الأمن السيبراني والتحول الرقمي

انعكاسات الجرائم الإلكترونية على الأمن القومي والاستقرار المالي في إفريقيا وأمريكا اللاتينية ومصر

بقلم

الباحثة نجلاء فتحي محمد فهيم

جامعة بنها/ مصر

00964- 7710122232 Alfaidcenter2011@gmail.com العراق - بغداد - الكرادة

مقدمة

مع تسارع التحولات الرقمية على مستوى العالم، تصاعدت الجرائم الإلكترونية والمخاطر السيبرانية لتصبح واحدة من أبرز التهديدات التي تؤثر بشكل مباشر على الأمن القومي والاقتصادي للدول. هذا الأمر يزداد وضوحاً مع الانتشار الواسع للتكنولوجيا الرقمية داخل المؤسسات الحكومية والمالية والبنية التحتية الحيوية.

حيث لم تعد الهجمات السيبرانية مقتصرة على اختراقات تقنية محدودة، بل أصبحت أدوات قادرة على تهديد استقرار كافة الدول، وإحداث اضطرابات في الأنظمة الاقتصادية، والتأثير المباشر على كفاءة واستمرارية القطاعات الحيوية والإستراتيجية فى الدولة.

كما أدى أيضاً، الانتشار السريع للإنترنت والتطبيقات المتقدمة مثل الذكاء الاصطناعي والتكنولوجيا المالية إلى تعقيد البيئة الرقمية، مما رفع من احتمالية التعرض للتهديدات السيبرانية على الصعيدين الإقليمي والدولي.

أما على المستوى الإقليمي، تواجه كل من إفريقيا وأمريكا اللاتينية تحديات متزايدة في مجال الأمن السيبراني نتيجة قصور البنية التحتية الرقمية وضعف التشريعات المنظمة للفضاء السيبراني. تضاف إلى ذلك محدودية القدرات الفنية والتقنية للتصدي للجرائم الإلكترونية المتطورة. وقد نتج عن هذا الوضع تزايد معدلات الهجمات السيبرانية التي طالت المؤسسات الحكومية والمالية وشبكات البنية التحتية داخل القارتين، مما خلق تهديداً بالغاً للأمن القومي والاستقرار الاقتصادي في تلك المناطق.

وفي مصر، ومع التحول المتسارع نحو الرقمنة والخدمات المالية الإلكترونية، باتت المخاطر السيبرانية تشكل تحدياً كبيراً للقطاع المالي المحلي. يتضح هذا، بشكل خاص مع انتشار استخدام تطبيقات الدفع الإلكتروني وتقنيات التكنولوجيا المالية، حيث يزداد تعرض المؤسسات المصرفية للهجمات الإلكترونية التي تستهدف البيانات المالية وأنظمة الدفع. أمام هذه التحديات، تظهر الحاجة المُلحة لتطوير استراتيجيات فعالة لتقوية الأمن السيبراني وتعزيز قدرة المؤسسات على إدارة المخاطر الرقمية بفعالية.

وبناء عل ماسبق، تهدف هذه الدراسة إلى تحليل طبيعة الجرائم الإلكترونية والتهديدات السيبرانية وتأثيراتها على الأمن القومي والإقتصادى والاستقرار المالي، مع التركيز بشكل خاص على التجربة المصرية في هذا المجال.

المحور الأول: أنماط الجرائم الالكترونية في القارة الأفريقية وأثرها على الأمن القومي

بحسب تقرير أصدره الإنتربول عام 2020 حول المخاطر التي تشكلها الجرائم الإلكترونية على أمن القارة الأفريقية، تم الإشارة إلى أن أفريقيا لا تزال تحتل أدنى مرتبة في معدلات الاتصال بالإنترنت على مستوى العالم. ووفقاً لبيانات الاتحاد الدولي للاتصالات، أظهرت تقارير عام 2019 أن 28% فقط من سكان القارة كانوا يستخدمون الإنترنت، مقارنةً بـ 83% في أوروبا. ومع ذلك، لم تمنع هذه المعدلات المنخفضة من تزايد جماعات الجرائم الإلكترونية والهجمات السيبرانية.[1]

[1] "Online crime in Africa a bigger threat than ever before, Interpol report warns". (2020), INTERPOL. 1https://www.interpol.int/en/News-and-Events/News/2020/Online-crime-in-Africa-a-bigger-threat-than-ever-before-INTERPOL-report-warns

00964- 7710122232 Alfaidcenter2011@gmail.com العراق - بغداد - الكرادة

ويشير التقرير إلى أن أحد العوامل الرئيسية التي تساهم في زيادة الجرائم المرتبطة بالإنترنت في أفريقيا هو نقص السياسات والاستراتيجيات الشاملة لمكافحة الجريمة السيبرانية في العديد من الدول. فعلى الرغم من أن الاتحاد الأفريقي اعتمد اتفاقية الأمن السيبراني وحماية البيانات الشخصية في عام 2014، إلا أن 14 دولة فقط من أصل 55 دولة عضو في الاتحاد وقعت عليها بحلول كانون الثاني 2020، بينما تتطلب الاتفاقية تصديق 15 دولة عضو على الأقل لتصبح سارية المفعول، وحتى كانون الثاني 2020، لم تصادق عليها سوى سبع دول فقط. وهو ما يعكس عدم إدراك العديد من الدول الأفريقية لأهمية الأمن السيبراني، مما يزيد من تفاقم المشكلة. وبحسب مؤشر الجريمة المنظمة العالمي، الصادر عن المبادرة العالمية لمكافحة الجريمة المنظمة العابرة للحدود، إحتلت القارة الأفريقية الترتيب الثاني عالمياً في إرتفاع مستوى الجرائم الالكترونية، وذلك خلال العام 2021، بنحو 5.25 نقطة من أصل 10 نقاط.[2]

طبيعة الجرائم الالكترونية في الدول الأفريقية

تتخذ الجرائم الالكترونية فى أفريقيا أنماطاً متعددة، تدور أغلبها حول مفهوم الإرهـاب السيبراني. ومن أبرز الهجمات السيبرانية التي أصابت دول القارة الإفريقية، خلال شهر أيار من العام 2022، أعلنت وكالة أمن شبكات المعلومات الإثيوبية (INSA) أن قراصنة حاولوا استهداف سد النهضة الإثيوبي الكبير (GERD). وقد تمكنت وكالة أمن الاتصالات الإثيوبية من إحباط هذه الهجمات قبل أن يتمكن القراصنة من الوصول إلى الشبكات. وفي أيلول من عام 2022، استهدفت مجموعة قرصنة تم اكتشافها فيما بعد الهجوم السيبراني، شركات الاتصالات ومزودي خدمات الإنترنت والجامعات في منطقتي "الشرق الأوسط" وأفريقيا. وفي آذار من العام 2024، تسبب هجوم إلكتروني كبير في تعطيل أنظمة الاتحاد الأفريقي لأكثر من أسبوع، مما أثر على أكثر من 200 جهاز مستخدم، حسبما أفاد نائب رئيس مفوضية الاتحاد الأفريقي. ولا يزال سبب هذا الهجوم غير معروف حتى يومنا هذا.[3]

ويمكن إستعراض أكثر الجرائم الالكترونية شيوعاً في أفريقيا بحسب ماتم ذكره في تقرير تقييم التهديدات السيبرانية في أفريقيا 2023، الصادر عن الانتربول على النحو التالي:

الهجوم السيبراني على الشركات من خلال الإحتيال الالكتروني

على الرغم من أن الدول الأفريقية تمثل فقط 0.75% من محاولات الاختراق الإلكتروني للأعمال التجارية (BEC) على مستوى العالم بين عامي 2021 ومايو 2022، إلا أن بيانات شركة "ترينـد مايكرو" - أحد شركاء القطاع الخاص لمكتب عمليات مكافحة الجرائم الإلكترونية في أفريقيا التابع للإنتربول - تشير إلى أن جنوب أفريقيا

---

[2] مؤشر الجريمة المنظمة العالمى. (2023)، فرنسا، ص 85.

[3] Center for Strategic and International Studies (CSIS), Washington , D.C. إن أعظم ما في عيد الغدير أنه لا يدعو إلى الكراهية أو الانغلاق، بل يفتح الباب أمام إحياء الإسلام الأخلاقي والإنساني، الإسلام.

00964- 7710122232 Alfaidcenter2011@gmail.com العراق - بغداد - الكرادة

وحدها سجلت أكثر من نصف حالات الاختراق الإلكتروني للأعمال التجارية المُبلّغ عنها في المنطقة خلال نفس الفترة. وقد زاد خطر هذه الاختراقات بشكل ملحوظ في أفريقيا نتيجة الانتقال السريع نحو اقتصاد رقمي متنامٍ. ومع تزايد اعتماد المستخدمين على التكنولوجيا في معاملاتهم اليومية، تزداد فرص الجهات الخبيثة لاستغلال المؤسسات الضعيفة.

علاوة على ذلك، تعاني العديد من مناطق أفريقيا من نقص في تدابير الأمن السيبراني الفعّالة، مما يزيد من خطر هجمات الاختراق الإلكتروني للأعمال التجارية. ومن العوامل الأخرى التي تسهم في زيادة هذه الهجمات غياب ممارسات الأمن السيبراني الأساسية داخل الشركات العاملة في القارة. فالكثير من المؤسسات تفتقر إلى سياسات كافية لإدارة بروتوكولات التحكم في الوصول، وعمليات المصادقة، ومعايير التشفير، مما يجعلها عرضة للهجمات من خلال أنظمة غير آمنة وحسابات مستخدمين بكلمات مرور ضعيفة. وتشير الإحصاءات من 22 دولة عضو في المنطقة الأفريقية إلى أنه تم الإبلاغ عن 399 حالة من حالات البريد الإلكتروني للأعمال التجارية إلى وكالات إنفاذ القانون في عام 2021.

1. التصيد الاحتيالي

في الفترة ما بين كانون الثاني وتموز 2022، أفادت شركة "كاسبرسكي" أحد الشركات المتخصص في الأمن السيبراني، باكتشاف نحو 15,769,298 مليون هدفاً احتيالياً في أفريقيا، وهو رقم يثير القلق. وقد تم تنفيذ معظم هذه الأنشطة الخبيثة عبر رسائل البريد الإلكتروني أو صفحات الويب باستخدام أسلوب شائع يُعرف بالتصيد الاحتيالي. حددت مجموعة "حوالي 1,352,412 IB" عنوان URL للتصيد الاحتيالي في المنطقة الأفريقية بين كانون الثاني وآب من العام 2022، مما يعكس مصدر قلق أمني كبير، حيث يمكن أن تؤدي هجمات التصيد الاحتيالي إلى عواقب وخيمة على الأفراد والمؤسسات التي قد تتعرض لها بشكل غير متوقع.

ويكشف تقرير مجموعة عمل مكافحة التصيد الاحتيالي، أن القطاع المالي بما في ذلك البنوك، هو الهدف الأكبر لهجمات التصيد، حيث يمثل أكثر من 23% من جميع الهجمات. ويعود انتشار هذه الهجمات إلى سهولة شراء أدوات تصيد مقابل 20 دولاراً في السوق السوداء، تشمل مواد ودروس فيديو لشن هجمات ناجحة. كما تتوفر خدمات ما بعد البيع مع تحديثات دورية لتفادي اكتشاف الرسائل من قبل حلول الأمن السيبراني، مما يسهل على المهاجمين، حتى غير المتمرسين، تنفيذ هجمات التصيد.

2. برامج الفدية

تشير بيانات شركة Shadowserver من يناير إلى ايلول 2022 إلى استهداف واسع للضحايا في أفريقيا من قبل جماعات برامج الفدية. وتؤثر هذه البرامج الخبيثة بشكل كبير على العمليات التجارية من خلال تشفير البيانات، مما يؤدي إلى دفع فدية أو توقف الأنظمة. وقد ساهم انتشار برامج الفدية في زيادة الجرائم الإلكترونية ذات الدوافع المالية في أفريقيا. وأفادت شركة Shadowserver أن جنوب أفريقيا هي الأكثر استهدافاً بهجمات برامج الفدية، حيث تمثل 42% من جميع الهجمات المكتشفة، تليها المغرب (8%)، وبوتسوانا ومصر (6% لكل منهما). كما تسجل تنزانيا وكينيا 4% من الهجمات. وبحسب شركة Trend Micro، تمثل برامج الفدية 1.4% من الجرائم الإلكترونية عالمياً في الفترة بين كانون الثاني وتموز 2022، لكن خطرها في أفريقيا يبقى كبيراً. وبالنسبة

00964- 7710122232 Alfaidcenter2011@gmail.com العراق - بغداد - الكرادة

للقطاعات الأكثر تعرضاً لمثل هذه الهجمات، فتشمل الوكالات الحكومية، التعليم، الطاقة، تجارة التجزئة، والسلع الاستهلاكية، بالإضافة إلى استهداف البنية التحتية الحيوية مثل الرعاية الصحية والنقل. وأظهرت بيانات من 42 دولة أفريقية أنه تم الإبلاغ عن 59 حالة فقط من برامج الفدية في 11 دولة.

3. برامج سرقة البيانات المصرفية

تشهد القارة الأفريقية طفرة ملحوظة في مجال التكنولوجيا الرقمية، لاسيما في مجالات التكنولوجيا المالية والتجارة الإلكترونية، وهو ما أدى إلى سهولة تنفيذ هجمات باستخدام برمجيات خبيثة، مثل برامج سرقة البيانات المصرفية، التي تمثل تهديداً كبيراً لأمن الأفراد والبنية التحتية السيبرانية للمؤسسات، نظراً لقدرتها على إحداث أضرار جسيمة إذا لم يتم اكتشافها بسرعة. ووفقاً لاكتشافات شركة "تريند مايكرو"، يُعتبر المغرب الدولة الأفريقية الأكثر تضرراً، حيث تم تسجيل 18,827 حالة. تليه جنوب أفريقيا بفارق بسيط، مع 6,560 حالة من البرمجيات الخبيثة. كما تم تسجيل 5,366 حالة في نيجيريا، و1,462 حالة في الكاميرون، و691 حالة في الجزائر. ومن بين البرمجيات الخبيثة التي يجب الانتباه إليها في المنطقة الأفريقية، يبرز برنامج RedLine Stealer. حيث أظهرت أبحاث مجموعة Group-IB، أنه فى الفترة بين كانون الثاني وآب 2022، تم اختراق حوالي 5,862,188 مليون حساباً من عناوين IP أفريقية باستخدام هذا البرنامج. وعادةً ما يتم توزيع هذا البرنامج الخبيث من خلال ألعاب وتطبيقات وخدمات مخترقة، بهدف سرقة معلومات حساسة مثل بيانات متصفح الويب، ومحافظ العملات المشفرة، وبيانات اعتماد التطبيقات لمستخدمي برامج شائعة مثل Telegram وشبكات VPN.

4. عمليات الاحتيال والابتزاز الإلكتروني

تشهد أنشطة الإحتيال والإبتزاز الإلكترونى انتشاراً بشكل ملحوظ في المنطقة الأفريقية. وتنتشر هذه الأنواع من الجرائم الإلكترونية في المنطقة الأفريقية، وذلك بسبب ضعف الوعي العام بوجودها وآليات عملها. كما أن الأشخاص الذين يعانون من صعوبات مالية يكونون أكثر عرضة لقبول عروض المحتالين، معتقدين أنها قد توفر لهم حلاً لمشاكلهم المالية. وقد كشف باحثون من شركة "تريند مايكرو" حوالي 7.7 مليون حالة اكتشاف لهجمات ويب خبيثة كجزء من دراستهم، حيث ارتبطت معظم هذه الحالات بمواقع احتيال بنسبة 40.31%. كما أُفيد بأن مخططات الابتزاز عبر البريد العشوائي لا تزال وسيلة شائعة للهجمات الإلكترونية عالمياً. ومن بين الدول الأفريقية التي تم تتبعها، كانت 69.24% (13,002) من مخططات الابتزاز المكتشفة في المغرب.

المحور الثاني: أنماط الجرائم الالكترونية في القارة اللاتينية وتهديد الأمن القومي

أظهرت نسخة مؤشر الجريمة المنظمة الصادرة خلال العام 2023، انتشاراً ملحوظاً للجرائم الإلكترونية في القارة اللاتينية. وتصدرت أمريكا الشمالية القائمة العالمية بنحو 7.25 نقطة من أصل 10 درجات. ويحتوي مكتب التحقيقات الفيدرالي على قائمة تضم أكثر من مئة مجرم مطلوب، بالإضافة إلى مجموعات متورطة في ارتكاب جرائم إلكترونية ضارة ضد الحكومة الأمريكية. وقد استهدفت هجمات الفدية الحكومات المحلية والجامعات والمناطق التعليمية ومقدمي الرعاية الصحية، مما أدى إلى إختراق البيانات وزيادة الطلب على حلول

00964- 7710122232 Alfaidcenter2011@gmail.com العراق - بغداد - الكرادة

الأمن السيبراني المبتكرة. وبالتالي، أصبحت الجرائم المرتبطة بالإنترنت سوقاً متنامية تتطور مع كل تقدم تكنولوجي، خاصة مع ظهور الذكاء الاصطناعي.

طبيعة الجرائم الالكترونية في دول القار اللاتينية

بحسب تقرير نُشر على موقع "Americas Quarterly"، تم الكشف عن أبرز الجرائم الإلكترونية والهجمات السيبرانية التي تعرضت لها دول القارة اللاتينية. **ومن هذه الهجمات مايلي:**[4]

خلال عام 2019، تأثرت أنظمة الدفع الخاصة بشركة النفط المكسيكية Pemex باختراق، حيث أكدت الشركة أنها احتوت الهجوم في الوقت المناسب ونفت تأثر بنيتها التحتية الحيوية، لكن لا تزال هناك تساؤلات حول كيفية حدوث هذا الهجوم.

وفي تموز 2020، اضطرت أكبر شركة مزود للإنترنت في الأرجنتين، Telecom Argentina، إلى تسريع إعادة أنظمتها بعد أن أصاب هجوماً إلكترونياً يطالب بفدية قدرها 7.5 مليون دولار من نحو 18000 محطة عمل. كان هذا الهجوم واحداً من أكثر من 1500 هجوم تم الإبلاغ عنها في البلاد في ذلك العام، بزيادة قدرها 60% عن العام 2019.

أيضاً في عام 2020، تعرضت المحكمة الانتخابية البرازيلية لعدة هجمات خلال الانتخابات الإقليمية لنفس العام، حيث استهدفت نظام فرز الأصوات. وأفادت المحكمة بأن القراصنة لم يتمكنوا إلا من تأخير الفرز، لكن ذلك كان كافياً لإثارة شكوك عميقة لدى البرازيليين، الذين اعتادوا معرفة نتائج الانتخابات في غضون دقائق من إغلاق صناديق الاقتراع.

وخلال عام 2021، تعرضت دول "كوستاريكا" لاختراق من قبل مجموعة القراصنة الروسية المعروفة باسم "كونتي"، التي كانت تُعتبر في ذلك الوقت أكبر مجموعة متخصصة في برامج الفدية. تمكنت هذه المجموعة من جمع حوالي 180 مليون دولار من ضحاياها. وباستخدام بيانات تم اختراقها، استطاع القراصنة تثبيت برامج ضارة على جهاز واحد داخل شبكة وزارة المالية، مما أدى إلى انتشار العدوى بشكل واسع. ثم استخرج المهاجمون مئات الآلاف من الجيجابايت من المعلومات الشخصية للكوستاريكيين، وقاموا بنشر عينة منها على الويب المظلم. كما قاموا بتشفير أنظمة الوزارة، مما جعل من الصعب على الحكومة معالجة المدفوعات أو تحصيل الضرائب، وأدى إلى تجميد عمل وكالة الجمارك. وللمطالبة بفدية قدرها 10 ملايين دولار، هددت المجموعة بنشر بقية البيانات المسروقة إذا لم يتم تلبية مطالبها.

وفي ذات السياق، تعرض النظام القضائي البرازيلي لـ 13 هجوماً متتالياً بين عامي 2020 و2022، مما أدى إلى شلل الخدمات وتأجيل قضايا المواطنين. كما واجه وزير المالية "في ريو دي جانيرو" صعوبة في تحصيل الضرائب، بينما كان على المواطنين الذين يحتاجون إلى وثائق تقديم طلباتهم شخصياً بعد اختراق المكتب في عام 2022. وفي "كيتو"، اضطرت الحكومة المحلية إلى تعليق الخدمات المقدمة للسكان في نيسان 2022

---

[4] Tornaghi, Cecelia. (2023), "The Dramatic Cyberattack That Put Latin America on Alert", Article, Americas Quarterly), Politics, Business & Culture in the Americas. https://www.americasquarterly.org/article/the-dramatic-cyberattack-that-put-latin-america-on-alert/.

00964- 7710122232 Alfaidcenter2011@gmail.com العراق - بغداد - الكرادة

للتعامل مع هجوم ببرامج الفدية وفي العام 2021، اكتشف الأرجنتينيون أن بياناتهم الشخصية ووثائقهم معروضة للبيع على الويب المظلم بعد اختراق مكتب التسجيل الوطني، RENAPER، حيث نشر المهاجم بطاقة هوية نجم كرة القدم ليونيل ميسي على تويتر. في الوقت نفسه، تعرضت أجهزة الاستخبارات البيروفية لهجوم كونتي، بينما تعرضت كوستاريكا لهجوم مماثل، مع قلة المعلومات المتاحة حول هذا الاختراق. كما أدت هجمات بارزة على وزارة الدفاع المكسيكية، SEDENA، من قِبل مجموعة Guacamaya الناشطة إلى تسريب آلاف الوثائق السرية ورسائل البريد الإلكتروني الخاصة، بما في ذلك تلك المتعلقة بصحة الرئيس المكسيكي. وقد اخترقت مجموعة الهاكرز أيضاً شبكات عسكرية وشركات تعدين في كولومبيا وغواتيمالا وتشيلي.

وفي أيلول من العام 2022، تعرضت وزارة الدفاع المكسيكية لهجوم من قبل قراصنة، الذين تمكنوا من الحصول على ستة تيرابايت من البيانات. شملت هذه البيانات اتصالات داخلية ومعلومات جنائية، بالإضافة إلى تفاصيل حول مراقبة المكسيك للسفير الأمريكي لدى المكسيك، كين سالازار. وقد أكد الرئيس المكسيكي أندريس مانويل لوبيز أوبرادور صحة هذه المعلومات، بما في ذلك البيانات الصحية الشخصية التي تم نشرها للجمهور.[5]

ويُقدّر الخبراء أن أمريكا اللاتينية تشهد نحو 1600 هجوم إلكتروني في الثانية. ووفقاً للإنتربول، سجلت المنطقة رقماً قياسياً عالمياً في الهجمات الإلكترونية خلال النصف الأول من عام 2020، حيث تجاوزت الهجمات عبر متصفحات الهواتف المحمولة المتوسط العالمي بثلاثة أضعاف. بينما يستهدف المتسللون مجموعة متنوعة من الأهداف، إلا أن الهجمات التي تستهدف الحكومات والمؤسسات العامة تثير قلقاً خاصاً.

ومن الواضح أن أمريكا اللاتينية تواجه تحديات كبيرة في تحديد المصدر الجغرافي للهجمات الإلكترونية البارزة، حيث تأتي هذه الهجمات من مختلف أنحاء العالم، بالإضافة إلى تزايد النشاط من داخل المنطقة نفسها. ومع ذلك، لا يزال العديد من صناع القرار في القطاعين العام والخاص ينظرون إلى الفضاء الإلكتروني كمسألة تقنية تتعلق بفرق تكنولوجيا المعلومات، بدلاً من اعتبارها قضية هيكلية تتطلب معالجة من قبل المدراء التنفيذيين والجهات الحكومية.

المحور الثالث: التحديات المشتركة بين القارتين الأفريقية واللاتينية في مجال الجريمة الإلكترونية

هناك العديد من التحديات المشتركة التي تواجه القارتين الأفريقية واللاتينية في مجال الجريمة الإلكترونية. وهذا يفتح المجال أمام إمكانية التعاون بين كلا القارتين لتحديد الآليات ورسم الاستراتيجيات التي تعزز وتدعم هذا التعاون في مكافحة مثل هذه الجرائم، التي تشكل تهديداً خطيراً على الأمن القومي للدول المختلفة. ومن أبرز هذه التحديات درجة مرونة الأمن السيبراني والقدرة على مواجهة الجرائم الالكترونية والتهديدات السيبراني وعمليات القرصنة.

---

[5] Center for Strategic and International Studies (CSIS), Washington , D.C. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

00964- 7710122232 Alfaidcenter2011@gmail.com العراق - بغداد - الكرادة

وفي هذا السياق، بحسب تقرير "توقعات الأمن السيبرانى للعام 2025"، نحو 36% في أفريقيا و42% في أمريكا اللاتينية، من المشاركين في إستطلاعات الرأي بشأن مدى تحقيق الأمن السيبراني في كل من القارتين، يفتقرون إلى الثقة في قدرة بلادهم على التعامل مع الحوادث السيبرانية الكبرى التي تستهدف البنية التحتية الحيوية.[6]

1. مستوى الأمن السيبراني في القارة الأفريقية

بالرغم من أن أغلب الدول فى القارة الأفريقية قد وضعت إستراتيجيات للأمن السيبرانى، إلا أن الإحصائيات تشير إلى أن أفريقيا تُعتبر من بين المناطق الأكثر عرضة للهجمات السيبرانية لاسيما مع تزايد اعتماد أفريقيا على التحول الرقمي. كما تشير الأبحاث التي أجرتها شركة "سيريانو" للأمن السيبراني، ومقرها كينيا، إلى أن تكلفة الجرائم الإلكترونية في أفريقيا ارتفعت من 500 مليون دولار أمريكي في عام 2015 إلى 3 مليارات دولار أمريكي في عام 2020.[7]

وفي عام 2020، كانت إفريقيا واحدة من أكثر المناطق تعرضاً للهجمات السيبرانية. وأظهرت بيانات مؤشر الأمن السيبراني العالمي أن سبع دول إفريقية فقط، وهي موريشيوس ومصر وتنزانيا وغانا وتونس ونيجيريا والمغرب، تمكنت من دخول قائمة أفضل 50 دولة في هذا المجال. وقد احتلت إثيوبيا المرتبة الأولى بين 109 دول من حيث التعرض للجرائم الإلكترونية، بينما تباينت مراكز الدول الإفريقية الأخرى، حيث جاءت زيمبابوي في المرتبة الخامسة وموزمبيق في السابعة عشرة. يعكس المؤشر التزامات الدول في مجال الأمن السيبراني من خلال خمس ركائز رئيسية: التدابير القانونية، التدابير الفنية، التدابير التنظيمية، تدابير تنمية القدرات، وتدابير التعاون. ويُعتبر المغرب الدولة الإفريقية الوحيدة التي حققت مركزاً ضمن الخمسين الأوائل في مؤشر الأمن السيبراني الوطني في تشرين الأول 2022، والذي يقيس استعداد الدول لمواجهة التهديدات السيبرانية وإدارة الحوادث المرتبطة بها. وبحسب اللجنة الاقتصادية لإفريقيا التابعة للأمم المتحدة، فإن عدم الاستعداد لمواجهة التهديدات السيبرانية قد يكلف الدول الإفريقية ما يصل إلى 10% من ناتجها المحلي الإجمالي سنوياً. وجدير بالذكر، أن الهندسة الاجتماعية دوراً في 52% من الهجمات الناجحة على المنظمات و91% على الأفراد في إفريقيا. وتشمل حوالي 29% من هذه الهجمات مواقع ويب مزيفة تحاكي صفحات المصادقة الخاصة بالشركات أو البنوك أو أنظمة الدفع.[8]

---

[6] "Global Security Outlook 2025". (2025), Insight Report, World Economy Reform, P. 30.

[7] Kurbalija, Jovan, and , Teleanu , Sorina " Stronger Digital Voices from Africa : Building African digital foreign policy and diplomacy". (2022), DiploFoundation, Federal Department of Foreign AffairsFDFA. P. 60.

[8] همام، محمود سامح . (2025)، " الهجمات السيبرانية في إفريقيا.. قراءة في التحديات والاستجابات"، مقال تحليلي، مجلة السياسة الدولية، مؤسسة الأهرام، الموقع الالكتروني، بتاريخ 25-2-2025.

00964- 7710122232 Alfaidcenter2011@gmail.com العراق - بغداد - الكرادة

2. مستوى الأمن السيبراني في أمريكا اللاتينية

شهد تمويل التهديدات في أمريكا اللاتينية تحولاً معقداً، حيث أصبحت جماعات الجريمة المنظمة تعتمد بشكل متزايد على العملات المشفرة في عمليات غسل الأموال. ويُعتبر غموض معاملات العملات المشفرة أداة جذابة لإخفاء مصادر التمويل، مما أدى إلى زيادة ملحوظة في أنشطة اختطاف العملات المشفرة في القطاع التجاري بالمنطقة. وتواجه منطقة أمريكا اللاتينية ارتفاعاً غير مسبوق في حوادث الأمن السيبراني، حيث تُصنّف البرازيل في المرتبة الثانية عالمياً من حيث معدل الجرائم الإلكترونية، بعد روسيا. ويُعتبر الأثر المالي لهذه الهجمات كبيراً، إذ تخسر الشركات البرازيلية وحدها ما يصل إلى 10 مليارات دولار أمريكي سنوياً نتيجة الجرائم الإلكترونية، بما في ذلك السرقة المالية وفقدان الملكية الفكرية واختراق المعلومات السرية. وتظهر خطورة هذه الحوادث من خلال حقيقة أن مؤسسات أمريكا اللاتينية، وفقاً لبيانات IBM Security، تواجه تكلفة متوسطة قدرها 2.56 مليون دولار أمريكي لكل خرق بيانات، بينما يبلغ متوسط الوقت اللازم لتحديد واحتواء الخرق في المنطقة 387 يوماً، مما يجعلها تحتل المرتبة الثانية عالمياً بعد "الشرق الأوسط".[9]

المحور الرابع: آفاق وسبل التعاون بين القارة الأفريقية وأمريكا اللاتينية في مكافحة الجرائم الالكترونية

شهدت قارتي أمريكا اللاتينية وأفريقيا العديد من أشكال التعاون في المجالات التجارية والاقتصادية، مما يفتح آفاقاً مهمة لتعزيز التعاون الأمني في مواجهة الجرائم الإلكترونية. إذا تتكون كل من القارتين من دول نامية تفتقر إلى تأثير كبير في النظام العالمي، سواء من حيث التقدم الاقتصادي أو التكنولوجي. علاوة على ذلك، تواجه دول الاتحاد الأفريقي ودول أمريكا اللاتينية تحديات متنوعة في مجال الأمن السيبراني، نتيجة لاختلاف السياقات السياسية والاجتماعية والثقافية. وفي ضوء ذلك هناك صوراً متنوعة في مجال التعاون الامني بين القارة الأفريقية وقارة أمريكا اللاتينية في مكافحة الجرائم الالكترونية، **يمكن توضيحها فيما يلي:**

1. التعاون في المجال التقني والفني

- تبادل الدورات التدريبية التقنية بهدف تزويد الافراد المعنيين في مجال مكافحة الجرائم الالكترونية بالوسائل الفنية والتقنية اللازمة لكشف هذه الجرائم.
- الإستفادة من تجارب التعاون الدولي الرائدة في مجال الكشف التقني عن الجرائم الالكترونية وتعقب المجرمين إلكترونياً.
- دعم البنية التحتية الرقمية في كافة دول القارة الافريقية ودول أمريكا اللاتينية، في مجال الاتصالات وتكنولوجيا المعلومات، والمؤسسات الأمنية.
- التعاون مع مزودي خدمات الإنترنت وشركات الحوسب السحابية لرصد ومنع الأنشطة والعمليات المشبوهة على الشبكة.

---

[9] "Latin America Cyber Security Market Size & Share Analysis - Growth Trends & Forecasts (2025 - 2030)", Modor Intelligence.
https://www.mordorintelligence.com/industry-reports/latin-america-cyber-security-market

00964- 7710122232 Alfaidcenter2011@gmail.com العراق - بغداد - الكرادة

- توعية المستخدمين بشأن الأمان الرقمي وسبل الإبلاغ عن الجرائم الإلكترونية، وإطلاق حملات توعوية مشتركة تسلط الضوء على مخاطر هذه الجرائم.
- تنفيذ بروتكولات التعاون مع شركات التكنولوجيا المتخصصة فى توفير الدعم الفني في مجالات التحقيق.

2. **التعاون القضائي**

- تدريب القضاة والمحققين في إفريقيا وأمريكا اللاتينية على كيفية التعامل مع الأدلة الرقمية ومكافحة الجرائم الإلكترونية.
- تبادل الخبرات القانونية بشأن أفضل الأساليب في محاكمة الجرائم الإلكترونية.
- تعزيز استخدام التقنيات المتطورة في التحليل الجنائي الرقمي للكشف عن الجرائم الإلكترونية وتعقبها.
- تطوير وسائل وطرق لتواصل المباشر بين جهات إنفاذ القانون في القارتين.
- تيسير تبادل الأدلة الرقمية بسرعة وكفاءة عبر منصات إلكترونية آمنة، مثل شبكة الإنتربول المخصصة لتبادل المعلومات الجنائية.
- وضع سياسات أمنية موحدة بين الدول الإفريقية واللاتينية لضمان حماية شاملة.
- سن وتحديث القوانين والتشريعات المنظمة للجريمة الالكترونية في كلا القارتين.
- ولمنع تداخل الاختصاص القضائي، **لابد من الاخذ في الاعتبار المبادىء التالية:**

أ. إعداد أدلة إجرائية موحدة توضح الأساليب المناسبة للتعامل مع الجرائم الإلكترونية العابرة للحدود، مع مراعاة عدم تعارض الاختصاصات.

ب. في الجريمة الالكترونية التي تمتد إلى عدة دول، يتم تحديد الاختصاص وفقاً لمدى تأثير الجريمة على كل دولة.

ت. إذا تورط مواطن من دولة إفريقية في جرائم بأمريكا اللاتينية، يتم التنسيق بين الدولتين بناءً على الاتفاقيات الموقعة بينهما.

ث. إذا كانت الجريمة الإلكترونية تستهدف أفراداً أو مؤسسات داخل دولة معينة، فإن لهذه الدولة الحق في المطالبة بالاختصاص القضائي لملاحقة الجاني.

ج. إذا كانت الجريمة قد أثرت بشكل مباشر على أمن أو اقتصاد دولة معينة، يمكن لتلك الدولة أن تطالب بالاختصاص القانوني. ومن الضروري التنسيق مع الدول الأخرى المتأثرة لتفادي الازدواجية في المحاكمة.

ح. تعزيز التعاون المستمر بين القارتين في مجال مكافحة التهديدات السيبرانية من خلال إبرام المزيد من المعاهدات والاتفاقيات الإقليمية الثنائية المشتركة، بهدف تعزيز الأمن اللازم لمكافحة الجرائم الإلكترونية وملاحقة الجناة، مما يسهم في تحقيق الأمن القومي للدول المختلفة في القارة الافريقية واللاتينية.

00964- 7710122232 Alfaidcenter2011@gmail.com العراق - بغداد - الكرادة

وأخيراً، تعكس البيانات السابقة، مدى خطورة الجرائم الإلكترونية والتهديدات السيبرانية على الأمن القومي في قارتي إفريقيا وأمريكا اللاتينية، خاصة في ظل ضعف مرونة الأمن السيبراني الذي تعاني منه العديد من دول القارتين. ويرجع ذلك إلى مجموعة من العوامل، من أبرزها نقص التشريعات والقوانين المنظمة للفضاء السيبراني، وضعف البنية التحتية الرقمية والأمنية، فضلاً عن محدودية الوعي المجتمعي والفني بمخاطر الهجمات الإلكترونية وآليات مواجهتها. ومن ثم، أصبح تعزيز التعاون الإقليمي والدولي ضرورة حتمية لمكافحة هذه الجرائم والحد من انعكاساتها الأمنية والاقتصادية المتزايدة.

وفي هذا السياق، لم تعد آثار الجرائم الإلكترونية مقتصرة على تهديد الأمن القومي بمفهومه التقليدي فحسب، بل امتدت لتشمل تهديد الاستقرار المالي والاقتصادي، خاصة ف ظل التوسع العالمي في تطبيقات التحول الرقمي والخدمات المالية الإلكترونية. وفي هذا الإطار، تُعد مصر من بين الدول التي تشهد تطوراً متسارعاً في البنية الرقمية والقطاع المالي الإلكتروني، الأمر الذي يجعلها أكثر عرضة للمخاطر السيبرانية المرتبطة في القطاع المالي، بإعتباره أكثر القطاعات تضرراً وتأثراً بالمخاطر السيبرانية.

ومن هنا، تبرز أهمية تناول انعكاسات الجرائم الإلكترونية والمخاطر السيبرانية على الاستقرار المالي المصري، نظراً لكونه أحد الأبعاد الحديثة المرتبطة بالأمن القومي والأمن الاقتصادي في العصر الرقمي.

المحور الخامس: المخاطر السيبرانية وانعكاساتها على الأمن الاقتصادي والاستقرار المالي في مصر

لم يعد الأمن السيبراني في العصر الرقمي مجرد أداة تقنية إضافية في البيئة الرقمية في ظل التطور السريع والمتصاعد في التكنولوجيا الرقمية والمالية، بل أصبح أحد الركائز الأساسية للحفاظ على استقرار أمن الاقتصادات الوطنية وتعزيز كفاءة الأنظمة المالية.

ومع التوسع المتزايد في تطبيقات التحول الرقمي داخل مصر، ازدادت درجة ارتباط القطاع المالي بالبنية التحتية التكنولوجية وشبكات الإنترنت، الأمر الذي أدى إلى اتساع نطاق التهديدات السيبرانية وارتفاع مستوى المخاطر العابرة للحدود. وفي ظل الاعتماد المتزايد على خدمات الدفع الإلكتروني والتكنولوجيا المالية، تحققت مكاسب كبيرة تتعلق بسرعة تنفيذ المعاملات وتحسين كفاءة الخدمات المالية وتعزيز الشمول المالي، إلا أن هذا التطور صاحبه ارتفاع ملحوظ في حجم وتعقيد المخاطر السيبرانية التي تستهدف المؤسسات المالية والمصرفية.

وفي هذا السياق، أصبحت الهجمات السيبرانية، مثل هجمات الفدية وسرقة البيانات والتصيد الاحتيالي، من أخطر التحديات التي تواجه الأنظمة المالية الحديثة، لما لها من آثار مباشرة وغير مباشرة على مستويات الثقة والاستقرار المالي.

ومن ثم، أصبح من الضروري تبني سياسات وآليات استباقية لتعزيز الأمن السيبراني، وتطوير الأطر التنظيمية والرقابية، والاستثمار في البنية التحتية الرقمية والكوادر البشرية المتخصصة، بما يضمن تحقيق تحول رقمي آمن ومستدام يدعم الاستقرار الاقتصادي في الأجل الطويل.

00964- 7710122232 Alfaidcenter2011@gmail.com العراق - بغداد - الكرادة

وفيما يلي، توضيح كيف يمكن أن تهدد المخاطر السيبرانية الأمن الاقتصادي والإستقرار المالي، ومن ثم الأمن القومي في مصر.

أولاً: واقع التحول الرقمي في القطاع المالي المصري

لقد شهد القطاع المالي المصري خلال السنوات الأخيرة تطوراً ملحوظاً في مؤشرات التحول الرقمي، مدفوعاً بجهود البنك المركزي المصري والدولة لتعزيز الشمول المالي وتوسيع استخدام الخدمات المالية الرقمية. ووفقاً لتقرير الاستقرار المالي الصادر عن البنك المركزي المصري لعام 2024، **برزت عدة مؤشرات تعكس تسارع وتيرة التحول الرقمي داخل القطاع المالي، من أهمها**[10]:

- **تطبيقInstaPay:** الذي حقق التطبيق نمواً متصاعداً، حيث تجاوز عدد مستخدميه 6.2 مليون مستخدم بنهاية عام 2023، مع معاملات مالية تخطت قيمتها 300 مليار جنيه مصري، وهو ما يعكس تنامي الثقة في خدمات الدفع اللحظي وتزايد الاعتماد عليها في الحياة اليومية.
- **المحافظ الإلكترونية:** ارتفع عدد المحافظ الإلكترونية إلى أكثر من 36 مليون محفظة، مما يعكس تغيراً تدريجياً في سلوك الأفراد نحو الاعتماد على الوسائل الرقمية بدلاً من التعاملات النقدية التقليدية، خاصة مع انتشار خدمات الهاتف المحمول.
- **البطاقات المصرفية:** شهدت بطاقات "ميزة" الوطنية توسعاً كبيراً، حيث تجاوز عددها 33 مليون بطاقة، في إطار جهود الدولة لتعزيز البنية التحتية للمدفوعات الإلكترونية وتشجيع المعاملات غير النقدية.

وتعكس هذه المؤشرات تنامي البنية التحتية الرقمية للقطاع المالي المصري، بما يساهم في رفع كفاءة الخدمات المالية وتحقيق مستويات أعلى من الشمول المالي. إلا أن هذا التوسع الرقمي المتسارع، صاحبه ارتفاع في حجم التحديات المتعلقة بأمن المعلومات وحماية الأنظمة المالية من التهديدات السيبرانية، الأمر الذي يتطلب ضرورة تطوير استراتيجيات فعالة لإدارة تلك المخاطر.

ثانياً: مظاهر المخاطر السيبرانية في البيئة المصرية

في ضوء التوسع الرقمي السريع، أصبح القطاع المالي المصري من أكثر القطاعات عرضة للهجمات السيبرانية، نظراً لاعتماده المكثف على البنية التكنولوجية والأنظمة الرقمية. وفي هذا الإطار، أشارت تقارير الجهاز القومي لتنظيم الاتصالات ومركز الاستجابة لطوارئ الحاسب الآلي(EG-CERT)[11]، إلى أن القطاع المالي يستحوذ على نسبة كبيرة من الهجمات الموجهة للبنية التحتية الحرجة في مصر، بما يعكس حساسية هذا القطاع وأهمية البيانات والمعاملات التي يديرها.

---

[10] البنك المركزي المصري. (2024). "الهيكل التنظيمي والمهام الاستراتيجية لقطاع الأمن السيبراني"، متاح إلكترونيا: وعية المستخدمين بشأن الأمان الرقمي وسبل الإبلاغ عن الجرائم الإلكترونية، وإطلاق حملات توعوية مشتركة تسلط الضوء على مخاطر هذه الجرائم.

[11] الجهاز القومي لتنظيم الاتصالات (2023).NTRA" الإستراتيجية الوطنية للأمن السيبراني 2023-2027". القاهرة، مصر. وعية المستخدمين بشأن الأمان الرقمي وسبل الإبلاغ عن الجرائم الإلكترونية، وإطلاق حملات توعوية مشتركة تسلط الضوء على مخاطر هذه الجرائم.

00964- 7710122232 Alfaidcenter2011@gmail.com العراق - بغداد - الكرادة

وفي ضوء ذلك، تُعد هجمات الفدية (Ransomware) من أخطر التهديدات السيبرانية التي تواجه المؤسسات المالية، حيث شهدت محاولات استهداف البنوك والمؤسسات المالية الصغيرة والمتوسطة ارتفاعاً ملحوظاً خلال السنوات الأخيرة. وتكمن خطورة هذه الهجمات في قدرتها على تعطيل الأنظمة التشغيلية وتشفير البيانات الحيوية، الأمر الذي قد يؤدي إلى توقف الأعمال وابتزاز المؤسسات مالياً مقابل استعادة بياناتها.

كما تشهد هجمات التصيد الاحتيالي (Phishing) انتشاراً متزايداً، اعتماداً على أساليب الهندسة الاجتماعية التي تستهدف استغلال ضعف الوعي الرقمي لدى المستخدمين. وقد ساهم هذا النوع من الهجمات في زيادة معدلات الاحتيال الإلكتروني وسرقة البيانات المالية، مما يؤكد أن العنصر البشري لا يزال يمثل إحدى أبرز نقاط الضعف في منظومة الأمن السيبراني.

ومن جهة أخرى، ظهرت مخاطر الطرف الثالث (Third-party Risks)، نتيجة الاعتماد المتزايد على مزودي خدمات التكنولوجيا والحوسبة السحابية، حيث يمكن أن يؤدي تعرض هذه الجهات لاختراقات أمنية إلى انتقال المخاطر بصورة غير مباشرة إلى المؤسسات المالية المرتبطة بها، وهو ما يفرض ضرورة تشديد الرقابة على مقدمي الخدمات الرقمية ووضع معايير صارمة للتعاقدات التقنية.

وبصفة عامة، تعكس هذه التطورات تصاعداً في تعقيد بيئة التهديدات السيبرانية داخل مصر، الأمر الذي يفرض تبني استراتيجيات متكاملة تجمع بين الحلول التقنية، والأطر التشريعية والتنظيمية، وبرامج التوعية المجتمعية، بهدف حماية النظام المالي وضمان استقراره في ظل التحول الرقمي المتسارع.

ثالثاً: انعكاسات المخاطر السيبرانية على الاستقرار المالي

تمثل المخاطر السيبرانية تهديداً مباشراً للاستقرار المالي، ليس فقط من خلال الخسائر التقنية أو التشغيلية، وإنما عبر تأثيراتها الواسعة على مستويات السيولة والثقة وكفاءة الأسواق المالية. **ويمكن توضيح اهم هذه الانعكاسات فيما يلي**[12]:

أ. تعطيل أنظمة الدفع والخدمات المالية

قد يؤدي أي اختراق أو تعطل في أنظمة الدفع والتسوية اللحظية، مثل نظام التسوية الإجمالية اللحظية (RTGS)، إلى اضطراب تدفقات السيولة بين البنوك وتعطيل تنفيذ المعاملات المالية. كما يمكن أن ينتج عن ذلك ارتفاع الطلب على السيولة قصيرة الأجل داخل سوق ما بين البنوك، الأمر الذي ينعكس سلباً على استقرار السوق النقدي وفعالية السياسة النقدية.

ب. التكاليف الاقتصادية المباشرة وغير المباشرة

لا تقتصر آثار الهجمات السيبرانية على الخسائر التقنية، بل تمتد لتشمل تكاليف الاستجابة للحوادث الأمنية، واستعادة البيانات، وتعويض العملاء، فضلاً عن الغرامات التنظيمية والخسائر المرتبطة بتراجع السمعة والثقة.

---

[12] Teng, H. W., Härdle, W. K., Osterrieder, J., Pele, D. T., Baals, L. J., Papavassiliou, V., ... & Molnár, B. (2026). Digital assets: risks, regulations, mitigation. Financial Innovation, 12(65). https://doi.org/10.1186/s40854-025-00848-y

00964- 7710122232 Alfaidcenter2011@gmail.com العراق - بغداد - الكرادة

وقد دفعت هذه المخاطر العديد من المؤسسات المالية المصرية إلى زيادة مخصصات الأمن السيبراني ضمن ميزانيات تكنولوجيا المعلومات، باعتباره استثماراً استراتيجياً لحماية الاستقرار المالي.

ج. تأثير الانتشار للمخاطر السيبرانية

نظراً للتشابك الكبير بين المؤسسات المالية عبر البنى التحتية الرقمية المشتركة، يمكن أن يؤدي اختراق مؤسسة مالية واحدة إلى انتقال التهديدات والبرمجيات الضارة إلى مؤسسات أخرى، مما يحول المخاطر السيبرانية من مشكلة تشغيلية محدودة إلى تهديد نظامي يؤثر على استقرار القطاع المالي بأكمله.

وتوضح هذه القنوات أن المخاطر السيبرانية أصبحت أحد المحددات الرئيسية للاستقرار المالي، وهو ما يستدعي تبني سياسات احترازية ورقابية تضع الأمن السيبراني ضمن أولويات السياسات الاقتصادية والمالية.

رابعاً: التحديات القائمة ومتطلبات الحد من المخاطر السيبرانية

تواجه مصر مجموعة من التحديات الهيكلية في مجال الأمن السيبراني، ترتبط بشكل أساسي بتسارع التحول الرقمي واتساع نطاق استخدام التكنولوجيا المالية. **ومن أبرز هذه التحديات**[13]:

1. نقص الكفاءات والمهارات في مواجهة الهجمات السيبرانية

تعاني المؤسسات من محدودية أعداد المتخصصين في الأمن السيبراني، إلى جانب استمرار هجرة الكفاءات التقنية إلى الخارج، مما يضعف القدرة على التعامل مع الهجمات المعقدة والاستجابة السريعة للحوادث الإلكترونية.

2. الاعتماد على أنظمة وتقنيات قديمة

حيث تعتمد بعض المؤسسات، وخصوصاً تلك العاملة في القطاع المالي، على أنظمة تشغيل قديمة أصبحت غير قادرة على مواكبة المتطلبات الأمنية الحديثة. هذه الأنظمة تشكل نقاط ضعف جوهرية يسهل استغلالها من قبل المهاجمين، نتيجة التعقيدات التي تواجه عملية تحديثها أو مواءمتها مع الأنظمة الرقمية المتقدمة.

وتبرز هذه التحديات أن الأمن السيبراني لم يعد مجرد شأن تقني بحت، بل أصبح قضية ذات أبعاد قومية وهيكلية تتطلب تنسيقاً فعالاً بين القطاعات التعليمية والتكنولوجية والتنظيمية. للوصول إلى المرونة السيبرانية، يتعين الاستثمار المستدام في تنمية رأس المال البشري، وترقية الأنظمة التكنولوجية والهياكل التحتية، إضافة إلى تطوير استراتيجيات إدارة المخاطر. كل ذلك يعزز من قدرة النظام المالي الرقمي على إيجاد التوازن المطلوب بين تعزيز الابتكار وضمان الاستقرار. وبناءاً على تلك التحديات، **يتطلب مواجهة وتعزيز الأمن السيبراني الاجراءات التالية:**

---

[13] الجهاز القومي لتنظيم الاتصالات (NTRA.(2023) "الإستراتيجية الوطنية للأمن السيبراني 2023-2027". القاهرة، مصر. https://www.tra.gov.eg/ar/

00964- 7710122232 Alfaidcenter2011@gmail.com العراق - بغداد - الكرادة

أ. تطوير التشريعات القوانين المنظمة: وفي هذه المجال، يعتبر قانون حماية البيانات الشخصية لعام 2020 أساساً ضرورياً لتحسين الأنظمة القانونية المتعلقة بالأمن السيبراني في مصر. ويتحقق ذلك، من خلال فرض ضوابط شديدة الصرامة على جمع ومعالجة البيانات، نظراً لأن القانون يعزز ويدعم إجراءات الحماية من الجرائم الالكترونية، ويقلل من مخاطر الانتهاكات وتسريب البيانات.

ب. اختبار القدرة على صد الهجمات السيبرانية: وهنا يجب على الجهات التنظيمية، إلزام المؤسسات المالية بإجراء اختبارات دورية تقيس قدرتها على مواجهة هجمات شديدة التعقيد والخطورة. وهذه الاختبارات سوف تساعد على التعرف المبكر على الثغرات الأمنية وتعزيز استمرار الأعمال وعدم عرقلتها أو تهديدها.

ت. تنمية وتطوير سوق التأمين السيبراني: يمثل تعزيز قطاع التأمين السيبراني خطوة استراتيجية لتخفيف الأضرار المترتبة على الهجمات السيبرانية. وهنا، يتبين أهمية دور شركات التأمين في طرح منتجات متخصصة تغطي مجموعة واسعة من الخسائر، بما في ذلك التكاليف التشغيلية وتأثيرات الأضرار المعنوية وحماية السمعة والمصداقية للمؤسسات المالية.

وفي هذا السياق، تُبرز تقنيات الذكاء الاصطناعي وأهميته في كشف الاحتيال المالي داخل البنوك المصرية، والتي أصبحت تشكل ضرورة مُلحة، لاسيما مع تطوّر أساليب الهجمات السيبرانية وتعقيدها، حيث لم تعد الأنظمة التقليدية التي تعتمد على القواعد الثابتة كافية للتصدي لهذه التحديات.

خامساً: أهمية تطبيقات الذكاء الاصطناعي في دعم الأمن السيبراني وتحقيق الأمن الإقتصادي في مصر

تكمن أهمية الذكاء الاصطناعي، فى دوره في تقديم حلول متقدمة مدعومة بالتقنيات الحديثة، مثل التحليل السلوكي في الوقت الفعلي، حيث تعتمد بعض البنوك المصرية، مثل بنك ADCB-Egypt بالشراكة مع SAS، على خوارزميات التعلم الآلي التي ترصد التغيرات غير المألوفة في أنماط الإنفاق[14].

فعلى سبيل المثال، إذا تمت معاملة مالية من موقع جغرافي غير مألوف أو بقيمة تتناقض ولاتتفق مع السجل التاريخي لنمط سلوك العميل المالي، يتم تعليق المعاملة مؤقتاً للتحقق من صحتها. فضلاً عن، تقليل الإنذارات الكاذبة، حيث أن باستخدام قدرات الذكاء الاصطناعي، يتم تعزيز دقة أنظمة الكشف لتقليل حالات التصنيف الخاطئ للمعاملات الصحيحة كأنشطة احتيالية. هذا الإجراء لا يحسن فقط من تجربة العملاء، لكنه يقلل أيضاً من الأعباء التشغيلية على عمليات المراجعة في البنوك.

أيضاً يساهم الذكاء الإصطناعي، في كشف الشبكات المنظمة للاحتيال، وذلك من خلال تطبيق تقنيات تحليل الرسوم البيانية، ويساهم ذلك في استكشاف العلاقات الخفية وغير الواضحة بين حسابات مختلفة وتظهر بصورة غير مترابطة.

---

[14] البنك المركزي المصري (2023).. " تقرير الاستقرار المالي لعام 2023"|، النصف الأول، مصر.

00964- 7710122232 Alfaidcenter2011@gmail.com العراق - بغداد - الكرادة

هذه الاجراءات والخطوات الاستباقية، من خلالها يمكن للبنوك من كشف الشبكات المعقدة والخطيرة، والتي تعمل على غسل الأموال أو تنفيذ عمليات احتيال سيبراني بطريقة ممنهجة. فالجمع بين هذه التقنيات جميعها يتيح فرص هائلة للبنوك المصرية، من تعزيز استراتيجياتها الأمنية ومواكبة التحول الرقمي بشكل قوي وفعّال ومستدام.

ولضمان تعزيز البيئة الرقمية الآمنة وتقوية البنية السيبرانية في القطاع المصرفي، قام البنك المركزي المصري خلال عام 2023 وما بعدها، بإطلاق مجموعة من الأطر والتنظيمات المصممة خصيصاً لتحقيق هذه الأهداف. **وفيما يلي أهم المبادرات والخطوات التي تم اتخاذها**[15]:

1. تنفيذ الإطار الشامل للأمن السيبراني لعام 2023، حيث ألزم البنك المركزي كافة البنوك بتبني إطار موحد للأمن السيبراني يتضمن أكثر من 200 عنصر أمني أساسي. وحتى نهاية عام 2024، تمكن البنك من إنجاز نحو 85%، من مشروع التقييم الذاتي لجاهزية الأمن السيبراني للبنوك، حيث تم فحص ومراجعة ما يقارب 30 ألف دليل امتثال لضمان الالتزام بالمعايير المحددة.

2. إنشاء وحدات مستقلة لمكافحة الاحتيال، وذلك عن طريق إلزام البنوك بتأسيس وحدات مكافحة الاحتيال كإدارات مستقلة تندرج تحت مسؤولية رئيس قطاع المخاطر، مع تقديم تقارير مباشرة إلى مجلس الإدارة. وقد منحت البنوك فترة امتثال تمتد لستة أشهر لتحقيق هذا الهدف وتنفيذ التوصيات.

3. أنشاء مركز الاستجابة لحوادث الأمن السيبراني للقطاع المالي (EG-FinCIRT)، وقد تم إنشاء هذا المركز ليشكّل خط الدفاع الأول ضد أي تهديدات سيبرانية تستهدف القطاع المالي. ويعمل المركز على مدار الساعة لرصد وتتبع الهجمات المحتملة، تحليل الأدلة الرقمية، وتوفير إنذارات مبكرة للبنوك لتجنب أو احتواء أي أضرار قبل وقوعها.

4. نظام "محافظ" للمراجعة الأمنية للتطبيقات المالية، ففي خطوة لتعزيز أمن التطبيقات المالية، اعتمد البنك المركزي نظاماً موحداً يضمن المراجعة الأمنية الدقيقة لجميع التطبيقات المالية المستجدة، بما في ذلك تطبيقات المحافظ الإلكترونية. ولا يتم السماح بإطلاق أي تطبيق جديد إلا بعد اجتيازه اختباراً شاملاً للتحقق من جاهزيته ومناعته أمام محاولات القرصنة.

بهذه الجهود، يعكس البنك المركزي المصري التزامه الراسخ بتطوير قطاع مصرفي قادر على مواجهة التطورات التكنولوجية والتهديدات السيبرانية بكفاءة وفعالية.

---

[15] المرجع السابق. & الجهاز المركزي للتعبئة العامة والإحصاء. (2024). (CAPMAS) "النشرة المعلوماتية ومؤشرات التحول الرقمي في المجتمع المصري"، متاحاً ألكترونياً على : https://www.capmas.gov.eg/mediaLanding/news/3335.

00964- 7710122232 Alfaidcenter2011@gmail.com العراق - بغداد - الكرادة

المصادر

أولاً: المصادر العربية

1. البنك المركزي المصري. (2023). "تقرير الاستقرار المالي لعام 2023"، النصف الأول، مصر.
2. البنك المركزي المصري. (2024). "الهيكل التنظيمي والمهام الاستراتيجية لقطاع الأمن السيبراني"، متاح إلكترونياً: https://www.cbe.org.eg/ar/cybersecurity/the-cybersecurity-organizational-structure.
3. الجهاز القومي لتنظيم الاتصالات (NTRA). (2023). "الاستراتيجية الوطنية للأمن السيبراني 2023-2027"، القاهرة، مصر.
4. https://www.tra.gov.eg/ar/.
5. الجهاز المركزي للتعبئة العامة والإحصاء (CAPMAS). (2024). "النشرة المعلوماتية ومؤشرات التحول الرقمي في المجتمع المصري"، متاح إلكترونياً على: https://www.capmas.gov.eg/mediaLanding/news/3335.
6. همام، محمود سامح. (2025). "الهجمات السيبرانية في إفريقيا.. قراءة في التحديات والاستجابات"، مقال تحليلي، مجلة السياسة الدولية، مؤسسة الأهرام، الموقع الإلكتروني، بتاريخ 25-2-2025.
7. مؤشر الجريمة المنظمة العالمي. (2023). فرنسا.

ثانياً: المصادر الاجنبية

1. Center for Strategic and International Studies (CSIS). Washington, D.C. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

2. "Global Security Outlook 2025". (2025). Insight Report, World Economy Reform.

3. Kurbalija, Jovan, and Teleanu, Sorina. "Stronger Digital Voices from Africa: Building African Digital Foreign Policy and Diplomacy". (2022). DiploFoundation, Federal Department of Foreign Affairs (FDFA),.

4. "Latin America Cyber Security Market Size & Share Analysis - Growth Trends & Forecasts (2025-2030)". Mordor Intelligence. https://www.mordorintelligence.com/industry-reports/latin-america-cyber-security-market.

5. "Online Crime in Africa a Bigger Threat Than Ever Before, INTERPOL Report Warns". (2020). INTERPOL. https://www.interpol.int/en/News-and-Events/News/2020/Online-crime-in-Africa-a-bigger-threat-than-ever-before-INTERPOL-report-warns.

6. Teng, H. W., Härdle, W. K., Osterrieder, J., Pele, D. T., Baals, L. J., Papavassiliou, V., ... & Molnár, B. (2026). "Digital Assets: Risks, Regulations, Mitigation". Financial Innovation, 12(65). https://doi.org/10.1186/s40854-025-00848-y.

7. Tornaghi, Cecelia. (2023). "The Dramatic Cyberattack That Put Latin America on Alert", Article, Americas Quarterly: Politics, Business & Culture in the Americas. https://www.americasquarterly.org/article/the-dramatic-cyberattack-that-put-latin-america-on-alert/.

00964- 7710122232 Alfaidcenter2011@gmail.com العراق - بغداد - الكرادة

تأسس مركز الفيض العلمي لاستطلاع الرأي والدراسات المجتمعية في بغداد بموجب شهادة التسجيل الصادرة عن الأمانة العامة لمجلس الوزراء -دائرة المنظمات غير الحكومية المرقمة (1J775330) بتاريخ ٢٠١٢/٤/٢٦، وهو مركز علمي بحثي يهتم بإجراء الاستطلاعات والدراسات الميدانية فضلا عن إعداد الأوراق البحثية والمقالات حول قضايا الحياة المجتمعية للأسرة والمواطن، والدولة بمؤسساتها المختلفة.

- لا يجوز نشر أي من إصدارات المركز ونتاجاته العلمية الا بموافقة خطية صريحة ويمكن الاقتباس بشرط ذكر المصدر كاملا.
- حقوق الطبع والنشر محفوظة لمركز الفيض العلمي لاستطلاع الرأي والدراسات المجتمعية

للتواصل

00964- 7710122232

Alfaidcenter2011@gmail.com

www.al-faidh.com

العراق - بغداد - الكرادة