يشير إلى مخاطر كبيرة طالت خصوصية المواطنين والأمن الوطني معا.[27]

هجمات برمجيات انتزاع الفدية ضد البنية التحتية الحرجة (% حسب المنطقة)



الرسم 6: هجمات برمجيات انتزاع الفدية ضد البنية التحتية الحرجة حسب المنطقة (%)، وفقًا لردود الاستبيان المقدمة من الدول الأفريقية الأعضاء في الإنتربول خلال عام 2024.

وفقا للبيانات الواردة من شركاء الإنتربول في القطاع الخاص،[28] نشط العديد من مجموعات قرصنة في المنطقة الأفريقية في عام 2024. وكان أبرزها مجموعة LockBit، وهي عصابة منتشرة جدا في مجال برمجيات انتزاع الفدية كخدمة بقيت نشطة جدا طيلة العام. وتُعرَف مجموعة LockBit بأساليبها العدائية في الابتزاز المزدوج، حيث تقوم بتشفير شبكات الضحايا وتهديدهم في الوقت ذاته بنشر البيانات المسروقة، وقد أعلنت مسؤوليتها عن الهجوم الذي تعرّض له صندوق المعاشات التقاعدية للموظفين الحكوميين في جنوب أفريقيا في شباط/فبراير.[29] وارتبطت أيضا بحوادث عديدة في غرب أفريقيا.[30] ورغم أن السلطات ضبطت مؤقتا مواقع الإنترنت الأسود التابعة لمجموعة LockBit أثناء حملة دولية، سرعان ما عادت المجموعة إلى نشر بيانات الضحايا أو إعادة نشرها، الأمر الذي تسبّب بتعطيل ميداني خطير وبانتهاكات كبيرة للبيانات.[31] وأثّرت الهجمة على صندوق المعاشات التقاعدية للموظفين الحكوميين وحدها على ملايين الأشخاص، وسلّطت الضوء على المخاطر الكبيرة التي يطرحها النشاط المتواصل لمجموعة LockBit.

23 https://adforensics.com.ng/cyberattack-on-africas-top-organizations-2024
24 https://adforensics.com.ng/cyberattack-on-africas-top-organizations-2024
25 https://therecord.media/lockbit-ransomware-takes-credit-for-south-african-pension-fund-attack
26 https://neweralive.na/telecom-hit-by-massive-cyberattack-over-400-000-files-leaked
27 https://dailysecurityreview.com/news/namibia-ransomware-attack-sensitive-data-of-government-officials-and-citizens-leaked/
28 According to data provided by BI.ZONE, 2024.
29 https://therecord.media/lockbit-ransomware-takes-credit-for-south-african-pension-fund-attack
30 https://toptechgh.com/lockbit-ransomware-member-extradited-see-attacks-on-africa
31 https://therecord.media/lockbit-ransomware-takes-credit-for-south-african-pension-fund-attack

وتقوم جهة فاعلة بارزة أخرى في برمجيات انتزاع الفدية، (Hunters International Hunters)، باستهداف قطاع الاتصالات بصورة خاصة والحكومة والمؤسسات المالية.[32] وفي تموز/يوليو 2024، اخترقت Hunters هيئة الطرقات الحضرية في كينيا، وسرقت حوالي 18 جيغابايت من البيانات.[33] وسددت ضربة أخرى في كانون الأول/ديسمبر حيث هاجمت قطاع الاتصالات اللاسلكية في ناميبيا وسرّبت معلومات حساسة عن المستهلكين[34]. وتعتمد هذه المجموعة نهجا خفيا حيث تستخرج البيانات بكل هدوء قبل تشفير النظم؛ فالضحايا الذين يرفضون طلبات الفدية يتعرضون لتسريب البيانات الخاصة بهم علنا، الأمر الذي يسبّب تعطيل العمليات ويقوّض ثقة عموم الناس. وأمّا Blacksuit، وهي مجموعة تنشط في برمجيات انتزاع الفدية والابتزاز، معروفة باستهداف المنظمات الكبيرة في العالم، وقد أظهرت ضراوتها حين هاجمت مختبرات الصحة الوطنية في جنوب أفريقيا في حزيران/يونيو 2024[35]. وقد عطّلت هذه الحادثة الخطيرة عمليات التشخيص في ملايين الفحوصات الطبية، وأدّت إلى إلغاء قسري لعمليات جراحية مهمة وعرّضت إلى الخطر أكثر من تيرابايت واحد من البيانات الحساسة جدا، الأمر الذي يبيّن بصورة صارخة إمكانيات برمجيات انتزاع الفدية في تهديد صحة البشر وسلامتهم.

3.1.2. الاحتيال بالبريد الإلكتروني المهني

حدّدت البلدان الأعضاء في الإنتربول في أفريقيا الاحتيال بالبريد الإلكتروني المهني كأحد التهديدات السيبرانية الكبيرة والمتنامية ضمن المشهد الأوسع نطاقا لعمليات الاحتيال الإلكتروني. فالبيانات الواردة من شركاء الإنتربول من القطاع الخاص[36] تشير إلى زيادة حادة في النشاط الإجرامي السيبري المتصل بالاحتيال بالبريد الإلكتروني المهني في أفريقيا، من حيث حجم الهجمات وتداعياتها المالية معا. كما أن عددا كبيرا من الجناة الناشطين في مجال الاحتيال بالبريد الإلكتروني المهني يعملون في القارة، وبخاصة في غرب أفريقيا. ووفقاً للبيانات الواردة من شركاء الإنتربول في القطاع الخاص، تمثل 11 دولة أفريقية معظم النشاط في مجال الاحتيال بالبريد الإلكتروني المهني الحاصل في القارة، ويتركّز هذا النشاط في نيجيريا وغانا وكوت ديفوار وجنوب أفريقيا. وفي غرب أفريقيا، تطوّرت بعض المجموعات الإجرامية وأصبحت مؤسسات منظمة جدا تُقدّر قيمتها بعدة ملايين من الدولارات الأمريكية وقائمة على عمليات الاحتيال بالبريد الإلكتروني المهني. وتضم نقابة Black Axe عبر الوطنية آلاف الأعضاء من حول العالم، وهي مسؤولة عن عمليات احتيال مالي واسعة النطاق درّت المليارات من الأموال.[37]

وتشير البيانات المقدمة من الدول الأفريقية الأعضاء في الإنتربول إلى أنه في عام 2024، كان القطاع المالي الأكثر استهدافا في الدول الأفريقية الأعضاء. فقد انخرطت الشركات في التجارة الدولية والمعاملات المالية المتكررة، فيما كانت الشركات التي تقوم فيها ضوابط أمنية غير متطورة عرضةً لهجمات الاحتيال بالبريد الإلكتروني المهني. لكن لم تكن أي صناعة محصّنة ضد هذه الهجمات؛ ففقد تضررت المنظمات من جميع الأحجام، من الشركات الصغيرة والمتوسطة الحجم إلى المؤسسات الكبيرة. وإضافة إلى المصارف ومؤسسات التمويل المتناهي الصغر، أُفيد عن حوادث كبيرة في قطاعات مثل تجارة الاستيراد والتصدير، النفط والغاز، والمنتجات الصيدلانية، والنقل والتجارة الإلكترونية. وكانت تزداد أيضا الهجمات على المؤسسات الحكومية وعلى القطاع التطوعي والأفراد في جميع أنحاء القارة.

ومن الصعب بمكان الحصول على أعداد دقيقة لحوادث الاحتيال بالبريد الإلكتروني المهني في أفريقيا بفعل النقص في الإبلاغ، إنما تكشف مؤشرات عديدة عن حجم المشكلة. ففي عام 2024 وحده، أفاد 19 بلدا أفريقيا بشكل جماعي عن 10.490 عملية توقيف متصلة بالجريمة السيبرانية، ما يشير إلى أن العدد الفعلي لقضايا الاحتيال بالبريد الإلكتروني المهني أعلى بكثير، نظرا إلى أنه يتم الإبلاغ رسميا عن نسبة تُقدّر بـ 35 في المائة فقط من الجرائم السيبرانية.[38] وبرزت قضية هامة تبيّن الأثر العالمي للشبكات الأفريقية لمرتكبي الجرائم السيبرانية في تشرين الثاني/نوفمبر 2024، حين حكمت السلطات الأمريكية على Babatunde Ayeni، وهو مواطن نيجيري يبلغ من العمر 33 عاما، بالسجن لمدة 10 سنوات بتهمة إعداد مخطط واسع النطاق للاحتيال بالبريد الإلكتروني المهني يستهدف المعاملات العقارية.[39] وإذ كان يعمل انطلاقا من نيجيريا والإمارات العربية المتحدة، قام Ayeni وشركاؤه في المؤامرة بهجمات للتصيد الاحتيالي بهدف سرقة بيانات تسجيل الدخول إلى البريد الإلكتروني من محامين ووكلاء عقاريين في الولايات المتحدة. ثم انتحلوا صفة هؤلاء المهنيين لإعادة توجيه دفعات إغلاق الرهونات العقارية إلى حسابات احتيالية. ألحق هذا المخطط الأذى بأكثر من 400 ضحية وأفضى إلى سرقة 19.6 مليون دولار أمريكي، وقد أُرسل هذا المبلغ إلى حسابات يتحكم بها الجناة.[40] وتؤكد هذه القضية على الطبيعة العابرة للحدود للجرائم المتصلة بالاحتيال بالبريد الإلكتروني المهني وكيف تستغل الشبكات الأفريقية لمرتكبي الجرائم السيبرانية النظم المالية العالمية لخداع الضحايا من حول العالم.

32 وفقا للبيانات المقدمة من شركة BI.ZONE، 2024
33 https://www.darkreading.com/cyberattacks-data-breaches/ransomware-targeting-infrastructure-telecom-namibia
34 https://magedata.ai/securefact/securefact-cyber-security-news-week-of-december-23-2024
35 https://www.bitdefender.com/en-us/blog/hotforsecurity/ransomware-attack-on-blood-testing-service-puts-lives-in-danger-in-south-africa
36 وفقا للبيانات المقدمة من شركة Trend Micro، 2024
37 https://africacenter.org/spotlight/black-axe-nigeria-transnational-organized-crime
38 https://therecord.media/orion-carbon-black-bec-scam-millions
39 https://www.justice.gov/usao-sdal/pr/nigerian-national-sentenced-ten-years-20-million-cyber-fraud-scheme
40 https://www.justice.gov/usao-sdal/pr/nigerian-national-sentenced-ten-years-20-million-cyber-fraud-scheme

ومن حيث أساليب العمل، تشير البيانات الواردة من البلدان الأفريقية الأعضاء في الإنتربول إلى أن الهجمات بالاحتيال بالبريد الإلكتروني المهني في القارة تستفيد من الهندسة الاجتماعية والتصيد الاحتيالي وانتحال الهوية واختراق الشبكات للتلاعب بالمعاملات المالية. وتتمثل إحدى التكتيكات الشائعة بأوامر التحويل الاحتيالية، حيث يعمد مرتكبو الجرائم السيبرانية إلى انتحال هوية المدراء التنفيذيين أو الشركاء في مؤسسات الأعمال أو مسؤولين حكوميين لخداع الموظفين ودفعهم إلى تحويل الأموال. فعمليات الاحتيال بانتحال صفة رئيس مجلس الإدارة أو بتغيير التفاصيل في الحسابات المصرفية، وبخاصة في القطاع العام، هي من بين المخططات الأكثر إبلاغا عنها. كما أن التصيد الاحتيالي وسرقة بيانات التعريف هما الطريقتان الأكثر استخداما للوصول إلى الحسابات، حيث يستخدم بعض الجناة الهندسة الاجتماعية القائمة على تطبيق WhatsApp من خلال انتحال هوية بعض الأشخاص المعروفين. كما تتعلق حالات أكثر تطورا باختراق الشبكة، حيث تُنشر البرمجيات الخبيثة لمراقبة تبادل الرسائل عبر البريد الإلكتروني والتدخل في عمليات الدفع. ففي أفريقيا الغربية والجنوبية، كثيرا ما يستخدم الجناة مجالات مشابهة أو تعديلات طفيفة في عناوين البريد الكتروني لخداع الضحايا. وتنتشر أيضا عمليات الاحتيال المتصلة بعروض الأسعار والدفع، حيث يرسل الجناة طلبات احتيالية للحصول على أسعار أو يدعون بأنه تم تغيير تفاصيل الحساب المصرفي.

كذلك، تشير التقارير الواردة من البلدان الأعضاء في الإنتربول إلى أن استخدام الجريمة السيبرانية كخدمة يساهم في التطوير المتزايد للهجمات بالاحتيال بالبريد الإلكتروني المهني. فقد كشفت وحدة مكافحة الجرائم الرقمية في شركة مايكروسوفت عن زيادة بنسبة 38 في المائة في الجرائم السيبرية كخدمة التي تستهدف حسابات البريد الإلكتروني للمؤسسات بين عامي 2019 و2022.[41] وباتت الجهات الفاعلة المسؤولة عن التهديد قادرة اليوم على الوصول إلى مجموعات جاهزة للتصيد الاحتيالي، بما يتيح لها تنظيم العمليات بصورة كفؤة. كما أن منصات غير مشروعة، مثل BulletProofLink، تسهّل على نحو أكبر الحملات الواسعة النطاق للاحتيال بالبريد الإلكتروني المهني عن طريق تقديم خدمات شاملة، بما في ذلك النماذج والاستضافة والأتمتة.[42] وهذه المنصات تساعد الجناة أيضا على تجاوز التدابير الأمنية مثل التنبيهات التي تعرض عبارة "ممنوع الدخول" من خلال استغلال عناوين بروتوكول الإنترنت المحلية.
إضافة إلى ذلك، تمثل مخططات الاحتيال بالبريد الإلكتروني المهني القائمة على الذكاء الاصطناعي تهديدا ناشئا. فقد أصدر الإنتربول نشرة بنفسجية تحذر من الجناة الذين يسيئون استخدام الذكاء الاصطناعي وتكنولوجيا التزييف العميق لدعم عمليات الاحتيال[43]. والذكاء الاصطناعي التوليدي يسمح لمرتكبي عمليات الاحتيال بصياغة رسائل إلكترونية مقنعة وأكثر خصوصية تقلّد الأسلوب والأنماط اللغوية لبعض الأشخاص أو المؤسسات، في حين تُستخدم فعلاً تكنولوجيا التزييف العميق لانتحال هوية المدراء التنفيذيين في الاتصالات الهاتفية أو المصوّرة. ويطرح التطور السريع للذكاء الاصطناعي خطرا كبيرا من خلال توسيع نطاق الهجمات بالاحتيال بالبريد الإلكتروني المهني وتعزيز مصداقيتها، الأمر الذي يتطلب مراقبة عن كثب من جانب البلدان الأعضاء.

4.1.2. الابتزاز الجنسي الرقمي

الابتزاز الجنسي الرقمي هو فئة من فئات الاعتداء الجنسي المبني على الصور عبر الإنترنت تستخدم فيه الجهات الفاعلة المسؤولة عن التهديد صورا صريحة من الناحية الجنسية لابتزاز ضحاياهم من خلال التهديد بتسريب هذه الصور من دون موافقة الضحية المستهدفة. ويمكن أن تكون هذه الصور مشروعة، وقد تمّ الحصول عليها عن طريق الإكراه أو الخداع أو تمّ تشاركها بشكل طوعي، أو قد تكون ناتجة عن الذكاء الاصطناعي أو تمّ التلاعب بها رقميا.[44] وتكون عادة دوافع الابتزاز الجنسي مالية؛ إنما تشمل دوافع أخرى الانتقام وإكراه الضحية.

وقد ظهر الاعتداء الجنسي المبني على الصور عبر الإنترنت، وبخاصة الابتزاز الجنسي الرقمي، كإحدى أبرز الجرائم السيبرانية في أفريقيا في عام 2024، وتظهر البيانات الواردة من البلدان الأفريقية الأعضاء في الإنتربول زيادة كبيرة في التقارير عن الابتزاز الجنسي الرقمي، حيث أشار أكثر من 60 في المائة من البلدان إلى ارتفاع ملحوظ. ومن المرجح أن يعكس هذا الاتجاه تحوّلات أوسع في البيئة الرقمية في المنطقة. ونظرا للنقص الواسع الانتشار في التقارير المقدمة، وبخاصة في ظل جرائم من هذا الطابع، من المرجح أن يكون الحجم الفعلي أكبر بكثير. والأهم أن البيانات الحالية تستثني التقارير المقدمة من ضحايا من خارج المنطقة، ما يشير إلى أن التهديد قد يكون أكثر انتشاراً بعد وأكثر ترابطا على الصعيد العالمي ممّا تبيّنه الأرقام الإقليمية.

41 Microsoft (2023): https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW15yVe

42 _INTERPOL Africa Cyberthreat Assessment Report 2024: https://www.interpol.int/en/content/download/21048/file/24COM005030-AJFOC Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf

43 _INTERPOL Africa Cyberthreat Assessment Report 2024: https://www.interpol.int/en/content/download/21048/file/24COM005030-AJFOC Africa%20Cyberthreat%20Assessment%20Report_2024_complet_EN%20v4.pdf

44 https://www.trendmicro.com/vinfo/sg/security/definition/digital-extortion

وينعكس التأثير المتنامي للاعتداء الجنسي المبني على الصور عبر الإنترنت في إجراءات الإنفاذ الأخيرة التي وضعتها المنصات الكبيرة. ففي منتصف عام 2024، أزالت منصة Meta أكثر من 63.000 حساب إنستغرام و7.000 كيانا على فايسبوك كان مرتبطا بالابتزاز الجنسي الرقمي في نيجيريا.[45,46] وفي حين يبقى من غير الواضح متى تم تحديد هذه الحسابات للمرة الأولى، يشير حجم هذا الإجراء إلى تفاقم حاد في نشاط التهديد أو تصاعد الضغوط الخارجية على المنصات للاستجابة- وهما مؤشرات مهمان على نمو الجريمة. وكان العديد من هذه الحسابات مرتبطا بالشبكات المنظمة لمرتكبي الجرائم السيبرانية، وقد كان بعضها متورطا في تجنيد وتدريب جناة وتوزيع كتيّبات عملية لارتكاب جرائم جنسية رقمية.[47,48] وهذا يدل على تطور في التكتيك: بالفعل، يُستخدم الابتزاز الجنسي كسلاح وليس فقط كجريمة معزولة، إنما كتكتيك وتقنية وإجراء متكرر في البيئة التقليدية للاحتيال الإلكتروني. كما تشير بعض التقارير إلى أن هذه الشبكات قد تتداخل مع مجموعات للجريمة المنظمة قائمة منذ زمن طويل في أفريقيا الغربية، على الرغم من ضرورة تأكيد هذا الأمر.[49]

وإلى جانب التغييرات في مدى الاستهداف والحجم، برزت وسائل تهديد جديدة. ويفيد شركاء الإنتربول في القطاع الخاص إلى زيادة حادة في الرسائل الإلكترونية للتصيد الاحتيالي التي تُستخدم لإطلاق حملات ابتزاز جنسي.[50] إضافة إلى ذلك، ازدادت مخططات الابتزاز عن طريق الذكاء الاصطناعي، حيث تُستخدم صور فاضحة، أكانت مركّبة أو معدلة، لخداع الضحايا. وقد سُجل العدد الأكبر من هذه الحوادث في المغرب ومالي ومصر وموريتانيا، بما يشير إلى التوزيع الجغرافي. ويبيّن هذا التقارب بين التصيد الاحتيالي وأدوات الذكاء الاصطناعي والتكتيكات عملية تنظيم الابتزاز الجنسي؛ فهو لم يعد يقتصر على الجناة الانتهازيين إنما بات مترسخا بشكل متزايد في البنى التحتية الأوسع نطاقا للاحتيال.

ورغم أن جزءا كبيرا من النشاط المعروف في مجال الاعتداء الجنسي المبني على الصور عبر الإنترنت على منصات Meta قد طال ضحايا من بين البالغين، أشارت أجهزة إنفاذ القانون إلى ازدياد مقلق في القضايا التي تطال مراهقين من الفتيان والفتيات، بما في ذلك الموجودين منهم خارج منطقة أفريقيا.[51,52] وهذا التحوّل الظاهر في ديموغرافية الضحايا وتوسّع النطاق الجغرافي قد يشيران إلى تغيير في الاستراتيجية. كما أنه يثير أسئلة حرجة بشأن الدوافع التي توجه الابتزاز الجنسي الرقمي. وفي حين يبقى الابتزاز المالي هدفا أساسيا، من خلال التهديد بنشر صور فاضحة عادة، تشير بعض الحوادث إلى دوافع مترسخة في التلاعب النفسي والإكراه أو نيّة إلحاق الأذى بسمعة الضحية. وفي هذه القضايا، يمكن أن يستغل الجناة مواطن ضعف الضحية للسيطرة عليها عوضا عن تحقيق مكاسب نقدية. فالأثر النفسي على الضحايا يكون كبيرا جدا. وفي جنوب أفريقيا، أفادت السلطات عن ارتفاع عدد الضحايا من بين المراهقين، وتوفيت ضحية من البالغين انتحارا إثر حادث ابتزاز جنسي.[53] وفي مصر، تلقت منصة دعم رقمية أكثر من 2.500 مناشدة متصلة بالابتزاز الجنسي في عام 2024، وردت بصورة رئيسية من نساء وفتيات.[54,55] وتعكس هذه الأرقام أزمة خفية إنما واسعة الانتشار، حيث تستغل الجهات الفاعلة المسؤولة عن التهديد الخوف والوصمة والاضطراب العاطفي بشكل مستمر كجزء من أساليب السيطرة التي تعتمدها.

وردا على التهديد المتنامي، كثّفت أجهزة إنفاذ القانون جهودها، بما في ذلك تعزيز التنسيق الدولي والتعاون عبر الحدود والعمل مع منصات القطاع الخاص. إنما لا زالت القيود لجهة القدرات والتحديات المتصلة بالولاية القضائية القانونية والتأخير في الوصول إلى البيانات عبر الحدود تعيق التحقيقات. وبما أن الجناة والضحايا يتخطون الحدود الوطنية، تكافح أطر الإنفاذ القائمة لمواكبة هذا الواقع.

45 https://www.npr.org/2024/07/24/nx-s1-5050709/meta-sextortion-scams-nigeria-facebook-instagram
46 https://www.reuters.com/world/africa/facebook-removes-63000-accounts-nigeria-over-sextortion-scams-2024-07-24/
47 https://tuxcare.com/blog/sextortion-scams-63k-instagram-account-in-nigeria-removed
48 https://www.theverge.com/2024/7/24/24205236/meta-nigeria-financial-sextortion-scam
49 https://www.unodc.org/documents/organized-crime/tools_and_publications/21-05344_eBook.pdf
50 According to data provided by Trend Micro, 2024.
51 https://www.reuters.com/world/africa/facebook-removes-63000-accounts-nigeria-over-sextortion-scams-2024-07-24/
52 https://businesstech.co.za/news/internet/790431/extortion-syndicates-targeting-boys-in-south-africa
53 https://www.theguardian.com/uk-news/article/2024/aug/21/how-west-africas-online-fraudsters-moved-into-sextortion
54 https://allafrica.com/stories/202408190082.html
55 https://www.reuters.com/article/technology/feature-egyptian-women-find-help-online-to-fight-sextortion-threats

3. الاتجاهات والأفكار في مجال الجريمة السيبرانية عبر المناطق الفرعية الأفريقية

تتبع اتجاهات الجريمة السيبرانية عامة أنماطا متشابهة في القارة الأفريقية، حيث حُدّدت عمليات الاحتيال الإلكتروني وعمليات الاحتيال بالبريد الإلكتروني المهني والابتزاز الجنسي الرقمي كالتهديدات السيبرانية الأكثر خطورة. غير أن طابع هذه التهديدات وحجمها يختلفان مع اختلاف المناطق الفرعية المختلفة بسبب الاختلافات في البنية التحتية الرقمية وقدرات إنفاذ القانون وتكتيكات الجريمة السيبرانية. وينظر هذا القسم في الاتجاهات والتطورات السيبرانية الإقليمية في غرب أفريقيا وشرق أفريقيا وأفريقيا الوسطى وأفريقيا الجنوبية وشمال أفريقيا، بما يوفّر الأفكار حول كيفية تجلّي الجريمة السيبرانية في كل إقليم فرعي.

1.3 غرب أفريقيا

- تمثل نيجيريا وغانا وكوت ديفوار والسنغال حصة كبيرة من الاقتصاد الرقمي والنشاط السيبري في غرب أفريقيا.[56]

- ولا تشكل هذه الدول مراكز للابتكار التكنولوجي والخدمات المالية فحسب، إنما أيضا أهدافا رئيسية للتهديدات السيبرانية التي تعيد رسم ملامح البيئة الإجمالية للأمن السيبري في المنطقة.

- يبقى الاحتيال بالبريد الإلكتروني المهني أحد التهديدات السيبرانية الأكثر إضرارا من الناحية المالية، حيث تستهدف المجموعات القائمة في غرب أفريقيا الشركات على المستوى العالمي.

- كما تبقى برمجيات انتزاع الفدية أحد أكبر التهديدات السيبرانية، حيث يقوم مرتكبو الجرائم السيبرانية، وبخاصة الذين يعتمدون نموذج برمجيات انتزاع الفدية كخدمة، باستخدام منظمات أفريقية كمساحات لاختبار برمجيات خبيثة جديدة.[57] وتتّبع هذه الهجمات عادة نموذج الابتزاز المزدوج، عبر تشفير البيانات والتهديد بتسريب معلومات حساسة في الوقت ذاته إذا لم تُدفع الفديات.

- وتظل الهجمات الموزعة لحجب الخدمة مصدر قلق كبير في المنطقة. ففي النصف الأول من عام 2024، سجلت غانا 1.753 حادثا متصلا بالهجمات الموزعة لحجب الخدمة، ووصلت الهجمات في ذروتها إلى 314 جيغابايت في الثانية، مما جعلها من بين الأهداف الأولى في أفريقيا على مستوى الهجمات الموزعة لحجب الخدمة.[58]

- وشهدت عمليات الاحتيال بالمحفظة الإلكترونية ارتفاعا حادا. ويستعين مرتكبو هذه العمليات بتكتيكات الهندسة الاجتماعية لاختراق الحسابات والتماس أموال طارئة من أشخاص غير متنبهين. فعمليات الاحتيال بالمحفظة الإلكترونية، بما في ذلك عمليات الاحتيال باستبدال شرائح SIM وانتحال هوية شركة اتصالات، واسعة الانتشار، في حين تساهم سرقة الهوية في ارتفاع مخططات احتيال متصلة بالاستثمارات والمراهنات والتسوق الإلكتروني.

- كذلك، تزداد عمليات الاحتيال الرومانسي، حيث يتم ابتزاز الضحايا بتهديدهم بنشر معلومات حساسة. ويطال أحد الاتجاهات الأخيرة الجناة الذين يخدعون الضحايا في البداية بقطع وعود رومانسية عليهم ويرغمونهم بعدها على استثمار الأموال النقدية في مخططات احتيال عن طريق العملات المشفرة.

56 https://arxiv.org/html/2402.01649v1
57 https://www.darkreading.com/cyberattacks-data-breaches/criminals-test-ransomware-africa
58 https://toptechgh.com/ghana-hit-with-4753-ddos-attacks-netscout-threat-intelligence-report-1h-2024

2.3 شرق أفريقيا

- تبرز بلدان شرق أفريقيا، كينيا وأوغندا وتنزانيا ورواندا وإثيوبيا، بسرعة كمراكز تكنولوجية ومالية، من خلال الارتقاء بالتحوّل الرقمي إلى حد كبير. غير أن هذا التقدم يجعل منها أهدافا جذابة بشكل متزايد للتهديدات السيبرانية، ويلقي الضوء على الحاجة الملحة لوضع أطر متينة في مجال الأمن السيبري.

- وقد أصبحت إثيوبيا البلد الأكثر استهدافا في العالم في مجال التهديدات السيبرانية في عام 2024، واحتلت أعلى مرتبة على المستوى العالمي من حيث عمليات كشف البرمجيات الخبيثة.[59]

- وتُستهدف باستمرار البنية التحتية الحرجة، بما في ذلك المؤسسات الحكومية، والخدمات المالية والمشاريع الإنمائية الكبيرة.

- كما شهدت عمليات الاحتيال باستبدال شرائح SIM زيادة ملحوظة في أوغندا وتنزانيا. ويستغل المجرمون مواطن الضعف في شبكة الهواتف المحمولة من خلال استبدال شرائح SIM بصورة احتيالية، عن طريق الخداع أو التواطؤ مع أشخاص من الداخل في أغلب الأحيان، ما يسمح لهم باختطاف أرقام هاتف الضحايا.

- ويشكل الابتزاز الجنسي الرقمي تهديدا سيبريا متزايدا في شرق أفريقيا. ففي أحيان كثيرة، يستغل المجرمون المواد الفاضحة لابتزاز الضحايا، ويستهدفون بصورة خاصة النساء والشباب.

3.3 أفريقيا الوسطى

- تستغل الهجمات السيبرانية في أفريقيا الوسطى في أحيان كثيرة الحماية الضعيفة للبنية التحتية والنظم القديمة جدا.

- وتبقى عمليات الاحتيال عن طريق الهندسة الاجتماعية من بين الجرائم السيبرانية الأكثر إبلاغا عنها، حيث يستفيد الجناة من التكتيكات المخادعة مثل فرص التوظيف الزائفة وعمليات الاحتيال الرومانسي لاستغلال الضحايا غير المتنبّهين.

- وتواجه المؤسسات المالية هشاشة متنامية في وجه الاحتيال بالبريد الإلكتروني المهني وعمليات التسلل إلى الشبكة. وقد أفادت الكاميرون والغابون عن زيادة كبيرة في الهجمات السيبرانية التي تستهدف المؤسسات المالية، ما يفضي إلى خسائر كبيرة.

4.3 أفريقيا الجنوبية

- تُعرف منطقة جنوب إفريقيا بامتلاكها أحد أكثر أنظمة الأمن السيبراني تقدمًا في القارة، حيث تقوم بلدان مثل جنوب أفريقيا وناميبيا وبوتسوانا باستثمارات كبيرة في تدابير الأمن السيبري، والأطر القانونية الشاملة والتكنولوجيات الأمنية الموجهة بالذكاء الاصطناعي.

- وقد اعتمد مرتكبو الجرائم السيبرانية على أدوات تعمل بالذكاء الاصطناعي لاستحداث عمليات انتحال متطورة بالأصوات والأشرطة المصورة باستخدام التزييف العميق، ما يؤدي إلى تفاقم كبير للهجمات عن طريق هذه العمليات من خلال تقليد رؤساء مجلس الإدارة والبائعين في عام 2024.[60]

- وتبقى الهندسة الاجتماعية إحدى التكتيكات المحورية في عدة حوادث سيبرية، وغالبا ما تشكل نقطة الهجوم الأولى. كما استهدفت عمليات التصيد الاحتيالي عن طريق الرسائل النصية القصيرة بصورة خاصة عملاء المصارف، عن طريق رسائل خادعة لاختراق حسابات المستخدمين.

- ويستغل مرتكبو الجرائم السيبرانية بشكل متزايد اتجاهات التكنولوجيات المالية الناشئة، بما في ذلك العمليات المصرفية الرقمية والعملات المشفرة. وقد تزايد انتشار القرصنة لتعدين العملات المشفرة، حيث أفادت المؤسسات المالية عن نمو كبير في هذا النوع من الحوادث خلال عام 2024.

59 https://adforensics.com.ng/cyberattack-on-africas-top-organizations-2024/

60 https://qtatech.com/en/article/why-are-cyberattacks-increasingly-targeting-african-financial-institutions?srsltid=AfmBOoqghmt5QRlVko-UqiSdk8zjt99y1nHYR24zzh1vf63gxMYTk2a

5.3 غرب أفريقيا

- في عام 2024، واجهت بلدان أفريقيا الشمالية، بما في ذلك مصر والجزائر والمغرب وتونس وليبيا مشهداً لا يفتأ يتطور للتهديدات السيبرانية، بفعل الاتجاهات العالمية للجرائم السيبرانية والديناميكية الجيوسياسية الإقليمية.

- وكانت مصر والمغرب من بين دول أفريقيا الأكثر استهدافا بسبب الانتشار الواسع للإنترنت فيهما واقتصادهما الكبيرة. وشكلت مصر حوالي 13 في المائة من جميع الهجمات السيبرانية في القارة عام 2024، واحتلت المرتبة الثانية بعد جنوب أفريقيا.[61]

- وما زالت حوادث سيبرية عديدة تقوم على الهندسة الاجتماعية في جميع أنحاء شمال أفريقيا، وتتراوح بين عمليات الاحتيال العادية والهجمات المتطورة جدا. وكانت مؤسسات الأعمال تُستهدف في أحيان كثيرة بالتصيد الاحتيالي عن طريق البريد الإلكتروني المتكيف مع اللغة المحلية لتعزيز مصداقيتها. وتبقى عمليات الاحتيال عن طريق اليانصيب والاستثمارات منتشرة، حيث تم الإبلاغ عن حالات عدة تتعلق برسائل عبر تطبيق واتساب تَعِد بجوائز مزيفة أو فرص استثمار في عملات مشفرة احتيالية.

غرب أفريقيا	أفريقيا الجنوبية	شمال أفريقيا	شرق أفريقيا	أفريقيا الوسطى
لقد حوّل النمو الرقمي السريع- وبخاصة الأموال عبر الهواتف المحمولة ووسائل التواصل الاجتماعي- غرب أفريقيا إلى بؤرة ساخنة للجرائم السيبرانية. • تطغى عمليات الاحتيال بالبريد الإلكتروني المهني وبرمجيات انتزاع الفدية، حيث تقود مجموعات قائمة في نيجيريا مثل Black Axe و Opera1erعمليات الاحتيال العالمية. • وسجّلت غانا حوالي 5.000 من الهجمات الموزعة لحجب الخدمة في أوائل عام 2024، حيث استُهدف قطاع الاتصالات بشكل كبير. • وتزداد عمليات الاحتيال المتصلة بالمحفظات الإلكترونية والاحتيال الرومانسي، وغالبا ما ترتبط بمخططات العملات المزيفة. • وتشكل عمليات التصيد الاحتيالي والتزييف العميق المعززة بالذكاء الاصطناعي تهديدات متزايدة.	تضم الأمن السيبري الأكثر تطورا في أفريقيا، إنما تبقى تحت الحصار. • ازدادت عمليات الاحتيال عن طريق التزييف العميق وتسجيل الصور القائمة على الذكاء الاصطناعي في عام 2024. • وتبقى جنوب أفريقيا الهدف الأكبر، وبخاصة على مستوى المالية والحكومة. • وتنتشر على نطاق واسع عمليات الاحتيال عن طريق العملات المشفرة والهجمات بتسجيل الصوت التي تستغل نمو التكنولوجيات المالية.	ازدادت الهجمات السيبرانية في عام 2024، مدفوعة بالتوتر الجيوسياسي والتوسع الرقمي. • كانت مصر والمغرب من بين بلدان أفريقيا الأكثر استهدافا، حيث شكلت مصر نسبة 13 في المائة من جميع الهجمات. • عمليات الاحتيال باستخدام الهندسة الاجتماعية والتصيد الاحتيالي، عن طريق تطبيق واتساب والاستثمارات المزيفة في أغلب الأحيان، منتشرة على نطاق واسع.	يفوق التوسع الرقمي جهوزية الأمن السيبري. • احتلت إثيوبيا المرتبة الأولى في العالم على مستوى عمليات الكشف عن البرمجيات الخبيثة في عام 2024، حيث تتعرض البنية التحتية الحرجة إلى الخطر. • وتزداد عمليات الاحتيال عن طريق استبدال شرائح SIM في أوغندا وتنزانيا. • ويصبح الابتزاز الجنسي والتحرش عبر الإنترنت، الذي يستهدف بصورة خاصة النساء والشباب، شائعا على نحو متزايد.	نظرا للمعرفة الرقمية المتدنية والبنية التحتية الضعيفة، تصبح المنطقة معرّضة للخطر. • شهدت الكاميرون تضاعف عدد الحوادث السيبرانية في عام 2024. • وتزداد عمليات الاحتيال عن طريق العملات المشفرة والهندسة الاجتماعية. • وتواجه المؤسسات المالية زيادة في عمليات الاحتيال بالبريد الإلكتروني المهني والهجمات عبر الشبكة، إنما تبقى قضايا عدة من دون حلّ بفعل محدودية القدرات في مجال الأمن السيبري.

الجدول 1: لمحة عامة عن الاتجاهات والمعلومات المتعلقة بالتهديدات السيبرانية في مختلف المناطق الفرعية في أفريقيا

61 https://global.ptsecurity.com/analytics/cybersecurity-threatscape-for-african-countries-q1-2023-q3-2024

4. التحديات المتصلة بمكافحة الجريمة السيبرانية في أفريقيا

1.4 الأطر القانونية والسياسية المجزّأة

ما زالت الجريمة السيبرانية تفوق النظم القانونية المصمّمة لتوقيفها. ونظرا إلى أن 65 في المائة من البلدان أفادت عن عدم وجود أي تحديثات لتشريعاتها المتصلة بمكافحة الجريمة السيبرانية في العام الماضي، في حين اعتبر أكثر من 75 في المائة من البلدان أن أطرها القانونية وقدراتها في مجال الملاحقة القضائية بحاجة إلى التحسين، ثمة أدلة واضحة على وجود ثغرات قانونية منهجية.[62]

وبهدف التصدي لهذه التحديات، يوفّر العديد من الصكوك الدولية والإقليمية أطرا لتعزيز التشريعات المتصلة بمكافحة الجريمة السيبرانية:

- **اتفاقية بودابست لمكافحة الجريمة السيبرانية:**[63] توفّر خطوطا توجيهية شاملة، بما في ذلك المادة 19 التي تحدّد الصلاحيات للوصول إلى البيانات ومصادرتها. وقد صادقت ستة بلدان أفريقية فقط عليها حتى تاريخه.
- **اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية:**[64] ترمي إلى تعزيز التعاون الدولي في مكافحة الجريمة السيبرانية، وتحظى بدعم متزايد في جميع أنحاء أفريقيا.
- **اتفاقية مالابو للاتحاد الأفريقي:**[65] تركّز على الأمن السيبري وحماية البيانات الشخصية؛ إنما صادقت عليها 15 دولة عضو فقط في الاتحاد الأفريقي حتى تاريخه.

وتلقي هذه الثغرات الضوء على الحاجة المتنامية للمواءمة مع الأطر القانونية الدولية- وهذه مسألة يتم استكشافها بمزيد من التفصيل في الفصل 6.

2.4 القيود على القدرات والإمكانيات

تشكل القوانين القوية جزءا فقط من الحل- بالفعل، تكافح معظم البلدان أيضا لإنفاذها. وتبيّن نتائج الدراسة الاستقصائية أن **90 في المائة من البلدان المجيبة** تعتبر أن قدراتها في مجال إنفاذ القانون والملاحقة القضائية بحاجة إلى بعض التحسين أو إلى تحسين كبير.

وتشمل القيود الأكثر شيوعا:

احتياجات التدريب: أفاد 95 في المائة من البلدان عن تدريب غير ملائم وغير متسق أو تدريب يعتمد على الجهات المانحة.

- **القيود على الموارد:** 95 في المائة من البلدان.
- **الوصول إلى أدوات متخصصة:** 95 في المائة من البلدان.
- **الثغرات في المهارات الفنية:** 74 في المائة من البلدان.
- **الثغرات في البنية التحتية:** 72 في المائة من البلدان.
- **الحواجز التشغيلية:** يواجه 58 في المائة من البلدان حواجز بيروقراطية وقانونية ومؤسسية في وجه التحقيقات الفعالة.

ورغم تزايد عدد الحالات، لا زالت معظم البلدان تفتقر إلى البنية التحتية الأساسية لمكافحة الجريمة السيبرانية:

- لدى **30 في المائة** من البلدان نظام للإبلاغ عن الحوادث.
- يستخدم **28 في المائة** من البلدان نظاما لإدارة الحالات.
- لدى **19 في المائة** من البلدان قاعدة بيانات للمعلومات الاستخباراتية عن التهديدات السيبرانية.
- لدى **29 في المائة** من البلدان مستودع للأدلة الرقمية.

إضافة إلى ذلك، لا تمتلك سوى قلة من المؤسسات الوطنية الموارد البشرية أو الفنية الكافية للاستجابة الفورية. وغالبا ما تتجاوز التكنولوجيا الإجرامية القائمة على السحابة، ومنصات المراسلة المشفرة والتحقيقات الدولية الإمكانيات الفنية والإجرائية للفِرَق المحلية.

62 INTERPOL Cyberthreat Assessment Survey

63 https://www.coe.int/en/web/cybercrime/the-budapest-convention

64 https://www.unodc.org/unodc/en/cybercrime/convention/home.html

65 African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention) https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

3.4 التهديدات الناشئة والتكتيكات المتطورة

باتت حصة متزايدة من الجرائم السيبرانية في أفريقيا مدعومة بأدوات وتكتيكات جديدة- وبخاصة تلك التي تتعلق بالذكاء الاصطناعي ووسائل الإعلام المركبة والمعلومات المضلّلة. وتتجاوز هذه التهديدات المتطورة قدرات العديد من الأجهزة الوطنية في مجال كشفها والتحقيق فيها أو احتوائها.

- **عمليات التزييف العميق والابتزاز التي يولّدها الذكاء الاصطناعي.**
وفي بلدان عديدة، لجأ المجرمون إلى استنساخ مقاطع مصوّرة أو مسجلة لابتزاز الضحايا. وهذه الأدوات الموجّهة بالذكاء الاصطناعي تمّكن من إجراء عمليات مقنِعة في انتحال الهوية، والتلاعب العاطفي والابتزاز- ولا تتطلب في أغلب الأحيان مهارات فنية متطورة.

- **حملات لمكافحة المعلومات المضلّلة**
أفادت بعض الأجهزة عن حالات استُخدمت فيها الأخبار الملفقة والصور المعدّلة والحسابات المزيفة على وسائل التواصل الاجتماعي لنشر الذعر والتحريض على الاضطرابات أو إلحاق الأذى بالسمعة. وتستهدف هذه الهجمات عادة الثقة- عبر استخدام قنوات الإعلام العامة كسلاح.

- **تعزيز البنية التحتية للهجوم الجاهز**
تُستخدم مرافق الاستضافة المضادة للرصاص بشكل متزايد لدعم العروض المتصلة باستخدام البرمجيات الإجرامية كخدمة، ممّا يعطي الجهات الفاعلة المتدنية المهارات إمكانية الوصول إلى مجموعات التصيد الاحتيالي، وحمولات البرمجيات الخبيثة والأتمتة القابلة للتطوير التي تستضيفها البنية التحتية المصمّمة للتهرّب من المداهمة.

ورغم هذه التهديدات التي تتطور بسرعة، تبيّن أن 86 في المائة من الأجهزة المشاركة في الاستبيان لم تدمج بعد الذكاء الاصطناعي في عملياتها لإنفاذ القانون.[66] وفيما يسخّر الجناة الذكاء الاصطناعي لتعزيز حجم العمليات والخداع، يمكن أن تترك هذه الثغرات في القدرات العديد من الأجهزة الوطنية خلف الركب.

4.4 محدودية التعاون عبر الحدود وتشارك المعلومات الاستخباراتية

الجرائم السيبرانية تعبر الحدود بشكل روتيني، إنما يواجه معظم البلدان الأفريقية التحديات في مجال التعاون الدولي. وفي الدراسة الاستقصائية التي أجريناها، ذكر 86 في المائة من الأجهزة أن قدراتها في مجال التعاون عبر الحدود بحاجة إلى التحسين، حيث صنّف 44 في المائة منها هذه القدرات على أنها بحاجة إلى تحسين كبير.

وأُفيد عن العديد من القيود الرئيسية:

- **العمليات البطيئة والرسمية:** غالبا ما تكون الإجراءات، مثل طلبات المساعدة القانونية المتبادلة وتسليم المجرمين، بطيئة جدا ولا تتماشى مع السرعة المطلوبة للاستجابة بفعالية للجرائم السيبرانية، الأمر الذي يؤكد على ضرورة وضع أطر تعاون أكثر مرونة وتبسيطا.

- **أوجه عدم التطابق القانونية والإجرائية:** تولّد الاختلافات في القوانين، ومعايير الأدلة الرقمية واللوائح المتصلة بخصوصية البيانات احتكاكا عند العمل عبر الولايات القضائية. ويتم تناول هذه المسائل القانونية بمزيد من التفصيل في القسم 4.1.

- **بناء الشبكات الميدانية والثقة**: تواجه بعض البلدان التحديات في تحديد النظراء الأجانب أو التواصل معهم، وقد توجد اتصالات قائمة محدودة أو أطر تنسيق في الوقت الفعلي، الأمر الذي يمكن أن يؤدي أحيانا إلى تضييع فرص العمل المشترك.

- **وصول محدود إلى المنصات والبيانات التي تستضيفها مواقع أجنبية:** تفيد الأجهزة عن صعوبة في الحصول على المعلومات من منصات أو مقدمي خدمات توجد مقارهم الرئيسية في الخارج، وبخاصة في القضايا التي تعني مواطنين أجانب أو بنية تحتية موجودة في ولايات قضائية أخرى.

إنما رغم هذه الحواجز، تبيّن العمليات الأخيرة الذي جرى تنسيقها في إطار مشروع الإنتربول للعملية المشتركة لمكافحة الجريمة السيبرانية في أفريقيا أنه حين تتواجد قنوات موثوقة وبروتوكولات مشتركة، يمكن أن تكون الاستجابات الإقليمية للجرائم السيبرانية سريعة وفعالة.

66 INTERPOL Cyberthreat Assessment Survey

5.4 العوائق في وجه الشراكات بين القطاعين العام والخاص ومساءلة المنصة

تعتمد التحقيقات في مجال الجريمة السيبرانية بشكل متزايد على التعاون من جانب الشركاء في القطاع الخاص، وعلى وجه الخصوص المنصات التكنولوجية ومقدمي خدمات الاتصالات والمؤسسات المالية. غير أن معظم الأجهزة الأفريقية لإنفاذ القانون تواجه عوائق كبيرة لجهة بناء هذه العلاقات.

- **قنوات غير واضحة للمشاركة**
غالبا ما تكافح الأجهزة للوصول إلى بيانات من شركات مثل Meta و TikTokو Snapchat، وتذكر غياب الاتصالات المباشرة، وأوقات الاستجابة البطيئة والإجراءات غير الواضحة. فمن دون اتفاقات أو نقاط اتصال رسمية، غالبا ما يتم تأخير الطلبات أو تجاهلها.

- **انخفاض الاستعداد المؤسسي**
أبرمت بلدان قليلة مذكرة تفاهم أو اتفاقات لتشارك البيانات مع شركات خاصة. وفي الوقت ذاته، تفتقر عدة أجهزة إلى القدرات الفنية أو القانونية لتقديم طلبات فعالة وقانونية.

- **عدم مشاركة قطاعات الاتصالات والتكنولوجيات المالية على نحوٍ كاف**
رغم دورها المحوري في عمليات الاحتيال- مثل استبدال شرائح وإساءة استخدام الأموال عبر الهواتف المحمولة- تبقى الاتصالات ومقدمي الخدمات المالية من بين الشركاء غير المستغَلين بالكامل في الاستراتيجيات الوطنية لمكافحة الجريمة السيبرانية.

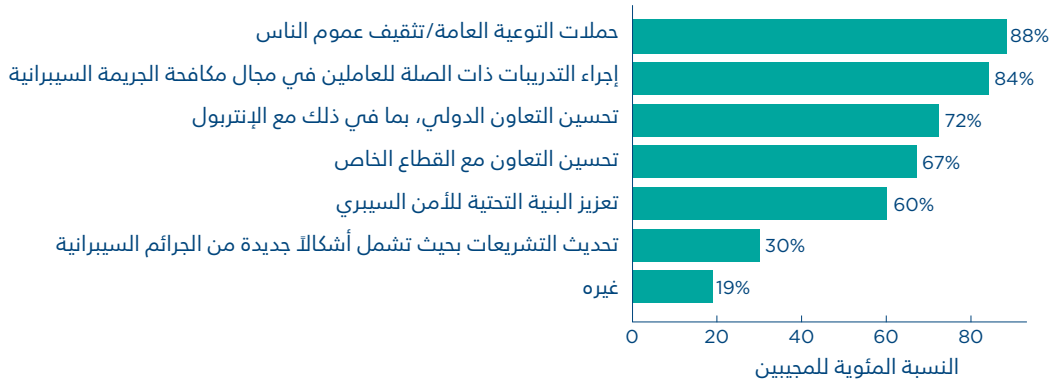
← تشير بيانات الاستبيان إلى أنّ 89 في المائة من البلدان الأفريقية صنّفت تعاونها مع القطاع الخاص على أنها بحاجة إلى تحسين ملحوظ أو بعض التحسين.[67]

وفيما تتحكم الكيانات الخاصة بالبنية التحتية الرقمية بشكل متزايد، سوف تعتمد قدرة أجهزة إنفاذ القانون على العمل أكثر فأكثر على إمكانية الوصول والثقة والتعاون المنظّم- ولا يمكن ترك أي من هذه العناصر للصدفة.

67 INTERPOL Cyberthreat Assessment Survey

5. التطورات الإيجابية في مشهد الأمن السيبري في أفريقيا

أحرزت أفريقيا تقدما ملحوظا في الأمن السيبري، مدفوعا بالإصلاحات القانونية والتطورات في الأدلة الجنائية ومبادرات التوعية العامة والتعاون الإقليمي واعتماد التكنولوجيات الناشئة. وتبيّن هذه التطورات التزاما متزايدا بمكافحة الجريمة السيبرانية وتعزيز الأمن القومي عبر القارة.



الرسم 8: الإجراءات الوقائية لمكافحة الجريمة السيبرانية التي اتخذتها أجهزة إنفاذ القانون في أفريقيا في عام 2024.

1.5 تعزيز الأطر الوطنية لمكافحة الجريمة السيبرانية

في عام 2024، ارتقت دول أفريقية عديدة بأطرها القانونية لمكافحة الجريمة السيبرانية، بما يعكس التزاما متزايدا بالأمن الرقمي.

- أصبحت **تونس** الطرف السبعين في اتفاقية بودابست لمكافحة الجريمة السيبرانية في آذار/مارس 2024، وعمدت إلى مواءمة إطارها القانوني مع المعايير الدولية لتيسير التعاون عبر الحدود في مجال مكافحة الجريمة السيبرانية.

- سنّت **نيجيريا** قانون مكافحة الجرائم السيبرانية (منعها والوقاية منها، إلخ.) في عام 2024، وأدخلت تعديلات على تشريعاتها لعام 2025. وتضم التغييرات الرئيسية تشكيل أفرقة التصدي للطوارئ الحاسوبية، وتوضيح الأحكام المتصلة بالتحرش الإلكتروني واعتماد رسم الأمن السيبري من أجل تمويل المبادرات الوطنية.[68]

- وقدّمت **غامبيا** إلى البرلمان قانونها الأول المخصص لمكافحة الجريمة السيبرانية (2023)، واتخذت بذلك خطوة أساسية باتجاه إضفاء الطابع الرسمي على نهجها إزاء مكافحة الجريمة السيبرانية.[69]

- وأعدت **غينيا-بيساو** استراتيجيتها الوطنية لمكافحة الجريمة السيبرانية في عام 2024[70] وخطت أيضا خطوات مهمة في جهودها الأوسع نطاقا في مجال التحول الرقمي. وفي كانون الثاني/يناير 2025، أطلقت الحكومة رسميا الاستراتيجية الوطنية للتحول الرقمي، التي تهدف إلى تحسين التنمية الاقتصادية وإدارة البيانات والحوكمة والخدمات العامة.[71]

- وأصدرت **بوركينا فاسو** القانون رقم 2024-014/ALT في تموز/يوليو 2024، الذي يعزز حماية نظم المعلوماتية ويدوّن الاستجابات للتهديدات السيبرانية بما في ذلك برمجيات انتزاع الفدية والاحتيال الإلكتروني.[72]

وتشير هذه الجهود التشريعية إلى اتجاه إقليمي باتجاه تحقيق اتساق القوانين المتصلة بالأمن السيبري مع المعايير الدولية، بما في ذلك الإشارات إلى اتفاقية بودابست واتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية.

68 https://placng.org/i/documents/cybercrimes-prohibition-prevention-etc-amendment-act-2024/
69 https://mocde.gov.gm/ministry-of-communications-and-digital-economy-of-the-gambia-embarked-on-a-two-day-retreat-to-discuss-the-cybercrime-bill-2023/
70 INTERPOL Cyberthreat Assessment Survey
71 https://unu.edu/egov/news/digital-transformation-project-guinea-bissau-egov-undp
72 https://www.mdenp.gov.bf/fileadmin/user_upload/storages/documents/administratifs/loi_014_systeme_d_information.pdf

2.5 تعزيز الإمكانيات المؤسسية والفنية

خلال الأشهر الـ 18 الماضية، خطت الدول الأفريقية خطوات كبيرة على مستوى تعزيز إمكانياتها لمواجهة الجريمة السيبرانية. وقد اضطلعت الاستثمارات في الوحدات المتخصصة، والبنية التحتية للأدلة الجنائية الرقمية وتنمية القدرات دورا محوريا في تعزيز التحقيق وإنفاذه.

- وفقا للردود الواردة في الدراسة الاستقصائية،[73] أفاد **67 في المائة** من البلدان المشاركة عن تنظيم فعاليات لبناء القدرات المتصلة بمكافحة الجريمة السيبرانية في عام 2024، في حين أعلن **44 في المائة** منها أنها استحدثت وحدات لمكافحة الجريمة السيبرانية، أو وسّعت نطاق الوحدات القائمة.

- **الجزائر:** في أواخر عام 2023، فتحت الجزائر مقرا رئيسيا جديدا للوحدة المركزية لمكافحة الجريمة السيبرانية، ووسّعت العمليات في الولايات الـ 58 كلها. وباتت الوحدات الآن مجزّأة حسب الوظيفة- المراقبة والدعم الفني والتحقيقات- الأمر الذي يبسّط الإنفاذ. كما أن التدريب الجاري يوطّد هذه الإصلاحات الهيكلية.[74]

- **سيشيل:** تلقّت قوة الشرطة في سيشيل في الأشهر الـ 18 الماضية مجموعة من الأدوات الرقمية ومعدات التدريب من الحكومة البريطانية[75] ومختبرا للأدلة الجنائية الرقمية كهبة من الحكومة الصينية،[76] بعد فترة قصيرة من إنشاء الوحدة الخاصة بمكافحة الجريمة السيبرانية عام 2023[77]. وترمي الأدوات الجديدة إلى تحسين التحقيقات السيبرانية وجودة معاملة الأدلة الرقمية.

- **بنن:** أنشأت الحكومة المركز الوطني لمكافحة الجريمة السيبرانية (المركز الوطني للتحقيقات الرقمية) لتجميع التحقيقات في الجريمة السيبرانية والأدلة الجنائية الرقمية في مركز واحد.[78] وفي آب/أغسطس 2024، أعلن المركز الوطني لمكافحة الجريمة السيبرانية تفكيك شبكة كبيرة لمرتكبي الجرائم السيبرانية في كومي، ما يبيّن فعاليته التشغيلية.[79]

- **توغو:** في إطار الاستراتيجية الوطنية للأمن السيبري للفترة 2024-2028، تنكب توغو على توطيد استجابتها للجريمة السيبرانية من خلال إنشاء كيان موحّد لإنفاذها،[80] وفتحت مختبرا جديدا للأدلة الجنائية الرقمية وتواصل الاستثمار في التدريب الفني لموظفي التحقيق.

- **الكونغو:** في أواخر عام 2024، نظمت الحكومة تدريبا متخصصا للموظفين القضائيين وموظفي إنفاذ القانون، وقد شمل عملية جمع الأدلة الرقمية وتقنيات التحقيق في الجريمة السيبرانية.[81]

وتعكس هذه التطورات تحولا أوسع في القارة من الاستجابات المجزأة أو المخصصة إلى مكافحة الجريمة السيبرانية على نحو أكثر تنظيما وبموارد أفضل وقائم على التكنولوجيا بشكل متزايد. كما أن الاستثمار المتواصل في البنية التحتية وتطوير القوة العاملة والتنسيق بين الأجهزة ستكون عناصر مهمة لإدامة هذه المكاسب وتوسيع نطاقها.

73 INTERPOL Cyberthreat Assessment Survey
74 https://www.horizons.dz/?p=74105
75 http://www.seychellesnewsagency.com/articles/19082/British+government+donates+digital+tech+to+Seychelles+Police+Force+for better+training+and+results+
76 http://www.seychellesnewsagency.com/articles/19616/China+gifts+Seychelles+Police+Force+digital+forensic+lab+to+help+deal+with+cybercrime
77 https://www.nation.sc/articles/16639/cybercrime-unit-in-the-offing--by-vidya-gappy
78 https://cybersecuritymag.africa/benin-renforce-lutte-contre-cybercriminalite-avec-creation-du-cnin
79 https://cybersecuritymag.africa/index.php/le-cnin-demantele-un-vaste-reseau-de-cybercriminels-come-au-benin
80 https://www.togofirst.com/en/justice/2805-14118-togo-to-set-up-single-center-to-fight-cybercrime
81 https://www.wearetech.africa/en/fils-uk/news/tech/congo-hosts-cybersecurity-training-for-judicial-and-law-enforcement

3.5 زيادة القدرة على الصمود في المجال السيبري من خلال التوعية العامة

في عام 2024، أفاد 88 في المائة من البلدان الأفريقية عن إطلاق حملات للتوعية العامة أو مبادرات تثقيفية ترمي إلى منع الجريمة السيبرانية، ويكون بذلك الإجراء الوقائي الأوسع انتشارا في القارة.

وتستهدف هذه المبادرات عادة المجموعات الهشة مثل الطلاب والشباب وأصحاب المؤسسات الصغيرة والمواطنين الأكبر سنا، باستخدام طرق تواصل متنوعة بما في ذلك محطات التلفزيون الوطنية، والإذاعة ووسائل التواصل الاجتماعي، والتنبيهات عن طريق الرسائل النصية القصيرة والبرامج المدرسية.

1. حملات موجهة للشباب والمدارس

يبقى استهداف الشباب محور تركيز استراتيجي لبلدان عديدة، بما يروّج للسلامة الإلكترونية والتوعية على التنمّر على الإنترنت ومحو الأمية الرقمية.

- **إسواتيني:** نظّمت وزارت المعلومات والاتصالات، بالتعاون مع هيئة الاتصالات في إسواتيني واليونسكو، دورات للتوعية على الأمن السيبري في المدارس.[84,83,82]
- **جنوب أفريقيا:** استضاف معهد المتخصصين في تكنولوجيا المعلومات في جنوب أفريقيا، من خلال مجموعة الاهتمام الخاص المعنية بالأمن السيبري التابعة له، أوّل محكمة صورية للأمن السيبري في Gqeberha. وقدم طلاّب في الثانوية حجا بشأن قضية وهمية للتنمر السيبري أمام لجنة قضاة، بما يهدف إلى تعميق فهمهم للضرر الرقمي وإيجاد حلول سياسية على مستوى المدرسة.[85]
- **المغرب:** تولّت الشرطة قيادة برامج توعية في المدارس بالشراكة مع وزارة التعليم، وفي أيار/مايو 2024، وحضر أكثر من 2.2 مليون شخص الأيام الوطنية المفتوحة التي نظمتها المديرية العامة للأمن الوطني في أغادير، والتي تضمنت عروض عن الجريمة السيبرانية وشارك فيها طلاّب من 845 مدرسة وشهدت إطلاق منصة E-Blagh للإبلاغ عن الجرائم السيبرانية.[87,86]
- وتطبق منظمات المجتمع المدني مثل Child Online Africa[88] و Better Internet for Kids[89] برامج مثل يوم الإنترنت الآمن في أفريقيا (Safer Internet Day Africa)، ومسابقة السلامة والرفاه على الإنترنت (Online Safety and Wellbeing Competition) وأسبوع المعرفة الرقمية، التي تستهدف المدارس والأهالي والمؤسسات الدينية.

2. وسائل الإعلام ومشاركة وسائل التواصل الاجتماعي

بهدف الوصول إلى أكبر عدد من الأشخاص، تعتمد البلدان بشكل متزايد على منصات التواصل الاجتماعي ومنصات الإعلام التقليدية لتوجيه الرسائل بشأن الوقاية من الجريمة السيبرانية.

- **غانا:** في تشرين الأول/أكتوبر 2024، أطلقت هيئة الأمن السيبري الشهر الوطني للتوعية على الأمن السيبري بعنوان "مكافحة المعلومات المضلّلة/المعلومات الكاذبة في ديموقراطية رقمية قادرة على الصمود- مسؤوليتنا المشتركة". وتخلّل الحملة تواصل إعلامي على مستوى الدولة، ومنتديات إقليمية وجهود لتثقيف عموم الناس في مجال بناء القدرة على الصمود قبل الانتخابات الوطنية.[90]
- **رواندا:** نظمت الهيئة الوطنية للأمن السيبري الحملة السنوية " Tekana Online" طيلة شهر تشرين الأول/أكتوبر 2024. واستعانت هذه المبادرة بالتلفزيون والإذاعة ووسائل التواصل الاجتماعي لتثقيف الأفراد والأسر والمنظمات على أفضل الممارسات لمواجهة التهديدات السيبرانية مثل الاحتيال الإلكتروني وبرمجيات انتزاع الفدية والتصيد الاحتيالي.[91]
- **الإنتربول:** في كانون الأول/ديسمبر 2024، نظّم الإنتربول حملة #Thinktwice على جميع منصات التواصل الاجتماعي الخاصة به. وركّزت الحملة على إذكاء الوعي للتهديدات الإلكترونية، بما في ذلك برمجيات انتزاع الفدية والتصيد الاحتيالي والعمليات الاحتيالية التي يُستخدم فيها الذكاء الاصطناعي التوليدي، لتشجيع المستخدمين على اتخاذ قرارات مستنيرة على الإنترنت.[92]

82 https://independentnews.co.sz/10470/local-news/cybersecurity-awareness-initiative-hits-schools/
83 https://www.facebook.com/story.php?id=100069400350741&story_fbid=850193827303955&
84 https://www.swazilandnews.co.za/fundza.php?nguyiphi=7578&
85 https://www.itweb.co.za/article/iitpsa-sigcyber-raises-awareness-on-cyber-bullying-at-inaugural-moot-court-event/6GxRKqYQrnmqb3Wj
86 https://www.mapnews.ma/fr/actualites/social/jpo-de-la-dgsn-un-nombre-record-de-2120000-visiteurs
87 https://en.hespress.com/85374-moroccan-police-launches-new-platform-e-blagh-to-combat-cybercrime.html
88 https://www.childonlineafrica.org/
89 https://better-internet-for-kids.europa.eu/en/saferinternetday/supporter-listing/africa-safer-internet-day
90 ncsam.csa.gov.gh
91 https://cyber.gov.rw/updates/article/ncsa-launches-cybersecurity-and-data-protection-awareness-campaign/
92 https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-campaign-warns-against-cyber-and-financial-crimes

3. توعية المجتمع المحلي ومشاركته الثقافية

تتسم الحملات المحلية الطابع التي تستخدم اللغات والقنوات الثقافية المألوفة بفعالية خاصة في المجتمعات المحلية المحرومة والريفية.

- **تشاد:** نفّذت السلطات في ندجامينا برامج للتوعية على الجرائم السيبرانية باللجوء إلى فنانين محليين ومحطات إذاعية خاصة- وكان هذا خيارا استراتيجياً في بلد ذات معدلات أمية متفاوتة حيث تعوّل عدة مجتمعات ريفية على التواصل الشفهي. وقد استخدمت هذه الحملات لغات محلية ورسائل مألوفة من الناحية الثقافية لتثقيف السكان على عمليات الاحتيال الإلكتروني، بما يساعد في توسيع إمكانية الوصول إلى السكان الذين لا يمكن الوصول إليهم بسهولة من خلال المحتوى الخطي أو الرقمي.[93]
- **جمهورية الكونغو الديموقراطية:** تنظم الشرطة فعاليات شهرية لإعادة الهواتف المسروقة لأصحابها الشرعيين. وإذ أُطلقت هذه المبادرة بالشراكة مع الهيئة الناظمة الوطنية لقطاع الاتصالات ومكتب المدعي العام، فقد حظيت بتغطية إعلامية واسعة النطاق وترمي إلى إثباط شراء الهواتف المستخدمة. وغالبا ما ترتبط هذه الأجهزة بالجرائم السيبرانية مثل تحديد السرقة والابتزاز والتشهير. وأذكت هذه الحملة الوعي إلى حدّ كبير وساهمت في خفض عدد هذه الجرائم.

4. قنوات التنفيذ المؤسسية والمشتركة بين القطاعات

تُنفَّذ بعض حملات التوعية الأوسع نطاقا في أفريقيا من خلال هياكل منسّقة تشارك فيها وزارات متعددة، وأجهزة إنفاذ القانون ومجموعات المجتمع المدني. وتحسّن هذه الشراكات المؤسسية التواصل واتساق الرسائل والموثوقية.

- **الجزائر:** قامت الإدارات المتخصصة في مكافحة الجرائم السيبرانية في الجزائر بالتنسيق بشكل وثيق مع وزارة التربية، ووزارة البريد والاتصالات اللاسلكية ومنظمات المجتمع المدني لإطلاق حملات التوعية العامة. واستهدفت هذه الجهود جماهير متنوعة، ونُشرت بشكل دوري عبر مجموعة من المنصات، بما في ذلك الإذاعة والتلفزيون ووسائل التواصل الاجتماعي والمنتديات العامة والإعلانات. وقد رصدت السلطات الفعالية من خلال مشاركة وسائل التواصل الاجتماعي، وتقارير متزايدة عن الجرائم السيبرانية واعتماد أوسع من جانب عموم الناس للتصرفات الوقائية.

4.5 تعزيز عمليات إنفاذ القانون

أظهرت البلدان قدرات ميدانية أكبر وتعاونا دوليا أوسع في عام 2024، وبخاصة من خلال مداهمتين ذات أثر عالٍ في مكافحة الجريمة السيبرانية قام الإنتربول بتنسيقهما.

- **كانت عملية Serengeti** (أيلول/سبتمبر- تشرين الأول/أكتوبر 2024) إحدى أكبر إجراءات الإنفاذ لمكافحة الجريمة السيبرانية في القارة حتى تاريخه. وهذه العملية التي تولى تنسيقها الإنتربول وأفريبول، والتي شملت 19 بلدا، أفضت إلى توقيف أكثر من 1.000 شخص، وتفكيك 134.000 بنية تحتية إلكترونية خبيثة وتحديد أكثر من 35.000 ضحية. وقد استهدفت السلطات مشغلي برمجيات انتزاع الفدية، ومرتكبي عمليات الاحتيال بالبريد الإلكتروني المهني، ومرتكبي الابتزاز الرقمي وشبكات الاحتيال عن طريق الاستثمارات. وقُدّرت الخسائر المالية الإجمالية المرتبطة بالمخططات الإجرامية التي تعطلت خلال العملية بمبلغ 193 مليون دولار أمريكي على المستوى العالمي. كما أن الشركاء في القطاع الخاص، بما في ذلك مزوّدي خدمة الإنترنت، دعموا العملية من خلال المساعدة في إزالة البنية التحتية وتأمين المنصات الرقمية.[94]
- جمعت **عملية Red Card** (تشرين الأول/أكتوبر 2024- آذار/مارس 2025)، التي أُجريت في إطار مشروع العملية المشتركة لمكافحة الجريمة السيبرانية في أفريقيا (AFJOC)، بين وحدات معنية بمكافحة الجريمة السيبرانية من كوت ديفوار وبنن وتوغو ورواندا وجنوب أفريقيا وزامبيا ونيجيريا. وفكّكت هذه العملية شبكة إلكترونية لعمليات احتيال متصلة بالقروض من خلال تحليل المجالات، وملفات APK وحسابات التواصل الاجتماعي. كما ساهمت أجهزة الاستخبارات في القطاع الخاص في إعداد التقارير عن الأنشطة السيبرانية، التي كانت ذات أهمية أساسية في تحديد البنية التحتية الإجرامية والجهات الفاعلة المسؤولة عن التهديدات.[95]

وتشير هاتان العمليتان معا إلى قدرة متزايدة لدى البلدان الأفريقية في المشاركة في تحقيقات معقدة عابرة للحدود في الجرائم السيبرانية، والتي أتاحها تعزيز التنسيق ووضع أطر لتقاسم المعلومات الاستخباراتية والتعاون بين القطاعين العام والخاص.

93 INTERPOL Cyberthreat Assessment Survey
94 https://www.interpol.int/en/News-and-Events/News/2024/Major-cybercrime-operation-nets-1-006-suspects
95 https://www.interpol.int/en/News-and-Events/News/2025/More-than-300-arrests-as-African-countries-clamp-down-on-cyber-threats

6. التوصيات والاستنتاجات

ردّاً على التهديدات والتحديات المنتظمة والثغرات في القدرات المحددة في هذا التقييم، يقترح الإنتربول التوصيات الاستراتيجية التالية الموجّهة لأجهزة إنفاذ القانون وصانعي السياسات والأجهزة الإقليمية والشركاء الدوليين. وتستند هذه التوصيات على التعليقات الواردة من البلدان الأعضاء والأفكار الميدانية والاتجاهات المرصودة، وتهدف إلى توجيه تحسينات مستدامة وعملية ومنسقة لقدرات أفريقيا في الرد على الجرائم السيبرانية.

وتُنظّم التوصيات ضمن ستة مجالات مواضيعية:

- تعزيز القدرات الوطنية.
- توطيد الأطر القانونية والمؤسسية.
- تحسين التعاون الإقليمي والدولي.
- توسيع نطاق الوقاية والتوعية العامة.
- تعميق الشراكات بين القطاعين العام والخاص.
- الاستفادة من التكنولوجيات الناشئة لمنع الجرائم السيبرانية.
-

1.6 تعزيز القدرات الوطنية

يجب أن تحظى أجهزة إنفاذ القانون الأفريقية بالدعم في بناء القدرات الميدانية والفنية والمؤسسية المطلوبة لكشف الجرائم السيبرانية والتحقيق فيها وتعطيلها بطريقة فعالة. وقد أحرزت عدة بلدان التقدم، إنما لا زالت التفاوتات قائمة في القارة. ويجب أن تضم الأولويات ما يلي:

- إقامة وحدات مخصصة لمكافحة الجريمة السيبرانية وتوسيع نطاقها عبر تزويدها بقدر كافٍ من الموظفين والولاية والموارد الفنية على المستوى الوطني؛
- الاستثمار في تدريب خاص على مكافحة الجريمة السيبرانية يكون موجها للمحققين والمحلّلين والمدّعين والقضاة، بما في ذلك في مجالات مثل الأدلة الجنائية الرقمية، وتحليل البرمجيات الخبيثة، والمعلومات الاستخباراتية المفتوحة المصدر والتعقّب المالي؛
- ضمان إمكانية الوصول المستدام إلى أدوات تحقيق حديثة، بما في ذلك برمجيات رقمية مرخّصة للأدلة الجنائية وحفظ آمن للأدلة الجنائية؛
- تشكيل وتفعيل فرق استجابة لحوادث الكومبيوتر على المستويين الوطني والقطاعي من خلال بروتوكولات واضحة للتنسيق بين الأجهزة؛
- استبقاء ضباط متخصصين في مكافحة الجريمة السيبرانية من خلال مسارات مهنية وحوافز واضحة، للحدّ من استنزاف المواهب وضمان الفعالية في الأجل الطويل.

يشكل الاستثمار المستدام في القدرات الوطنية العمود الفقري في أي بيئة فعالة ومستقلة للتصدي للجرائم السيبرانية.

2.6 توطيد الأطر القانونية والسياسية

يتوقف إنفاذ مكافحة الجرائم السيبرانية على وجود أطر متينة وقائمة وقانونية قابلة للإنفاذ. إنما لا زالت عدة بلدان أفريقية تواجه ثغرات تشريعية تحدّ من قدرتها على ملاحقة مرتكبي الجرائم السيبرانية، والوصول إلى الأدلة العابرة للحدود أو التعاون على المستوى الدولي.

وبهدف التصدي لهذه المسائل، أوصى الإنتربول بما يلي:

- تسريع وتيرة اعتماد وتنفيذ القوانين الوطنية الشاملة لمكافحة الجريمة السيبرانية، المتوائمة مع المعايير الدولية والتي تشمل الجرائم المعتمِدة على الإنترنت والمدعومة بالإنترنت.
- ضمان الاعتراف القانوني بالأدلة الرقمية وقبولها قانونا، بما في ذلك الأدلة التي تمّ الحصول عليها عبر الحدود؛
- تنسيق التعريفات والإجراءات القانونية عبر الولايات القضائية، للحدّ من التجزئة القانونية وإتاحة التعاون الإقليمي الفعال؛
- المصادقة على الاتفاقيات الدولية والإقليمية وتفعيلها، مثل اتفاقية بودابست لمكافحة الجريمة السيبرانية، واتفاقية الاتحاد الأفريقي بشأن الأمن السيبري وحماية البيانات الشخصية (اتفاقية مالابو) واتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية؛
- وضع مسارات قانونية واضحة من أجل الوصول في الوقت المناسب إلى البيانات التي تحتفظ بها منصات أجنبية، بما في ذلك من خلال معاهدات المساعدة القانونية المتبادلة أو أطر الإفصاح عن حالات الطوارئ.

وتشكل الإصلاحات القانونية خطوة ضرورية باتجاه بناء الثقة في قدرات إنفاذ القانون وضمان المساءلة عن الأنشطة في مجال الجرائم السيبرانية. ويجب أن تُقابَل هذه الجهود باستثمارات في التدريب القضائي وتخصص النيابة العامة.

3.6 تحسين التعاون الإقليمي والدولي

نظرا للطبيعة العابرة للحدود الوطنية للجريمة السيبرانية، لا يمكن لأي بلد أن يتصدى للتهديد بمفرده. فالتعاون الإقليمي والعالمي أساسي لإجراء تحقيقات عبر الحدود وتعطيل البنى التحتية للجهات المسؤولة عن التهديد وتقاسم المعلومات الاستخباراتية في الوق الفعلي.

وبهدف تعزيز قدرات الاستجابة الجماعية، يوصي الإنتربول بما يلي:

- المصادقة على المعاهدات الدولية لمكافحة الجريمة السيبرانية وتنفيذها، مثل اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية واتفاقية بودابست بشأن مكافحة الجريمة السيبرانية، للسماح بإجراء تحقيقات أسرع عبر الحدود وتسليم مرتكبي الجرائم السيبرانية؛
- تعزيز آليات تقاسم المعلومات الاستخباراتية بين الدول الأفريقية من خلال توسيع المشاركة في العملية المشتركة لمكافحة الجريمة السيبرانية في أفريقيا، وفي برامج إقليمية ودولية أخرى لمكافحة الجريمة السيبرانية؛
- إضفاء الطابع المؤسسي على آليات التحقيق العابرة للحدود، بما في ذلك العمليات الرسمية لتقاسم الأدلّة وإحالة القضايا والتحقيقات الموازية؛
- استخدام منصات اتصالات مأمونة، مثل قناة منظومة I-24/7 للإنتربول، من أجل التنسيق السريع في مجال إنفاذ القانون عبر الحدود.
- دعم العمليات المشتركة وأفرقة المهام المتعددة البلدان، التي تركز على تعطيل شبكات مرتكبي الجرائم السيبرانية الناشطة في جميع أنحاء المنطقة.

يبقى الإنتربول وأفريبول ملتزمان بتيسير التعاون المنظّم في أفريقيا ومع الشركاء العالميين. سيكون التعاون المستمر أمرًا أساسيًا لسدّ الفجوات في إنفاذ القانون والتصدي لمجموعات الجريمة السيبرانية المنظمة التي تعمل خارج الحدود الوطنية.

4.6 توسيع نطاق الوقاية والتوعية العامة

في حين تكتسي الإمكانيات الفنية والأدوات القانونية أهمية أساسية في مكافحة الجريمة السيبرانية، تبقى الوقاية خط الدفاع الأكثر فاعلية من حيث الكلفة والأكثر قابلية للتطوير. وتعتمد عدة جرائم سيبرية في أفريقيا- مثل التصيد الاحتيالي وعمليات الاحتيال الإلكتروني وعمليات الاحتيال الرومانسي- على الهندسة الاجتماعية وتستغل مستويات متدنية من الوعي الرقمي.

وبهدف تعزيز جهود الوقاية، يوصي الإنتربول بما يلي:

- إطلاق حملات محددة الهدف للتوعية العامة، وبخاصة المجموعات المعرضة لخطر كبير مثل الشباب والنساء والمؤسسات الصغيرة والمتوسطة الحجم ومستخدمي الإنترنت للمرة الأولى؛
- دمج التثقيف في مجال الأمن السيبري في المناهج المدرسية والتدريب المهني وبرامج تعليم البالغين؛
- تعزيز الممارسات الأساسية للأمن السيبراني (النظافة الرقمية)، مثل استخدام كلمة سر قوية والمصادقة متعددة العوامل والإبلاغ عن رسائل مشبوهة؛
- تشجيع الضحايا على الإبلاغ عن الحوادث، من خلال تعزيز الثقة في إنفاذ القوانين وضمان السرية، وبخاصة في حالات الابتزاز الجنسي أو الاحتيال الإلكتروني؛
- إشراك منظمات المجتمع المدني المحلية، بما في ذلك مجموعات النساء وشبكات الشباب، للمساعدة في نشر الرسائل بطرق مناسبة من الناحية الثقافية.

ومن خلال تزويد الأفراد والمجتمعات المحلية بالمعرفة للتعرّف إلى التهديدات السيبرانية وتلافيها، يمكن للبلدان أن تحدّ من الإيذاء، وتقلّص المجموعة المستهدفة من قبل مرتكبي الجرائم السيبرانية وتخفّف عبء التحقيق الذي تتحمله أجهزة إنفاذ القانون.

5.6 تعميق الشراكات بين القطاعين العام والخاص

غالبا ما تعتمد التحقيقات في الجرائم السيبرانية على البيانات والبنية التحتية والأفكار التي تكون لدى كيانات في القطاع الخاص- بما في ذلك مزوّدي الاتصالات اللاسلكية والمؤسسات المالية ومنصات وسائل التواصل الاجتماعي والشركات المعنية بالأمن السيبري. إنما لا يزال مجال إنفاذ القانون في أفريقيا يواجه الحواجز على مستوى الوصول إلى المعلومات في الوقت المناسب والحصول على الدعم الفني من هذه الجهات.

وبهدف بناء بيئة تعاونية بشكل أكبر، يوصي الإنتربول بما يلي:

- إضفاء الطابع الرسمي على قنوات التعاون بين أجهزة إنفاذ القانون وأصحاب المصلحة الرئيسيين في القطاع الخاص، بما في ذلك الأطر لتقاسم مأمون وقانوني للبيانات؛
- إقامة منتديات وطنية وإقليمية بشأن الجرائم السيبرانية والانضمام إليها (مثلا مجموعة الخبراء في الجريمة السيبرانية التابعة للإنتربول)، تجمع بين الهيئات الناظمة والمحققين والمدّعين والجهات الفاعلة في القطاع العام من أجل مواءمة الأولويات وتقاسم المعلومات الاستخباراتية؛
- تيسير الحصول في الوقت المناسب على الأدلة الرقمية من المنصات العالمية، من خلال تحسين الاتفاقات القانونية والبروتوكولات الفنية وقنوات الاتصال الموثوقة؛
- الاستفادة من خبرة القطاع الخاص وما يتمتع به من بنية تحتية في مجالات مثل المعلومات الاستخباراتية عن التهديد وتحليل البرمجيات الخبيثة والاستجابة للحوادث؛
- تشجيع مساهمات القطاع الخاص في المبادرات لبناء القدرات، بما في ذلك التدريب ومجموعات الأدوات وبرامج التوجيه المعدّة لموظفي القطاع العام.

ومن خلال تحفيز الثقة والمواءمة الميدانية بين القطاعين العام والخاص، يمكن أن تطلق البلدان العنان للإمكانيات الحرجة وتسرّع وتيرة تعطيل شبكات مرتكبي الجرائم السيبرانية.

6.6 الاستفادة من التكنولوجيات الناشئة لمنع الجريمة السيبرانية

في حين تتطور الجريمة السيبرانية، يجب أن تتطوّر أيضا الأدوات والاستراتيجيات المستخدمة لمكافحتها. ويشكّل الذكاء الاصطناعي والتعلّم الآلي وتحليل البيانات والأتمتة فرصا جديدة بحيث تتمكن أجهزة إنفاذ القانون من استباق نشاط مرتكبي الجرائم السيبرانية وكشفه وتعطيله على نطاق واسع. غير أن اعتماد هذه التكنولوجيات يبقى غير متكافئ بين البلدان الأفريقية.

وبهدف تعزيز الإنفاذ الأكثر استباقا والموجّه بالبيانات، يوصي الإنتربول بما يلي:

- استكشاف إمكانيات استخدام الذكاء الاصطناعي وأدوات التعلّم الآلي لكشف التصيد الاحتيالي وكشف الحالات الشاذة وتصنيف الأدلة الرقمية؛
- تطوير الإمكانيات الوطنية والإقليمية في مجال تحليل البيانات من أجل تعقّب أنماط الجريمة السيبرانية ودعم عملية رصد التهديد في الوقت الفعلي؛
- الاستثمار في بنية تحتية مأمونة قائمة على السحابة لإدارة الحالات والأدلة الجنائية الرقمية وتبادل المعلومات عبر الحدود؛
- اختبار أدوات الأتمتة لجمع الأدلة والاستجابة للحوادث ورصد الشبكة في أجهزة إنفاذ القانون؛
- بناء الأطر الأخلاقية والقانونية للاستخدام المسؤول للتكنولوجيات الناشئة في التحقيقات في الجرائم السيبرانية، عبر الاستلهام من مبادرات مركز الابتكار للإنتربول في مجال الذكاء الاصطناعي.

توفر التقنيات الناشئة مسارًا نحو إنفاذ أسرع وأكثر ذكاءً وقابليةً للتوسع، ولكن ذلك مشروط باستخدامها بحذر وبما يضمن وجود الضوابط الوقائية اللازمة.

نبذة عن الإنتربول

إن الإنتربول هو أكبر منظمة دولية للشرطة في العالم. ويتمثل دوره في مد يد العون إلى أجهزة إنفاذ القانون في البلدان الأعضاء الـ 196 لمكافحة الجريمة عبر الوطنية بجميع أشكالها. وهو يسعى إلى مساعدة أجهزة الشرطة في العالم أجمع على مواجهة التحديات المتنامية للجريمة في القرن الحادي والعشرين بتزويدها بالدعم التقني والميداني بفضل بنية تحتية متطورة. وتشمل الخدمات التي يقدمها الإنتربول تدريبا محدد الأهداف، ودعما متخصصا لعمليات التحقيق، وقواعد بيانات متخصصة وقنوات مأمونة للاتصالات الشرطية.

رؤية الإنتربول: "الوصل بين أجهزة الشرطة لجعل العالم أكثر أمانا"

تتمثل رؤية الإنتربول في إقامة عالم يكون فيه كل موظف من موظفي إنفاذ القانون قادرا، من خلال المنظمة، على التواصل بشكل مأمون وعلى تبادل المعلومات الشرطية الحيوية والاطلاع عليها كلما وحيثما دعت الحاجة، من أجل ضمان سلامة المواطنين في العالم.ويقدم الإنتربول باستمرار حلولا جديدة ومتطورة لمواجهة التحديات التي تعترض أجهزة الشرطة والأمن على الصعيد العالمي ويشجع على استخدامها.

نبذة عن برنامج الإنتربول لمكافحة الجريمة السيبرانية

في عصر رقمي متغير، يتعرض فيه أكثر من نصف البشرية لخطر الوقوع ضحية للجريمة السيبرانية، يتولى برنامج الإنتربول العالمي لمكافحة الجريمة السيبرانية تقديم الدعم لأجهزة إنفاذ القانون الدولية. ونحن ملتزمون بإعداد وقيادة استجابة عالمية ترمي إلى منع هذه الجريمة، وكشفها، والتحقيق فيها، وتعطيلها،بهدف الوصول في نهاية المطاف إلى الحد من تأثيرها على العالم وحماية المجتمعات من أجل عالم أكثر أمانا.

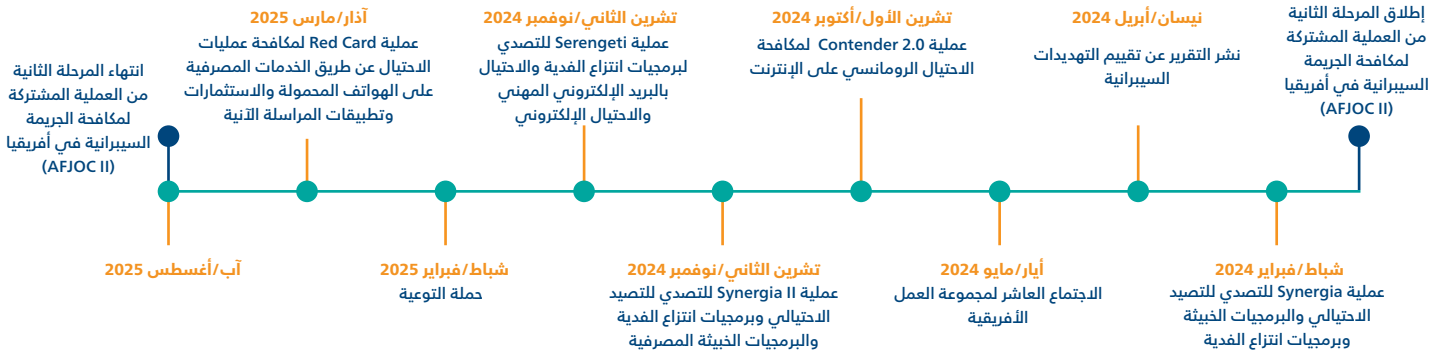
وتركز استراتيجية الإنتربول لمكافحة الجريمة السيبرانية على أربعة أهداف رئيسية:

- تبنّي نهج استباقي وديناميكي لمنع الجريمة السيبرانية وتعطيلهاعبر تكوين صورة دقيقة عن مشهد تهديدات الجريمة السيبرانية من خلال توفير المعلومات وتحليل المعلومات الاستخباراتية.
- منع الجريمة السيبرانية، التي تسبب ضررا كبيرا على الصعيد الوطني والإقليمي والعالمي، وكشفها، والتحقيق فيها وتعطيلها بفعالية، من خلال الإشراف على العمليات عبر الوطنية وتنسيقها ومساعدة البلدان الأعضاء على تنفيذها.
- المساعدة على تطوير استراتيجيات البلدان الأعضاء وقدراتها لمكافحة الجريمة السيبرانية وذلك عبر إرساء شراكات مفتوحة وشاملة ومتنوعة، وبناء الثقة في بيئة أمنية سيبرية عالمية.
- تعزيز دور الإنتربول وقدراته في رسم إطار الأمن العالمي من خلال المشاركة في المنتديات الدولية التي تتناول الجرائم السيبرانية.
- وننفّذ استراتيجيتنا وأهدافنا من خلال نموذج عمل بسيط وبنّاء، يرتكز على ثلاثة أركان أساسية:

- التصدي لتهديدات الجريمة السيبرانية: استجابة سريعة ومنسقة لتهديدات الجريمة السيبرانية الفورية والناشئة؛
- عمليات مكافحة الجريمة السيبرانية: تنفيذ استراتيجية ميدانية إقليمية لمكافحة الجريمة السيبرانية بشكل فعال؛
- بناء القدرات في المجال السيبري: تعزيز الاستراتيجيات والقدرات من خلال مشاريع ومنصات مبتكرة.

وتعوّل هذه الأركان على شبكتنا الواسعة من الشراكات مع القطاعين العام والخاص، مما يؤدي إلى تعزيز التعاون والنهوض بالخبرة الجماعية لمكافحة الجريمة السيبرانية.

وللحصول على مزيد من المعلومات، يرجى الاتصال بنا بالبريد الإلكتروني: EDPS-CD@interpol.int



نبذة عن العملية المشتركة لمكافحة الجريمة السيبرانية

العملية المشتركة لمكافحة الجريمة السيبرانية هي مبادرةأطلقها الإنتربول لتعزيز قدرة أجهزة إنفاذ القانون الوطنية في أفريقيا على منع الجريمة السيبرانية والكشف عنها والتحقيق فيها وتعطيلها. ويتحقق ذلك من خلال ما يلي:

- جمع المعلومات حول أنشطة الجرائم السيبرانية وتحليلها؛
- تنفيذ عمل منسق يقوم على البيانات الاستخباراتية التي تُجمع؛
- تشجيع التعاون واتباع أفضل الممارسات في أوساط البلدان الأفريقية الأعضاء.

وقد موّلت المرحلة الأولى من هذه المبادرة وزارةُ الخارجية والكومنولث والتنمية في المملكة المتحدة ونُفّذت في الفترة من عام 2021 إلى 2023. وتستند المرحلة الثانية، التي لا تزال تحظى بدعم من وزراة الخارجية والكومنولث والتنمية في المملكة المتحدة، إلى الإنجازات التي تحققت خلال المرحلة الأولى، وتهدف إلى مواصلة تعزيز قدرات أجهزة إنفاذ القانون الوطنية في أفريقيا.

أنشطة المشروع

- الدعم التحليلي والمعلومات الاستخباراتية - يشكل الجمع السريعوالدقيق لمعلوماتاستخباراتية دقيقة أمرا حيويا لأيّ استجابة من جانب أجهزة إنفاذ القانون للجريمة السيبرانية. وتشكل تقارير الأنشطة السيبرانية التي نُصدرها موارد مهمة، إذ توفّر الأفكار عن التهديدات السيبرانية التي تستهدف بلدان أو أقاليم محددة.
- تطوير القدرات والإمكانيات الإقليمية لمكافحة الجريمة السيبرانية - ثمة منصات تعاونية، مثل منصة التعاون لمكافحة الجريمة السيبرانية والمنصة المتعددة الاختصاصات لمكافحة الجريمة السيبرانية، تتيح التواصل بشكل مأمون وتبادل بيانات عن العمليات؛
- إطار العمل المشترك - يتيح مواجهة تهديدات الجرائم السيبرانية من خلال التعاون بين أجهزة إنفاذ القانون والقطاع الخاص ومنظمات أخرى دولية//حكومية دولية؛
- دعم العمليات وتنسيقها - تساهم عملياتنا في تفكيك الشبكات الإجرامية الضالعة في الجريمة السيبرانية؛
- حملات التوعية - ترمي إلى تعريف الناس والمؤسسات في أفريقيا بالممارسات الجيدة المعتمدة في المجال السيبري؛
- اجتماعات مجموعة العمل لرؤساء الوحدات- تجمع بين ممثلين من جميع البلدان الأفريقية تقريبا للتصدي للتحديات الإقليمية المتصلة بالجريمة السيبرانية وتعزيز التعاون الميداني من خلال اجتماعات جانبية ومناقشات استراتيجية.

مكتب الإنتربول لعمليات مكافحة الجريمة السيبرانية في أفريقيا هو المسؤول عن العملية المشتركة لمكافحة الجريمة السيبرانية في أفريقيا (AFJOC). وهو يعمل بشراكة وثيقة مع أصحاب المصلحة الرئيسيين في المنطقة، ولا سيما آلية الاتحاد الأفريقي للتعاون الشرطي وأفريبول، ومع أوساط إنفاذ القانون والقطاع الخاص.

جهة الاتصال

مكتب الإنتربول لعمليات مكافحة الجريمة السيبرانية في أفريقيا Africadesk@interpol.int

الإنتربول

INTERPOL

@INTERPOL_HQ

INTERPOL

INTERPOL HQ

INTERPOL_HQ