الأمن السيبراني في القطاع المالي مع الإشارة لواقع الأمن السيبراني في ليبيا

*أ. وفاء إمحمد إمحمد عبد الله

الملخص:

ساهمت التطورات والابتكارات التقنية في التأثير الكبير على القطاع المالي، خاصة المصارف التي شهدت تحولاً من القنوات التقليدية إلى القنوات الالكترونية وظهور المصارف الرقمية، فجاءت هذه التحولات مترافقة مع مخاطر تتعلق بالتكنولوجيا، الأمر الذي استدعى ضرورة التركيز على الأمن السيبراني بشكل عام. واستعداد المؤسسات المالية لاتخاذ تدابير لتخفيف المخاطر المصاحبة لهذا التطور ومعالجتها. خاصة أن القطاع المصرفي يرتبط بالعديد من القطاعات الأخرى فيما يتعلق بالتمويل الأمر الذي يجعله أحد أهم الأطراف التي تدعم مختلف القطاعات الاقتصادية داخل الدولة، كما أن ليبيا أصبحت تتجه نحو التحول الرقمي، الأمر الذي يستوجب عليها قبل القيام بذلك بشكل كامل أن تعزز أمنها السيبراني لتستطيع مواجهة أثاره السلبية وما تحويه من مخاطر وهجمات سيبرانية يمكن أن يعرض قطاعها المالي للكثير من المخاطر.

الكلمات المفتاحية: الأمن السيبراني– القطاع المالي– التحول الرقمي.

المقدمة:

رافق التوسع في استخدام التكنولوجيا والتحول الرقمي بالقطاع المالي، زيادة التعرض للتهديدات والحوادث الالكترونية، كما أنه أصبح يشكل تحديًا كبيرًا، فأصبحت الهجمات الالكترونية منتشرة على نطاق واسع في هذا القطاع أكثر من غيره، فوفقًا لدراسة صادرة عن صندوق النقد العربي أن الهجمات السيبرانية التي يشهدها قطاع الخدمات المالية تفوق القطاعات الأخرى بنسبة 65%، وذلك وفق تقديرات البنك الدولي، كما أن كلفة الهجمات السيبرانية في قطاع الخدمات المالية قد تصل إلى ما يقدر 270– إلى 350 مليار دولار سنويًا حال اتساع نطاق انتشارها، بالإضافة إلى أن التكلفة الناجمة عن الهجمات السيرانية في القطاعات المالية من واقع الخسائر المحققة جراء هجمات فعلية في 50 دولة حول العالم أن متوسط الخسائر السنوية المحتملة من هذه الهجمات قد يكون

*عضو هيئة تدريس كلية الاقتصاد والعلوم السياسية، جامعة طرابلس – ليبيا

كبيرًا بما يقدر بنحو 9% من صافي دخل المصارف على مستوى العالم، أو حوالي 100 مليار دولار في حال تشابهت هذه الهجمات مع مثيلاتها السابقة.(صندوق النقد العربي، 2019)

وباعتبار القطاع المصرفي أحد القطاعات المؤثرة في الاقتصاد ككل، فهو يرتبط بالعديد من القطاعات الأخرى فيما يتعلق بالتمويل الأمر الذي يجعله أحد أهم الأطراف التي تدعم مختلف القطاعات الاقتصادية داخل الدولة. فأصبحت تشكل تهديدًا خطيرًا له، فوفقًا لتقديرات البنك الدولي فإنه في عام 2016 عانى الكثير من العملاء من الهجمات السيبرانية بنسبة 65% بما يمثل زيادة بنسبة 29% عن عام 2015، وفي فبراير 2016 تمت سرقة 81 مليون دولار من حساب البنك المركزي البنغلاديشي عبر شبكة سويفت، وفي نوفمبر من نفس العام تمت سرقة حوالي 2.5 مليون جنيه استرليني من حوالي 9000 عميل لدى بنك Tesco، وفي مايو 2019 سرق أكثر من 7000 عملة بيتكوين من بورصة العملات المشفرة Binance، وهي الأكبر في العالم من حيث الحجم.(Christian &Ansgar، 2020:ص11553). ومن جهة أخرى تعرضت المملكة المتحدة العربية السعودية للهجمات السيبرانية، وكان أبرزها عام 2013 هجوم تعرضت له جهة حكومية تسبب بأضرار بالغة لـ30000 جهاز، وفي عام 2016 تعرضت لتهديد استهدف تعطيل خدمات جهات حكومية بقطاع النقل، وعام 2017 تعرضت لتعطيل موقعين لجهات حكومية بقطاعات حيوية وتقنية.(الحديدي، 2022:ص78)، الأمر الذي جعل المؤسسات والمصارف وشركات الخدمات المالية في حاجة إلى التعامل مع النشاط الضار لمجرمي الانترنت، خاصة أن المصارف بحاجة ماسة للحفاظ على سرية بياناتها المصرفية والحفاظ على خصوصية عملائها وحمايتهم من أي عمل قد يلحق الضرر بهم، ومواجهة المخاطر والتهديدات والهجمات السيبرانية بكفاءة وفاعلية بما يضمن الحفاظ على تنظيم القطاع المصرفي والاشراف والرقابة والتدقيق لضمان جودة الخدمة وحفظ حقوق متلقيها ومقدميها.

وقد تم تصميم الأمن السيبراني في الخدمات المالية والمصرفية لحماية أصول العملاء وبياناتهم، وتعزيز إجراء المزيد من المعاملات عبر المواقع الالكترونية، كما يمكن لأدواته أن تساعد في تقليل مخاطر الأمن السيبراني والحوادث والتهديدات عبر شبكة الانترنت. وعلى ذلك فإن القطاع المصرفي لديه العديد من الفرص لتحسين أمنه السيبراني، لذلك عليه أن يركز على تعزيزه؛ حيث يمكنه اتباع تقنيات جديدة لتحسينه على شبكاته. ومن جهة أخرى وفي الوقت الذي تسعى فيه المصارف وجميع المؤسسات المالية لتحسين خدماتها ومواقعها الالكترونية إلا

أن هذه الجهود يمكن أن تضيع إذا لم تبذل الجهود لفهم أهمية الأمن السيبراني. وبذلك أصبح لزامًا على جميع المؤسسات المالية مواكبة أحدث التطورات والتقنيات المساندة لعملياتها وخدماتها ويتحتم عليها وضع استراتيجية للأمن السيبراني وتطوير الأطر القانونية والتنظيمية المنظمة له بما يساعدها على تقييم مخاطر السيبرانية ومتابعة شبكات المعلومات داخل القطاع ومراكز تكنولوجيا المعلومات.

تساؤلات الدراسة:

إن التطور السريع الحاصل في القطاع المالي والتكنولوجي قد ساهم في زيادة العقبات أمام المؤسسات المالية، كما أن الأمن السيبراني أصبح يمثل مصدر قلق للقطاع المالي، حيث يمكن أن تشن جهات فاعلة منفردة هجمات لسرقة الأموال من حسابات مصرفية فردية الأمر الذي يتسبب في اضطرابات في النظم المالية واثارة الذعر بين المواطنين فينعكس سلبًا على القطاع المالي ككل، حيث تشكل محاولات التطفل على أنظمة تكنولوجيا المعلومات للمصارف والمؤسسات المالية الأخرى خطرًا كبيرًا، فمن خلال دراسة أجرتها مؤسسة كارنيغي للسلام الدولي في عام 2020 كان عدد الهجمات الالكترونية على المؤسسات المالية يتزايد بأربعة أضعاف على أساس سنوي، كذلك بلغ متوسط تكلفة الهجمات على القطاع المالي 5.72 ملايين دولار في عام 2021، ووفقًا للتقرير الصادر عن المنتدى الاقتصادي العالمي بعنوان المخاطر العالمية في 2023، جاءت مخاطر الأمن السيبراني في المرتبة الثامنة بين المخاطر التي تهدد العالم، وجاءت في المرتبة الرابعة من المخاطر التي تهدد بيئة الأعمال. كما أوضح مسح أجراه صندوق النقد الدولي على 51 دولة خلال عام 2023، أن معظم المسؤولين الماليين في الدول النامية لم يستأنفوا إصدار لوائح للأمن السيبراني أو يتخذوا خطوات لإنقاذ تلك اللوائح، كما أن 56% من المصارف المركزية أو السلطات الرقابية على مستوى العالم ليس لديها استراتيجية إلكترونية وطنية للقطاع المالي، وحوالي 42% يفتقرون إلى نظام مخصص للأمن السيبراني أو إدارة مخاطر التكنولوجيا، وحوالي 68% يفتقرون إلى وحدة مخاطر متخصصة، وما يقرب 64% لم يقوموا بإجراء اختبارات للأمن السيبراني لديهم أو تقديم الإرشادات لتعزيزه، وحوالي 54% يفتقرون إلى نظام مخصص للإبلاغ عن الحوادث السيبرانية، و48% ليس لديهم لوائح للجرائم الالكترونية.(هند مختار، 2023: https://www.youm7.com/6130353). من هنا يتضح لنا أن تأمين البيانات والحفاظ على السرية أصبح يشكل تحديًا كبيرًا أمام القطاع المالي، وعلى الرغم من ذلك فإن معظم المؤسسات المالية خاصة في المنطقة العربية، لم تتخذ خطوات لتعزيز الأمن السيبراني لديها بشكل كافي. وعلى ما سبق جاءت هذه الدراسة لإيجاد إجابات حول التساؤلات التالية:

- ما أهمية الدور الذي يقوم به الأمن السيبراني بالقطاع المالي؟
- ماهي التهديدات التي يمكن أن تهدد القطاع المصرفي الالكتروني؟
- ماهي التحديات التي تواجه المنطقة العربية لتعزيز أمنها السيبراني؟
- ماهي أهم المخاطر السيبرانية التي يواجهها القطاع المالي والمصرفي؟
- كيف يمكن بناء قدرات ناجحة للأمن السيبراني بالدول العربية؟

أهداف الدراسة: تهدف الدراسة إلى إلقاء الضوء على ما يتعلق بالأمن السيبراني بالقطاع المالي وذلك من خلال:

1. التعرف على أهمية الأمن السيبراني بالقطاع المالي.
2. التعرف على أهم التهديدات والمخاطر السيبرانية التي تواجه القطاع المالي.
3. التعرف على التحديات التي تواجه المنطقة العربية فيما يخص أمنها السيبراني.
4. التعرف على واقع الأمن السيبراني في ليبيا.
5. معرفة كيف يمكن للدول العربية أن تعزز أمنها السيبراني.

أهمية الدراسة:

تأتي أهمية الدراسة من خلال ما يحويه موضوع الأمن السيبراني من أهمية، والحال الذي يمكن أن تؤول إليه المؤسسات المالية في حالة قيامها بمواكبة التطورات والابتكارات التقنية والتكنولوجيا، بدون أن تضع أطر قانونية وتنظيمية تضمن لها القيام بأعمالها بكل أمان وبشكل يساعدها على الحد من التأثيرات السلبية للتحول الرقمي، خاصة فيما يخص المؤسسات المصرفية كونها أصبحت تشكل المحرك الأساسي للنشاط الاقتصادي، وذلك من خلال ما تقوم به من توجيه المدخرات نحو استثمارها في مشاريع استثمارية وانتاجية، إضافة إلى تسهيل عمليات الدفع والتحصيل، فقد أصبحت المصارف تواجه تحديات التكيف والابتكار والتعامل مع هذه التطورات، بما يعزز قدراتها على وضع سياساتها المالية وصقل جودتها بهدف تحسين خدماتها ونشاطها، مما أوجب عليها ضرورة الاهتمام بتعزيز أمنها السيبراني بشكل تطبيقي.

منهجية الدارسة:

تم الاعتماد على المنهج الاستقرائي بأداتيه الوصف والتحليل؛ وذلك من خلال الرجوع إلى مختلف الأدبيات النظرية والتطبيقية والتقارير؛ بهدف التعرف على الجوانب النظرية المتعلقة بالأمن السيبراني وما يحتويه من

مخاطر وتهديدات للقطاع المالي، بالإضافة إلى إجراء المقابلات الشخصية مع ذوي الاختصاص وعلاقتهم المباشرة بموضوع الدراسة.

الدراسات السابقة:

1. دراسة جغل وزقرير(2023) بعنوان الأمن السيبراني والشمول المالي في ظل التحول الرقمي للقطاع المالي(التهديدات السيبرانية، آليات التحوط. هدفت الدراسة إلى تسليط الضوء على أهمية الأمن السيبراني ضمن استراتيجية التحول الرقمي للقطاع المالي لتوسيع نطاق الشمول المالي. وقد توصلت الدراسة إلى نتائج أهمها أن التحول الرقمي حقق انجازًا كبيرًا في زيادة معدلات الشمول المالي، ولكن في نفس الوقت جلب مخاطر سيبرانية تفوق حجم الكوارث الطبيعية وأصبحت تهدد الاستقرار المالي والنظام المالي بأكمله، وقد أوصت الدراسة بأنه يجب على الهيئات المعنية بالشمول المالي توعية العملاء بمخاطر الأمن السيبراني، كما يجب توحيد الجهود الدولية في صد هذه الهجمات الالكترونية، وعلى الدول النامية إعادة النظر في تدابير الأمن السيبراني لديها والاقتداء بالدول الرائدة في الأمن السيبراني.
2. دراسة رضا وجواد(2023) بعنوان واقع الأمن السيبراني في البنوك الالكتروني العراقية، هدفت هذه الدراسة إلى التعريف بمفهوم الأمن السيبراني وأهدافه وأبعاده، بالإضافة إلى التعريف بمفهوم البنوك الالكترونية، وقد توصلت الدراسة إلى نتائج أهمها أن الفضاء الالكتروني الحر يقدم خدمات لا غنى عنها في جميع مفاصل الحياة، وقد بدأ العراق يهتم بمجال الأمن السيبراني فقد تم استحداث الدراسات العليا في ثلاث جامعات عراقية ، وتم تشكيل فريق وطني مختص بهذا المجال، أما فيما يخص قانون درائم المعلوماتية فإنه لا زال معلقًا على الرغم من طرح أول مسودة للقانون في عام 2011، ولغاية 2021، ولم يقر هذا القانون في مجلس النواب والسبب يرجع إلى أن المشرعين لهذا القانون يحاولون تقييد حرية التعبير والرأي، وأن عدم اقرار هذا القانون له آثار كبيرة على الأمن السيبراني للبلدان في الجانب المالي فقد أصدر صندوق النقد الدولي حزمة من التوصيات في مجال الأمن السيبراني الخاص بالبنوك والتي على الدول الالتزام بها لتكون بمأمن من الهجمات السيبراني وفي العراق البنك المركزي العراقي ملتزم بهذه التوصيات وذلك بالرجوع إلى مهام أحد أهم دوائره وهي تقنية المعلومات والاتصالات.
3. دراسة صواق وآخرون(2023) بعنوان أثر جاهزية الأمن السيبراني على الخدمات المصرفية الالكترونية من خلال تقليل المخاطر المدركة. هدفت هذه الدراسة إلى تسليط الضوء على أثر جاهزية البيئة المادية والبشرية

للأمن السيبرانية على استخدام الخدمات المصرفية الالكترونية، وقد توصلت الدراسة إلى وجود علاقة تأثير غير مباشرة لبعدي جاهزية البيئة المادية والبشرية للأمن السيبراني في استخدام الخدمات المصرفية الالكترونية من خلال تقليل المخاطر المدركة للعملاء، وقد أوصت الدراسة بضرورة اعتماد بنك التنمية المحلية بغرداية آليات لتقليل المخاطر المدركة للعملاء، كون العميل يفضل التعامل مع البنك الذي يعالج عناصر المخاطر بنجاح ويقدم خدمات مصرفية إلكترونية موثوقة وآمنة.

4. دراسة يعقوب وآخرون(2022) بعنوان مؤشر مقترح للإفصاح المحاسبي عن المخاطر السيبرانية في سوق العراق للأوراق المالية على وفق المتطلبات الدولية. وقد هدفت هذه الدراسة إلى اقتراح مؤشر للإفصاح عن المخاطر السيبرانية في التقارير السنوية، وقد توصلت الدراسة إلى نتائج كان أهمها برز الاهتمام بالإفصاح عن المخاطر السيبرانية خصوصًا بعد ازدياد الهجمات السيبرانية على جميع القطاعات. وقد أوصت الدراسة بأهمية تضمين مخاطر الأمن السيبراني كأحد المقررات الدراسية في مرحلة البكالوريوس والجامعة. بالإضافة إلى تبني المؤشر المقترح للإفصاح عن مخاطر الأمن السيبراني في سوق العراق للأوراق المالية.
5. دراسة البغدادي(2021) بعنوان اقتصاديات الأمن السيبراني في القطاع المصرفي، وقد هدفت هذه الدراسة إلى إبراز التحديات التي تواجه المجتمع من أجل تحقيق الأمن السيبراني، وقد توصلت الدراسة إلى أن الطبيعة المتطورة للمخاطر السيبرانية ليست قابلة للتنظيم بشكل محدد، كما أن القضايا الخاصة بالأنترنت يمكن معالجتها من خلال اللوائح المتعلقة بكل من المخاطر التشغيلية والتقنيات. وقد أوصت الدراسة بضرورة وضع أسس لمراجعة وإدارة هذه المخاطر والتحديد الدقيق لمسئوليات مختلف الجهات، وضرورة قيام الأجهزة الرقابية بتوفير الدورات التدريبية العالية المستوى وتنظيم الندوات، والعمل على تكثيف التوعية لدى العملاء من خلال البرامج المسموعة والمرئية والندوات التثقيفية لرفع المستوى الخاص بثقافة الأمن السيبراني لدى المتعاملين بالقطاع المالي والمصرفي، كما أن الدول العربية تحتاج للمزيد من الاستثمار في مجال الأمن السيبراني من خلال توطين التكنولوجيا والبنى التحتية السيبرانية.
6. دراسة السمحان(2020) بعنوان متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود. هدفت هذه الدراسة معرفة متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، وقد توصلت هذه الدراسة إلى أن هناك عدة تعليمات يمكن أن تساعد في الحفاظ على مستوى جيد من الأمان والسلامة السيبرانية أهمها ضرورة عمل نسخ احتياطية لملفات المعلومات بانتظام لمنع هجمات الأمان

على الانترنت. وبالتالي فقد أوصت الدراسة منها التأكيد على ضرورة اهتمام جامعة الملك سعود بمتطلبات حماية أنظمة المعلومات الإدارية بالجامعة، وإدراج مجال الفضاء السيبراني ضمن مناهج التعليم في المملكة، وتوعية العاملين بكافة مؤسسات الدولة وتنمية المعايير المهنية لديهم.

7. دراسة علي ومحمد(2020) الأمن السيبراني في دول مجلس التعاون لدول الخليج العربية بمنظور جيوبولتيكي معاصر، هدفت هذه الدراسة إلى دراسة جيوبوليتك الأمن السيبراني ومعرفة مرتكزات القوة السيبرانية لدول مجلس التعاون لدول الخليج العربية واستراتيجية الروع التي تمتلكها هذه الدول في مواجهة أخطار الهجمات السيبرانية، وقد توصلت الدراسة دون أن تقدم أي توصيات أهمها أن قضية الأمن السيبراني على رأس أولويات قضايا الأمن القومي لدول مجلس التعاون في محاولة لمواجهة تصاعد التهديدات السيبرانية، بالإضافة إلى تبني دول مجلس التعاون استراتيجيات وطنية تعمل على محوري الدفاع والهجوم بهدف تحقيق الردع السيبراني؛ وذلك من خلال تعظيم معايير الأمن للشبكات الالكترونية فضلاً عن اعتماد سياسة الدفاع الالكتروني المشترك.

التعقيب على الدراسات السابقة:

معظم الدراسات السابقة أكدت أن التحول الرقمي والتكنولوجي ساهم بشكل كبير على تعزيز الأمن السيبراني، فبالرغم من الفوائد العظيمة التي يمكن أن تجنيها المؤسسات المالية والخدمية من وراء هذا التطور، إلا أنه جلب معه مخاطر سيبرانية أصبحت تشكل خطرًا كبيرًا يهدد العمل المؤسسي والمالي. الأمر الذي أصبح يستدعي معه ضرورة الاهتمام بإدارة هذه المخاطر بشكل فعال ودقيق في مختلف المجالات، والأمر الذي لا يمكن أن يتم دون وجود وعي كامل بخطورة وجود مثل هذه المخاطر، وأهمية تحقيق متطلبات ومهارات الأمن السيبراني.

مفهوم الأمن السيبراني:

يعتبر الأمن السيبراني من أهم أولويات المؤسسات المالية والتي من بينها المصارف وذلك حرصًا منها على خلق بيئة مصرفية آمنة لحماية بيانات العملاء والموظفين المالية والشخصية، وحماية المرتكزات الرئيسية التي يقوم عليها أمن وحماية المعلومات الذي أصبح ملازمًا للأمن السيبراني، بالإضافة إلى سعيها الدائم لتطوير استراتيجياتها لمواجهة التهديدات السيبرانية.

وقد عرف الأمن السيبراني بأنه النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات، ويضمن إمكانية الحد من الخسائر والأضرار التي تترتب في حالة تحقق المخاطر والتهديدات، كما

يتيح إعادة الوضع إلى ما كان عليه بأسرع وقت ممكن، بحيث لا تتوقف عجلة الإنتاج ومن ثم لا تتحول الأضرار إلى خسائر دائمة. (شمران، 2022: ص495). كما عرف الأمن السيبراني بأنه مجموعة الوسائل التقنية والتنظيمية والإدارية التي يتم استخدامها لحماية الشبكات والأجهزة والبرامج والبيانات من الهجمات أو الأضرار أو الوصول غير المصرح به وسوء الاستغلال.(علي ومحمد، 2023: ص373)

وعلى ما سبق ترى الباحثة أن الأمن السيبراني هو القيام بإجراءات أمنية تستهدف حماية أنظمة المعلومات والعمليات التي تحدث؛ للحد من التأثيرات السلبية للتطور والتوسع والتحول الرقمي وتكنولوجيا المعلومات وزيادة استخدام الشبكة العنكبوتية من قبل الأفراد والمؤسسات المالية، مما يجعلهم يستخدمون هذه التكنولوجيا دون الخوف من الهجمات الالكترونية.

أهمية الأمن السيبراني:

للأمن السيبراني أهمية كبيرة في كافة المجالات تتمثل فيما يلي: العمارات، (الحمامصة، 2022:ص35)

1- توفير الحماية الفائقة لخصوصية المعلومات والإبقاء على سريتها؛ وذلك لعدم السماح لغير المخولين بالوصول إليها واستخدامها.
2- الحفاظ على المعلومات وسلامتها وتجانسها، وذلك بكف الأيادي من العبث بها.
3- تحقيق وفرة البيانات وجاهزيتها عند الحاجة إليها، مع توفير بيئة عمل آمنة.
4- حماية الأجهزة والشبكات ككل من الاختراقات لتكون درع واقٍ للبيانات والمعلومات.
5- استكشاف نقاط الضعف والثغرات في الأنظمة ومعالجتها.
6- استخدام الأدوات الخاصة بالمصادر المفتوحة وتطويرها لتحقيق مبادئ الأمن السيبراني.

البعد الاقتصادي للأمن السيبراني:

يرتبط الأمن السيبراني ارتباطًا وثيقًا بالاقتصاد، فالتزامن واضح، بين اقتصاد المعرفة وتوسع استخدام تقنيات المعلومات والاتصالات، كما بالقيمة التي تمثلها البيانات والمعلومات المتداولة، التي تتيح تعزيز التنمية الاقتصادية لبلدان كثيرة عبر استفادتها من فرص الاستخدام التي تقدمها الشركات الكبرى التي تبحث عن إدارة كلفة انتاجها بأفضل الشروط إلا أن هذا الواقع المشرق، يطرح مسائل مختلفة سواء ما يتعلق منها بحماية مقدم الخدمة والعمل أو بحماية المستهلك على الأنترنت ويضاف إلى ذلك دخول العالم عصر المال الالكتروني ضمن بيئة تقنية متحركة بعد إطلاق خدمات المحفظة الالكترونية، إذ تتزايد استثمارات المصارف والمؤسسات المالية في

مجال المال الرقمي وتتنافس الشركات على إصدار تطبيقات تسمح بآليات دفع أمنة، ويحفظ المال في المحفظة الالكترونية وبالبقاء من خلالها وبالاستخدام كرصيد افتراضي وقد وضعت بعض الدول تشريعات خاصة بهذا المال وغني عن القول ما يمكن أن يثيره هذا الأمر من صعوبات.(العمارات والحمامصة، 2022:ص31)

وإذا ما نظرنا إلى الدول الكبرى نجد بأنها تتنافس بشراسة على موقع الصدارة في العالم السيبراني. وليس أدل على هذا من حرب تجارية اندلعت بين الولايات المتحدة والصين تمحورت حول منع شركة Huwawei الصينية الكبرى المصنعة للتكنولوجيا من دخول السوق الأمريكية في ظل اتهامات لها بالتلاعب والتجسس لصالح الحكومة الصينية. حذر الكثيرون من أن تنافسًا سيبرانيًا بين الولايات المتحدة والصين كفيل بالإضرار بالاقتصاد العالمي ككل. بل تتنافس السرديات حول الفضاء السيبراني كذلك. تطرح الصين استراتيجيتها الدولية للتعاون في الفضاء السيبراني بوصفها استراتيجية بديلة عن استراتيجية القوى الكبرى الغربية في إدارة العلاقات السيبرانية. تؤكد الصين أن استراتيجيتها قائمة على المنافع المشتركة لكل الدول والمناطق بلا استثناء، وعلى احترام مبدأ السيادة بحيث لا تستخدم الدول الأنترنت للتدخل في شؤن الدول الأخرى، وعلى تجنب سباقات التسلح وسياسات الردع في الفضاء السيبراني لما لها من تأثير سلبي على السلم والأمن الدوليين، تقوم الاستراتيجية على التنافس الحر والعادل وتروج لأهمية إتاحة فرصة المشاركة المتكافئة للجميع في الفضاء السيبراني من خلال إتاحة التكنولوجيا اللازمة لهذا الأمر ومن خلال إتاحة فرص متساوية لجميع اللغات وإتاحة فرص للتبادل الثقافي والحضاري بين الشعوب جميعها خدمة للإنسانية. تتنافس الصين بسرديتها عن الفضاء السيبراني واقعًا سيبرانيًا يبدوا منحازًا لمصالح الدول الكبرى الغربية على حساب الدول غير الغربية، صغيرها وكبيرها. (مركز الحضارة للدراسات والبحوث، 2022: ص56ص66)

وفي المنطقة العربية نجد أنه على مدى السنوات الأخيرة الماضية، شهدت المنطقة نموًا مستمرًا ولكن بطيئًا في معظم مجالات البنية التحتية لتكنولوجيا المعلومات والاتصالات والوصول إليها واستخدامها، حيث إن 85.9% من المنازل لديها وصول للأنترنت المنزلي و 52.8% من المنازل يتواجد بها جهاز كمبيوتر و67.6%من الشباب في الفئة العمرية بين 24-15 عامًا لديهم القدرة على الوصول للأنترنت، ويعتبر سوق الهاتف المحمول في المنطقة العربية متقدمًا للغاية في بعض الأجزاء، حيث تتجاوز الاشتراكات بخدمات الهاتف المحمول 100 اشتراك لكل 100 نسمة في 11 دولة من دول المنطقة تضم دول مجلس التعاون الخليجي بالإضافة إلى المغرب وتونس وسوريا والجزائر وموريتانيا، وفي المجمل فإن متوسط معدل الاشتراك في خدمات الهاتف المحمول لعام 2020

يقدر بـ 98 لكل 100 نسمة وهي أقل من المتوسط العالمي البالغ 105 اشتراكات لكل 100 نسمة وهي أقل من المتوسط العالمي البالغ 105 اشتراكات لكل 100 نسمة، وفي المجمل فإن الدول الفقيرة أو الأقل تنمية لا يوجد لديها خدمات انترنت واتصالات جيدة، وهي تتوزع على نطاق دول الجنوب في مناطق مختلفة، ولا تزال بعيدة جدًا عن المعدلات العالمية الخاصة بالمؤشرات السابقة المتعلقة بالأسر التي لديها اتصال بالأنترنت أو معدل استخدام الشباب لخدمات الأنترنت ومعدلات الاشتراكات في خدمات الأنترنت بالهواتف. ومن ناحية أخرى تختلف حظوظ الدول الفقيرة مقارنة بالدول الغنية من حيث القدرة على الاستفادة من عوائد الأنترنت وبالمثل تختلف حظوظ الفقراء عن حظوظ الأغنياء داخل الدولة ذاتها، وهو واقع يرمز إليها البعض بالفجوة الرقمية العالمية، كما أن الدول النامية بوجه عام أقل قدرة على الاستفادة من هذا الفضاء بسبب ضعف سرعات الأنترنت وبسبب الرقابة الحكومية التي تمارسها الدولة على انسياب المعلومات إلى المواطنين ومنهم تتميز المجتمعات النامية بوجود أجيال اتصال مختلفة في داخلها، فبينما تنعزل أجزاء من الشعب خاصة في الريف والمناطق النائية تمامًا عن التطورات الحديثة يعيش البعض في جيل أكثر تقدمًا من أجيال الاتصال والتواصل، فيملك ربما محمولاً تقليديًا أو هاتفًا أرضيًا، بينما يتصل الجيل الثالث بالأنترنت والأقمار الصناعية ويعيش واقعًا معولمًا مختلفًا بالكلية، بضغط هذه الانقسامات على البنية المجتمعية للدول النامية وتماسكها، بينما تقل هذه الانقسامات بشكل واضح في المجتمعات المتقدمة حيث يشارك معظم أبناء هذه المجتمعات بنسب تزيد عن 80% في الفضاء السيبراني، كما هو الحال الولايات المتحدة التي تصل نسبة المشاركين في الفضاء السيبراني فيها إلى قرابة 90%، ليست الدول سواسية، ولا حتى في الفضاء السيبراني. (سمير، 2022، ص ص66 67) ويمكن تقسيم مجالات الاقتصاد السيبراني لثلاثة مجالات رئيسية هي:(شادي، 2022: ص 85ص92)

1. المؤسسة للرقمنة: تتمثل هذه المجالات الصناعية المؤسسة للعالم الرقمي، وهي في جلها صناعات تقليدية، ولكن يعتمد البناء الرقمي عليها، فهي بنيته التحتية بشكل أساسي ، وتشمل:

أ. الاتصالات: والتي تشهد ثورة هائلة تتمثل في الجيل الخامس من الاتصالات والتي لا تمثل، بل نقلة كبيرة على مستوى التعقيد والبناء ستسمح بسرعات غير مسبوقة في الاتصالات بالأنترنت، وصناعات رقمية لم يكن ممكناً تطبيقها من قبل نظرًا لعدم وجود البنية التحتية اللازمة.

ب. صناعة الأجهزة: التطور الهائل في الاتصالات يرتبط أيضًا بتطور هائل في الأجهزة التي يتم استخدامها في الولوج للشبكة الرقمية واستخدام هذه القدرات الجديدة في عالم الاتصالات، وبالتحديد أجهزة الهاتف

المحمول التي تمثل حوالي 90% من مستخدمي الانترنت في العالم، بما يعادل حوالي 4.28 مليار مستخدمي عالميًا.

ج. صناعة وخدمات المعلومات: إن صناعة وخدمات المعلومات بما تضمه من معالجة للبيانات، وتكنولوجيا المعلومات، والحوسبة، تشكل جزء مهمًا في البنية التحتية للمجال الرقمي.

2. الاقتصاد الرقمي: هنا تكمن المساحات الأشهر للعالم الرقمي؛ حيث تقبع المنصات والتطبيقات وغير ذلك من منتجات العالم الرقمي، وهي مساحات تتطور بشدة كل يوم، لذا يمكن الإشارة لعدد من أهم هذه المساحات كمنصات التواصل، الاقتصاد التشاركي، والبرمجيات والمنصات والبنية التحتية.

3. الاقتصاد المرقمن: هذا النوع من المجالات يضم كافة الأعمال التي على أرض الواقع ، ولكن تم تعزيزها من خلال الفضاء السيبراني، ويمكن أن نذكر أهم التطورات التي قدمها الانترنت لهذه الأعمال فيما يلي:

أ. التجارة الالكترونية والتي تمثل أشهر التطورات التي أنتجها الاقتصاد الرقمي لتطوير المجالات الاقتصادية التقليدية، فمن عالم تحكمه منافذ البيع التقليدية، الذي يذهب لها المستخدم كي يشتري احتياجاتها من البضائع المختلفة، إلى عالم لم يعد المستخدم فيها لحاجة لأي شيء سوى وجود قدرة شرائية، فمنصات التجارة الالكترونية لم تعد فقد تقدم خدمات الشراء عبر الانترنت وتقوم بتوصيل المنتجات المطلوبة بأسرع وقت.

ب. التكنولوجيا المالية: لم يقتصر مجال التكنولوجيا المالية فقط على المدفوعات، بل تعداها لمناحي كثيرة، فمن ناجية ظهرت مجالات الاقراض الصغير ومتناهي الصغر وهي لا تتعلق فقط بالقيمة الصغيرة للقروض ولكن بإتاحة مساحة للاقتراض لمن لا يستطيع أن يستفيد من خدمات المصارف في هذا الاطار نظراً لعدم امتلاكه حسابات مصرفية أو عدم تأهله لتقديم ضمانات للقروض هنا تتحقق قدرة العميل على الدفع عبر مراجعة بيانات الهاتف التي يسمح بها من خلال التطبيقات المخصصة لهذا الغرض، ومن ثم التحقق من أماكن زياراته ومن اتمامه لمدفوعاته بشكل منتظم ودفع فواتيره في مواعيدها، وهو ما يتيح في النهاية قدرة الحصول على قروض متنوعة الأحجام في ظرف دقائق معدودة.

أنواع الجرائم السيبرانية:

هناك عدة جرائم تنطوي تحت مظلة الجرائم السيبرانية هي الآتية:(العمارات، 2023: ص45ص47)

1- جرائم التعدي على البيانات المعلوماتية: وهي جرائم اعتراض بيانات معلوماتية، والبيانات هي كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة الحاسب الآلي، كالأرقام والحروف والرموز وما إلى ذلك.

2- جرائم التعدي على الأنظمة المعلوماتية: تشمل جرائم الولوج غير المشرع إلى نظام معلوماتي أو المكوث فيه، وجرائم إعاقة عمل معلوماتي، النظام المعلوماتي في مجموعة البرامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات.

3- إساءة استعمال الأجهزة أو البرامج المعلوماتية: تتضمن كل من قدم أو أنتج أو ووزع أو حاز بغرض الاستخدام جهازًا أو برنامجًا معلوماتيًا أو أي بيانات معلوماتية معدة أو كلمات سر أو كودات دخول، وذلك بعرض اقتراف أي من الجرائم المنصوص عليها سابقًا.

4- الجرائم الواقعة على الأموال: مثل الاحتيال والغش بوسيلة معلوماتية و جرم الاختلاس أو سرقة أموال بوسيلة معلوماتية، وجرم أعمال التسويق والترويج غير المرغوب فيها، كذلك جرم الاطلاع على معلومات سرية.

5- جرائم التعدي على الملكية الفكرية للأعمال الرقمية: تشمل جرائم وضع اسم مختلس على عمل، وجرم تقليد عمل رقمي أو قرصنة البرمجيات، وجرم بيع أو عرض عمل مقلد أو وضعه في التداول، وجرم الاعتداء على أي حق من حقوق المؤلف أو الحقوق المجاورة.

6- جرائم البطاقات المصرفية والنقود الإلكترونية: تشمل أعمال تقليد بطاقات مصرفية بصورة غير مشروعة واستعمالها عن قصد، وتزوير إلكترونية بصورة غير مشروعة عن قصد.

7- الجرائم التي تمس المعلومات الشخصية: هي كل ما تتعلق بمعالجة البيانات ذات الطابع الشخصي دون حيازة تصريح مسبق، وإنشاء معلومات ذات طابع شخصي لأشخاص لا يحق لهم الاطلاع عليها.

8- جرائم العنصرية بوسائل معلوماتية: كجرم نشر وتوزيع المعلومات العنصرية، وجرم توزيع معلومات بوسيلة إلكترونية من شأنها إنكار، أو تشويه أو تبرير أعمال جماعية أو جرائم ضد الانسانية.

9- جرائم تشفير المعلومات: تشمل أفعال تصدير أو استيراد وسائل تشفير، وأفعال تقديم وسائل تشفير تؤمن السرية بلا حيازة تصريح من قبل المراجع الرسمية المختصة في الدولة، وأيضاً بيع أو تسويق أو تأجير وسائل تشفير ممنوع.

أنواع التهديدات المرتبطة بالقنوات المصرفية الالكترونية:

ذكر تقرير صندوق النقد العربي أن أبرز أنواع التهديدات المرتبطة بالقنوات الالكترونية على القطاع المصرفي تتمثل فيما يلي: (صندوق النقد العربي، ص ص 11-9)

1. استهداف البنية التحتية: استهداف أبرز الهجمات الالكترونية تعطيل عمل البنية التحتية للمصرف، ومن أشهر أنواع التهديدات ما يلي:

أ. البرمجيات الخبيثة وتعطيل الخدمة: وهي برمجية إدراجها عمدًا في نظام الحاسوب لأغراض ضارة. وعندما يتم تثبيت البرمجية الخبيثة فقد يصعب جدًا ازالتها. قد يتراوح أذاها من إزعاج بسيط كبعض النوافذ الإعلانية خلال عمل المستخدم، إلى أذى غير قابل للإصلاح يتطلب مثلاً إعادة تهيئة القرص الصلب كالفيروسات. ويستخدم القراصنة أساليب لاختراق أو تعطيل شبكات الحاسوب، وقد يكون الضرر يقتصر على سرقة معلومات محددة أو يكون مدمرًا يؤدي إلى تعطيل شبكة بأكملها.

ب. استغلال الثغرات: ويسمى بالهجوم دون انتظار، وهو استغلال نقاط الضعف في برمجيات وثغراتها الأمنية خاصة غير المعروفة منها للعامة. وكلما تأخر اكتشاف الثغرة منح ذلك مزيد من الوقت للمهاجمين في توسيع نطاق الهجوم وإضافة ضحايا جدد.

ج. استهداف الهواتف الذكية: ويرتبط بهذا التهديد مجموعة من الحقائق التالية:

- أغلب المستخدمين لا يلم بصفة عامة بالمخاطر الأمنية للهواتف الذكية.
- انتشار استخدام الهواتف الذكية أدى إلى زياد لجوء القراصنة لبرمجة التطبيقات الخبيثة.
- التحايل على مالكي الهواتف لتوجيههم على تحميل تطبيق خاضع لسيطرة من قبل القراصنة.
- دخول العملاء من خلالهم لحساباتهم المصرفية مما يتيح الفرصة لقراصنة المعلومات المصرفية من الدخول على تلك الحسابات أو اصابة النظام الالكتروني للمصرف بالفيروسات التي تسبب عطل النظام أو بعض أجزائه.

2. الرسائل المزيفة عبر وسائل الاتصال المختلفة: إن الاستدراج هو هجوم على هوية شخص قد يكون عميلاً لأحد المصارف، وغالبًا ما ينطوي على طلب للمستخدمين بالكشف عن تفاصيل شخصية عبر موقع وهمي على الشبكة العنكبوتية، أو باستخدام المكالمات الهاتفية والرسائل النصية.

إدارة مخاطر الأمن السيبراني في المصارف:

تعتمد المصارف على التكنولوجيا السيبرانية، ولكنها تصبح عرضة للأمن السيبراني، وضرورة استراتيجية للمصارف لمكافحة الأمن السيبراني، وتعد إدارة المخاطر السيبرانية مجالاً تقنيًا بطبيعته، ويعتمد الكثير من البيانات المتاحة على مؤشرات تقنية خاصة بالهجمات والأنظمة خاصة بتكنولوجيا المعلومات، في حين أن هذا يتيح استخبارات التهديد السيبراني والوظائف الفنية الأخرى، فإنه لا يمكن الوصول إليه بسهولة لعالم الاجتماع أو الاقتصادي الذي يتطلع إلى تحديد علاقات معينة في البيانات. هناك تعقيد آخر وهو أن البيانات التقنية لتكنولوجيا المعلومات نادرًا ما يتم جمعها جنبًا إلى جنب مع مقاييس التأثير. كما أن معظم مصادر البيانات الموضحة أعلاه هي من مصادر مختلفة ويتم توفيرها من قبل بائعين مختلفين. إن التوجيهات التنظيمية المتعلقة بإدارة المخاطر الالكترونية يمكن أن يعزز التصنيف المشترك لعمل الوكالات التنظيمية والإشرافية في توفير التوجيه المتعلق بالأمن السيبراني والمرونة الالكترونية، بما في ذلك تحديد الممارسات الفعالة أو التهديدات الناشئة، والمساعدة في استخدام لغة مشتركة لتعزيز الأساليب التنظيمية الفعالة مع تقليل مخاطر المتطلبات التنظيمية والإشرافية المتكررة والمتضاربة، وقد تم تطوير معايير جديدة للإبلاغ عن معلومات المخاطر السيبرانية في السنوات الأخيرة عن طريق ORX للمخاطر الالكترونية وأمن المعلومات CISR بما في ذلك حجم الخسائر ومصدرها، ومعلومات عن الجهات الفاعلة في التهديد وهدفها، ونوع أصول تكنولوجيا المعلومات التي تم اختراقها، والثغرة الأمنية المحددة (ضعف البرامج) التي تم استغلالها. كما أن الافتقار إلى قدرات الحماية الكافية يمكن أن يعرض البيانات لخطر انتهاكات البيانات. في ضوء ذلك، هناك متطلبات من اتفاقية بازل وحوكمة المصارف تتعلق بالأمن السيبراني وتدابير حماية البيانات لمقدمي خدمات الدفع عبر الحدود. والغرض من هذه المتطلبات هو تسهيل الحد الأدنى المعياري لمستوى الأمن السيبراني بالنظر إلى الطبيعة المتطورة للهجمات السيبرانية. حيث تتضمن هذه المتطلبات تدقيق المخاطر الالكترونية من مزودي الخدمة الخارجيين، بما في ذلك المصدر الأجنبي، ويعتبر هذا أمرًا بالغ الأهمية عند التخفيف من المخاطر الالكترونية من سلاسل التوريد وتقترح أيضاً اختبار رموز المصدر يمكن أن يثير مخاوف بشأن حماية الملكية الذكية، وهي ميزة نسبية للعديد من الشركات الدولية. (رشوان وقاسم، 2022: ص ص 12-13)

أهمية وجود معايير محددة تنظم المخاطر السيبرانية:

أشار تقرير صندوق النقد الدولي في اجتماعه الثالث لمجموعة العمل الاقليمي للتقنيات المالية الحديثة إلى نقاط في هذا الخصوص وهي كالتالي: (اسماعيل، 2019: ص ص3-4)

أ. تنظيم مخاطر الانترنت، يرى البعض أن الطبيعة المتطورة للمخاطر السيبرانية ليست قابلة للتنظيم بشكل محدد، كما أن القضايا الخاصة بالأنترنت يمكن معالجتها من خلال اللوائح الحالية المتعلقة بكل من المخاطر التشغيلية والتقنيات في القطاع المصرفي. فيما يشير البعض الآخر إلى أن هناك حاجة ملحة إلى وجود هيكل تنظيمي للتعامل مع الطبيعة الفريدة للمخاطر الالكترونية، وذلك بالنظر إلى التهديدات المتزايدة الناتجة عن التحول المكثف نحو قطاع مالي رقمي في الآونة الأخيرة.

ب. البحث المستمر والمكثف نحو إجراءات وقائية من المخاطر من خلال لوائح تجعل تلك الاجراءات أكثر وضوحًا أمام مجالس إدارات تلك المؤسسات، الأمر الذي يؤدي إلى خلق حافز أكبر على الاستثمار بشكل مستمر في تعزيز الأمن السيبراني.

ج. إن إدراج المخاطر السيبرانية ضمن المخاطر التشغيلية للمؤسسات المالية يعتبر غير كافي، حيث إن المعايير الرقابية على المصارف تتطلب أهمية تضمين الاستراتيجيات والسياسات الخاصة بتلك المصارف جزء خاصًا بإدارة المخاطر السيبرانية، يتم مراجعتها بانتظام من قبل مجالس إدارات المصارف مع زيادة حجم المخاطر السيبرانية.

التحديات التي تواجه الدول العربية فيما يخص الأمن السيبراني: (أسماعيل، 2019:ص7)

1- التطور السريع في مجال تقنية المعلومات والاعتماد المتزايد على التقنيات للقيام بمعظم العمليات المالية، مما يؤدي إلى زيادة التعرض للتهديدات والحوادث الإلكترونية.

2- الهجمات والقرصنة الإلكترونية الدولية التي تتعرض لها المصارف ببعض الدول العربية وآليه البنوك في التصدي لها ومدى فعالية الجدار الأمني في هذا الشأن.

3- حداثة مفهوم الأمن السيبراني على مستوى الدول العربية والحاجة إلى تقوية الخبرات المصرفية في هذا المجال ببعض الدول العربية.

4- ضمان تحقق الأمن السيبراني عند قيام المصارف بإجراء عقود لأطراف ثالثه تختص بأمن نظم المعلومات، للحد من وجود عمليات احتيال وقرصنة على الأنظمة الإلكترونية في تلك البنوك.

5- الارتفاع النسبي في تكلفة تطبيق تقنيات أمن نظم المعلومات والفضاء السيبراني بصورة ملحوظة.

6- صعوبة تطبيق ضوابط أمن نظم المعلومات والفضاء السيبراني نظراً لضعف ثقافة الأمن السيبراني لدى بعض العاملين في القطاع المالي والمصرفي.

7- الحاجة إلى وجود آلية رقابة واضحة على البنوك والشركات المالية للتأكد من وجود ضوابط وسياسات لتحقيق الأمن السيبراني.

ولقد أورد المنتدى العالمي للخبرات السيبرانيةGFCE في وثيقته بأن هناك خمسة أبعاد حاسمة لبناء القدرة الأمنية السيبرانية الناضجة لأي دولة والتي تتمثل في الآتي:

1. سياسة واستراتيجية الأمن السيبراني: يستكشف قدرة البلد على وضع استراتيجية للأمن السيبراني وتنفيذها وتعزيز قدرة صمود أمنها السيبراني من خلال تحسين الاستجابة للحوادث والدفاع السيبراني وقدرة حماية البنية التحتية والحيوية. ويراعى هذا البعد الاستراتيجيات والسياسات الفعالة عند توفير القدرة الوطنية للأمن السيبراني، مع الحفاظ على فوائد فضاء سيبراني حيوي للحكومة وقطاع الأعمال التجارية الدولية والمجتمع عمومًا.
2. ثقافة ومجتمع الأمن السيبراني: يستعرض العناصر المهمة لثقافة الأمن السيبراني المسؤولية، مثل فهم المخاطر المتعلقة بالفضاء السيبراني في المجتمع، ومستوى الثقة في خدمات الانترنت، وخدمات الحكومة الالكترونية والتجارة الالكترونية، وفهم المستخدمين لمسألة حماية المعلومات الشخصية عبر الانترنت. وعلاوة على ذلك يستكشف هذا البعد وجود آليات للإبلاغ تعمل كقنوات موجهة إلى المستخدمين من أجل الإبلاغ عن الجرائم السيبرانية. وبالإضافة إلى ذلك، يستعرض هذا البعد دور وسائل الإعلام ووسائل التواصل الاجتماعي في تشكيل قيم ومواقف وسلوكيات في مجال الأمن السيبراني.
3. بناء المعارف والقدرات في مجال الأمن السيبراني: يستعرض مدى توافر البرامج وجودتها واستيعابها لمختلف مجموعات أصحاب المصلحة، بما في ذلك الحكومة والقطاع الخاص والسكان ككل، ويتعلق ببرامج إذكاء الوعي بالأمن السيبراني وبرامج التعليم الرسمي للأمن السيبراني، وبرامج التدريب المهني.
4. الأطر القانونية والتنظيمية: يدرس قدرة الحكومة على تصميم وسن التشريعات الوطنية التي تتعلق بشكل مباشر وغير مباشر بالأمن السيبراني، مع التركيز بشكل خاص على موضوعات المتطلبات التنظيمية للأمن السيبراني، والتشريعات المتعلقة بالجرائم السيبرانية والتشريعات ذات الصلة. وتفحص القدرة على إنفاذ مثل هذه القوانين من خلال إنفاذ القانون والملاحقة والهيئات التنظيمية وصلاحيات المحاكم. علاوة على ذلك يلاحظ هذا البعد قضايا مثل أطر التعاون الرسمية وغير الرسمية لمكافحة الجريمة السيبرانية.

5. المعايير والتكنولوجيا: يتناول الاستخدام الفعال والواسع النطاق لتكنولوجيا الأمن السيبراني لحماية الأفراد والمنظمات والبنية التحتية الوطنية، ويبحث هذا البعد تحديدًا في تنفيذ معايير الأمن السيبراني والممارسات الجيدة، ونشر العمليات والضوابط وتطوير التكنولوجيا والمنتجات من أجل تقليل مخاطر الأمن السيبراني.

الأمن السيبراني وواقع التشريعات السيبرانية في ليبيا:

أطلق مصرف ليبيا المركزي في 22 – 6 – 2021 مشروع سايبر ليبيا وهو مبادرة تعنى بتكوين بنية تشريعية للمعاملات الالكترونية ما يؤسس لتحول رقمي جاد يفتح المجال لاستثمار آمن في المجال السيبراني، هذا وكان قد أعلن مصرف ليبيا المركزي تسلمه التقرير النهائي لأعمال هذا المشروع، والذي يهدف إلى إنجاز حزمة من التشريعات المنظمة للتحول الرقمي والاستثمار في الفضاء السيبراني، وتعتبر لجنة الأمم المتحدة (الاسكوا) هي الشريك الاستراتيجي لهذا المشروع، بالتعاون مع عدد من المؤسسات الوطنية والخبراء الدوليين، وقد قام في نهاية 2022 فريق مشروع سايبر ليبيا بعقد مباحثات موسعة في العاصمة المصرية القاهرة بالشراكة مع البنك المركزي المصري ولجنة الأسكوا وخبراء في مجال القانون والدفع الالكتروني وأمن المعلومات وإدارة المخاطر والتسويق الالكتروني وبمشاركة مؤسسات رائدة في المجال السيبراني والمالي.

ولكي يتم التعرف أكثر على هذا المشروع ومعرفة واقع التشريعات السيبرانية في ليبيا، تم استخدام أسلوب المقابلة الشخصية، حيث قامت الباحثة بإجراء مقابلة شخصية مع الدكتور نبيل أبوجناح نائب مشروع سايبر ليبيا، وقد تم طرح مجموعة من التساؤلات تم الاجابة عليها خلال المقابلة وهي:

- ما مدى جاهزية الدولة الليبية للتحول الرقمي خاصة في القطاع المصرفي، وهل تمتلك البنية التحتية لدعم هذا التحول؟
- ما هي التشريعات والقوانين التي يستند عليها مشروع سايبر ليبيا، وما أهمية وجود مثل هذه التشريعات؟
- هل الدولة الليبية لديها إطار علمي وقانوني لتسهيل اعتماد التحول الرقمي وتطبيق الأمن السيبراني؟
- ما مدى استعداد الدولة الليبية من حيث الأمن السيبراني، وما هي المعوقات التي تحول دون تطبيق الأمن السيبراني داخل ليبيا؟

من هنا أوضح الدكتور نبيل نائب مشروع سايبر ليبيا أن الفضاء السيبراني هو الفضاء الرابع لليبيا بالإضافة إلى الفضاء الجوي والبري والبحري، وكما لهذه الفضاءات من مخاطر تتم مواجهتها بالعديد من الوسائل كالجمارك والشرطة والميناء، فإن للفضاء السيبراني العديد من المخاطر التي يمكن أن تعترضه حيث أن الفضاء السيبراني

يتوجب فيه التحول الرقمي والالكتروني الكامل، وما يحتويه من معلومات غاية في السرية، فقد أصبحت تحيط به العديد من المخاطر كان لا بد من ايجاد الخطط والأساليب والطرق للحماية السيبرانية من القرصنة والاختراق. وعلى سبيل المثال لا الحصر لهذه الطرق برامج لحماية الاجهزة من أي اختراق كبرنامج الجدار الناري، واكواد التشفير والترميز، وبرامج المراقبة لمعلومات الشبكة وغيرها.

وقد تم التأكد من خلال المقابلة الشخصية بأن الدولة الليبية لديها بنية تحتية تقنية قابلة للتطوير وتغطي معظم مناطق ليبيا، إلى جانب انتشار خدمات الأنترنت وبسرعات معقولة وبأسعار ميسرة مع سهولة النفاذ في معظم مناطق ليبيا، بالإضافة إلى استخدام شبكات التواصل الاجتماعي على نطاق واسع. كما أن مشروع سايبر ليبيا يساعد الدولة للتحول الرقمي، وتحسين الخدمات التي تقدمها المؤسسات المختلفة عبر الشبكة العنكبوتية، كما أن الرؤية الاساسية لهذا المشروع هي السعي لتطوير الصناعة المصرفية في ليبيا من خلال الاستفادة من ثمار تكنولوجيا الاتصالات وتقنية المعلومات، بالإضافة إلى أن هذا المشروع يرتكز على التشريعات السيبرانية المتمثلة في ستة قوانين متعلقة بالفضاء السيبراني وهي قوانين المعاملات والتوقيع، وحماية البيانات الشخصية، والجرائم الالكترونية، والاتصالات الالكترونية وحرية التعبير، وحقوق الملكية الفكرية في المجال السيبراني، والتجارة الالكترونية وحماية المستهلك، فهذه القوانين تساعد على زيادة استخدام الفضاء الالكتروني وما يمنحه من فرص للاستثمارات المحلية والأجنبية.

وقد أوضح الدكتور نبيل أبوجناح أهمية التشريعات السيبرانية في أنها تساعد على تسريع التنمية الاجتماعية والاقتصادية؛ وذلك من خلال التحول الرقمي، كما تساعد في دعم وتحفيز التجارة الالكترونية سواء على النطاق المحلي أو الاقليمي أو الدولي، إلى جانب بناء ثقة المستخدمين في خدمات الفضاء السيبراني، وكذلك امكانية تطوير الخدمات الرقمية وتحقيق الشمول الرقمي، وتطوير الخدمات الحكومية المقدمة للمواطنين ممن خلال منصات رقمية متعددة، بالإضافة إلى امكانية تطوير التحول للاقتصاد الرقمي مما يساهم في تنوع الأنشطة الاقتصادية وتحسين الخدمات وتطويرها، وامكانية تطوير الخدمات المالية وتحقيق الشمول المالي. وعند سؤاله عن التهديدات والمعوقات التي يمكن أن تعيق تحقيق الأمن السيبراني، أوضح أنه لا توجد استراتيجية وطنية واضحة المعالم للاستثمار في هذا الفضاء، إلى جانب عدم وجود أطر قانونية وتشريعية متكاملة تواكب التطور الحاصل في هذا الفضاء حيث هناك مادة في نص دون وجود قانون كامل. إلى جانب غياب أو ضعف التشريعات الحاكمة للعمل في هذا الفضاء وهذا يقوض الاستثمار فيه، بالإضافة إلى فقدان الثقة والخصوصية الرقمية والأمن وتزايد المخاطر بالفضاء السيبراني وتطبيقاته.

وأضاف أنه بالرغم من كل ذلك لا تزال هناك فرص يمكن تداركها كإمكانية التحول للاقتصاد الرقمي مما يساهم في تنوع الأنشطة الاقتصادية وتحسين الخدمات وتطويرها، بالإضافة إلى إمكانية تطوير الخدمات الحكومية المقدمة للمواطنين من خلال منصات رقمية متعددة الأغراض. حيث بين الدكتور نبيل أن مصرف ليبيا المركزي من خلال مشروع سايبر ليبيا يسعى لطرح حزمة نموذجية متطورة من التشريعات تجمع فيها كل المبادرات والمحاولات السابقة حيث بنيت المبادرة على ثلاث أسس رئيسية وهي: وجود مبادرات مبعثرة من عدة مؤسسات بخصوص قانون المعاملات الالكترونية وقانون الجرائم الالكترونية. وأن مصرف ليبيا المركزي يقود مشروع مهم وهو مشروع المدفوعات الوطني ويسعى لطرح منتجات جديدة في سوق المدفوعات الليبي من التجارة الالكترونية. بالإضافة إلى أن مصرف ليبيا المركزي يعتبر المستشار الاقتصادي للدولة الليبية ويسعى لتطوير وتنويع الأنشطة الاقتصادية من خلال التحول للاقتصاد الرقمي.

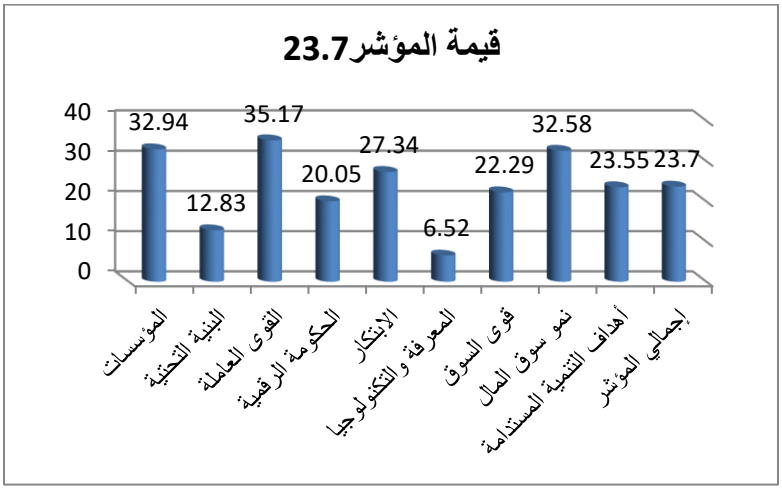
ومن جهة أخرى ومن خلال قيام الباحثة بزيارة الشركة الليبية والبريد والاتصالات وتقنية المعلومات القابضة، بوصفها الشركة التي أُسست لغرض الاستثمار في البنية التحتية للاتصالات في داخل البلاد وخارجها، ومن خلال الاطلاع على دليل الاستراتيجية لأمن المعلومات والأمن السيبراني، 2023-2025. فقد وضعت الشركة عدة معايير واجراءات احترازية لمواجهة أخطار الأمن السيبراني ومن هذه الاجراءات، سياسة خصوصية بيانات العملاء، وسياسة إدارة هويات الدخول والصلاحيات، اعتماد اجراء لإدارة آلية الوصول للمعلوماتية، سياسة إدارة الحوادث المعلوماتية والسيبرانية، سياسة إدارة المخاطر والأصول التقنية والمعلوماتية والسيبرانية، سياسة استخدام البريد الالكتروني، سياسة تأمين تطبيقات الويب، سياسة إدارة جوانب أمن المعلومات والأمن السيبراني المتعلقة بالموردين، وهم الأشخاص الغير موظفين بالمؤسسة ولكنهم على صلة وتواصل مباشر مع الموظفين، سياسة تقييم نقاط الضعف واختبارات الاختراق، سياسة استضافة نظام الكتروني أو أجهزة تقنية خاصة بطرف خارجي داخل مركز البيانات، سياسة أمن المعلومات والأطراف الخارجية، سياسة التشفير، سياسة جوانب الأمن المعلوماتي والسيبراني للموارد البشرية، والوصول عن بعد.

ومع إدراك الدولة الليبية بأن التطور التكنولوجي هو أحد الوسائل الرئيسية في برنامج الاصلاح السياسي والاقتصادي والاجتماعي على حد سواء وأن هذا التطوير سيؤثر ايجابًا على المواطنين والمستثمرين والشركات التي تتعامل مع الجهات الحكومية والذي سينعكس بالتالي على هذه الحكومة فقد تم وضع مقترح استراتيجية التحول الرقمي الحكومي في ديسمبر 2022، حيث صيغت هذه الاستراتيجية بعد الاطلاع على مجموعة من التجارب

الدولية والاقليمية واسترشدت بتركيباتها وبياناتها ونتائجها بغية الاستفادة المثلى منها باعتبارها تشكل طيفًا متنوعًا من الخبرات التي يمكن البناء عليها واستنباط أفضل الممارسات منها، وتتمحور رؤية استراتيجية التحول الرقمي في ليبيا حول المستخدم وتركز بشكل تفصيلي على تقديم خدمات حكومية أفضل للمستخدمين سواء كانوا أفراد (مواطنين وأجانب) أو شركات أو مؤسسات حكومية. تدفع هذه الرؤية نحو بناء جهاز حكومي مبتكر يقدم تجربة رقمية متميزة وخدمات ذكية وإجراءات استباقية ويعزز فرص إنشاء مجتمع واقتصاد رقمي متكامل وشامل يعمل على تحسين نوعية حياة المواطن من خلال توجيه النشاطات المختلفة للتحول الرقمي لتحقيق أهداف التنمية المستدامة وتمكين الأفراد بما يحقق الرفاه والنمو والازدهار لكافة أفراد المجتمع. وتتلخص الرؤية في أنه بحلول عام 2030، سيتمكن الجميع في دولة ليبيا من التمتع من أي مكان وفي أي وقت وبأي وسيلة اتصال متاحة بخدمات حكومية عالمية المستوى بطريقة سلسلة وسهلة وآمنة.(مقترح استراتيجية التحول الرقمي الحكومي في دولة ليبيا، 2022)

واقع الاقتصاد الرقمي في ليبيا وفق الاسس المختلفة:

بحسب مؤشر الاقتصاد الرقمي العربي 2022 فقد جاءت ليبيا في ترتيب متأخر، من بين 22 دولة عربية بمعدل 23.7 للمؤشر. وعلى هذا الأساس لا زالت ليبيا تحتل مرتبة متأخرة في معظم المجالات حيث تصنف ليبيا من ضمن الدول العربية التي تحتاج لتعزيز قدراتها الرقمية وبنيتها التحتية.(تقرير مؤشر الاقتصاد الرقمي للدول العربية 2022)، ومن خلال الشكل التالي والمتعلق بأسس الأداء بمختلف المستويات والذي جاءت فيه ليبيا بالترتيب 18 بين 22 دولة عربية نلاحظ أن ليبيا تعاني من تأخر في مختلف المجالات فقد كان أداء المؤسسات في المرتبة 20 بنسبة 32.94، بينما أخذت المرتبة 21 في تحقيق أهداف التنمية المستدامة 23.55، وبالنسبة لمعدل نمو سوق المال فقد جاءت ليبيا في الترتيب 18، أما فيما يخص القوى العاملة والحكومة الرقمية فقد جاءت ليبيا في الترتيب 17، أما عن الابتكار والمعرفة والتكنولوجيا وقوى السوق، جاءت ليبيا في المرتبة 16، وكذلك جاءت بنفس الترتيب البنية التحتية، والشكل(1) يوضح ذلك.



الشكل(1) واقع الاقتصاد الرقمي في ليبيا المصدر: تقرير مؤشر الاقتصاد الرقمي للدول العربية 2022

من هنا ترى الباحثة أن ليبيا فعلاً بحاجة ماسة لتعزيز قدرتها الرقمية بشكل أكبر، خاصة في الابتكار والمعرفة والتكنولوجيا، الذي يعتبر من أهم مؤشرات التحول نحو الاقتصاد الرقمي كونه يبين مدى القدرة على خلق التميز في المعاملات التجارية الالكترونية، وكذلك البنية التحتية التي تعبر عن قدرة الدولة في توفير خدمات الاتصالات وقدرة الأفراد على الوصول إليها بأقل تكلفة كما يعكس مستوى انتشار خدمات الاتصالات على مستوى الدول العربية الأخرى الداخلة بالمؤشر.

وبالرغم من أن مؤشر الاقتصاد الرقمي العربي أشار إلى أن ليبيا ضمن الدول العربية التي تحتاج إلى زيادة الاستثمار في مجالات البحث والتطوير في كافة القطاعات. إلا أننا وبالنظر إلى ما جاء به صندوق النقد الدولي للاقتصاد والتمويل في الشرق الأوسط(CEF) والذي يعد أحد أهم مراكز التدريب الاقليمية (RTCs) التابعة لصندوق النقد الدولي والذي يعنى بتقديم خدمات التدريب للبلدان الأعضاء في جامعة الدول العربية البالغ عددها 22 بلد، وتطوير مهارات المسؤولين العموميين فيها وتعزيز قدراتهم على وضع السياسات الاقتصادية وصقل جودتها. ومن الدورات ما يخص السياسات المالية والمصرفية والتطور المالي وكذلك إدارة المخاطر السيبرانية والمخاطر الالكترونية والرقابة عليها. ودورات خاصة بالتكنولوجيا المالية والنقود الالكترونية، إلا أننا نجد أن نسبة

مشاركة ليبيا في هذه الدورات لا تتجاوز 3.5% خلال السنوات السابقة. وهذا الرقم يعتبر ضئيل جدًا إذا ما نظرنا للفائدة التي يمكن أن تجنيها ليبيا من الاشتراك بمثل هذه الدورات.

وحيث إن الاستثمار في الفضاء السيبراني يستوجب التحول الرقمي فإنه ومن خلال تحليل مؤشرات نجاح التحول الرقمي في ليبيا، نجد أن مؤشرات عام 2022، وفيما يخص مؤشر تطور الحكومة الالكتروني جاءت ليبيا في المرتبة 162، كما أن نسبة استخدام نظم الأرشفة الالكترونية لكافة المؤسسات الحكومية لا تتعدى نسبة 20%، بالإضافة إلى أنه يتم التحقق الأني من مطابقة البيانات اللازمة للخدمات الالكترونية بنسبة 10% فقط ، إلى جانب أنه لم تُعَد أي أبحاث في مجالات التحول الرقمي المختلفة، أما عن باقي المؤشرات فلا يوجد أي منها. (مقترح استراتيجية التحول الرقمي الحكومي في دولة ليبيا، 2022)

وبناء على ذلك فأن ليبيا في حاجة إلى خطوة جدية وفعالة على جميع مستويات الدولة وفي مختلف قطاعاتها، مع أهمية سرعة شروعها في التطبيق الفعلي للاستراتيجيات والمقترحات وعدم الاكتفاء بوضعها بشكل نظري. مع ضرورة استكمال البنية التشريعية والقانونية اللازمة لتنظيم جميع قطاعات الدولة خاصة القطاع المالي، بصفته قطاع داعم لمختلف القطاعات الأخرى، وتوفير بيئة مناسبة وجاذبة للاستثمار سواء المحلي أو الأجنبي.

النتائج:

من خلال استعراض الجانب النظري والدراسات السابقة ونتائج التحليل والمقابلات الشخصية توصلت الدراسة إلى النتائج التالية:

أولاً– توصلت الدراسة من خلال الجانب النظري والدراسات السابقة إلى:

1. إن التحول الرقمي بات من المتطلبات الأساسية لنجاح المؤسسات المالية واستمرارها في تقدمها وقدرتها على مواكبة التغيرات المستمرة في بيئتها التي تعمل بها. بالإضافة إلى قدرة الأفراد والشركات في امكانية الوصول للتمويل بغض النظر عن الموقع الجغرافي وخدمة شريحة أكبر وأوسع.
2. إن استخدام المؤسسات المالية وخاصة المصارف لتقنيات التشفير يضمن حماية بيانات المعاملات المالية والمعلومات الحساسة الأخرى عند نقلها عبر الشبكة، كما يضمن أن يتم فهم البيانات فقط من قبل الاطراف المخول لها.
3. إن مخاطر الأمن السيبرانية متعددة الأبعاد وتتطلب أمنًا داخل السلطات ورقابة قوية للحد منها.

4. أدى تزايد الاعتماد على الخدمات المالية الرقمية للدول خاصة النامية منها إلى تزايد التهديدات السيبرانية عليها،كما أن الوضع الأمني قد تسبب في تأخرها في اتخاذ تدابير لتعزيز أمنها السيبراني.
5. الهجمات السيبرانية أصبحت تعتمد بشكل كبير على استخدام الذكاء الاصطناعي والأدوات البرمجية المتطورة مما زاد الأمر تعقيدًا.

ثانيًا- من خلال المقابلة الشخصية توصلت الدراسة إلى الآتي:

1- تمتلك الدولة الليبية بنية تحتية تقنية قابلة للتطوير وتغطي معظم مناطق ليبيا مما يساعد في إمكانية الاستثمار في الفضاء السيبراني، وامكانية التحول للاقتصاد الرقمي، وكذلك امكانية تطوير كافة الخدمات الحكومية المقدمة للمواطنين.
2- عدم وجود استراتيجية واضحة المعالم للاستثمار في الفضاء السيبراني بليبيا.
3- لا يوجد أطر قانونية تسند عليها الدولة الليبية فيما يخص الأمن السيبراني، بل هناك مادة في نص دون وجود قانون كامل، بمعنى وجود بعض النصوص القانونية المبعثرة كما أن هناك بعض القوانين التي يرتكز عليها الأمن السيبراني في مشروع سايبر ليبيا لم تعتمد بعد بل هي عبارة عن مسودة قانون، كقانون المعاملات الالكتروني والتوقيع الالكتروني (مسودة قانون من شبكة ليبيا للتجارة وأخرى من وزارة العدل) وقانون الجرائم الالكترونية (مسودة قانون من وزارة العدل، لم تعتمد بعد)، وقانون الاتصالات وحرية التعبير(قانون خاص بالاتصالات ولا يوجد قانون يعنى بحرية التعبير).
4- هناك العديد من الموظفين ذو التخصص المالي وليس لديهم دراية كافية عن علوم الحاسب الآلي، مما يجعلهم أكثر عرضة لمخاطر الأمن السيبراني.
5- لا تزال هناك فرص يمكن تداركها كإمكانية التحول للاقتصاد الرقمي، مما يساهم في تنوع الأنشطة الاقتصادية وتحسين الخدمات وتطويرها، بالإضافة إلى إمكانية تطوير الخدمات الحكومية المقدمة للمواطنين من خلال منصات رقمية متعددة الأغراض.

ثالثًا- من خلال التحليل توصلت الدراسة إلى ما يلي:

1- تحتل ليبيا مرتبة متأخرة في معظم المجالات، حسب تقرير مؤشر الاقتصاد الرقمي العربي 2022.
2- ليبيا بحاجة لتعزيز قدرتها الرقمية بشكل أكبر، خاصة في الابتكار والمعرفة والتكنولوجيا، الذي يعتبر من أهم مؤشرات التحول نحو الاقتصاد الرقمي كونه يبين مدى القدرة على خلق التميز في المعاملات

التجارية الالكترونية، وكذلك البنية التحتية التي تعبر عن قدرة الدولة في توفير خدمات الاتصالات وقدرة الأفراد على الوصول إليها بأقل تكلفة كما يعكس مستوى انتشار خدمات الاتصالات على مستوى الدول العربية الأخرى الداخلة بالمؤشر.

3- ليبيا مازالت لا تملك الدعائم الأساسية للبرنامج العالمي للأمن السيبراني والتي تؤهلها للانضمام لقائمة الدول في مؤشر القوة السيبراني الوطني، إلا أنها تسعى لتبني استراتيجية للتحول الرقمي واعداد استراتيجية شاملة قانونية للأمن السيبراني.

4- عدم المشاركة الفعالة للكوادر الليبية في الدورات الدولية والتي يمكن أن تساعد في تعزيز قدراتهم على وضع السياسات الاقتصادية وصقل جودتها خاصة فيما يتعلق بالتكنولوجيا المالية وإدارة المخاطر السيبرانية والمخاطر الالكترونية والرقابة عليها.

5- الضعف الشديد في بعض مؤشرات نجاح التحول الرقمي في ليبيا وانعدام وجودها في بعض المؤشرات الأخرى.

التوصيات:

1- نشر الوعي عند الموظفين في الأمور المتعلقة بالأمن السيبراني، خاصة الموظفين الغير متخصصين بعلوم الحاسب الآلي، وتعريفهم بأهمية امتثالهم للسياسات الموضوعة للحد من المخاطر السيبرانية، وتدريبهم على كيفية الرد في حالة الاشتباه مع مراقبة جودة الدورات وفعاليتها التدريبية بشكل مستمر.

2- ضرورة تخصيص الموارد والاستثمارات اللازمة لتعزيز دفاعات الأمن السيبراني والذكاء الاصطناعي، كحماية تطبيقات الويب وتحديد مواطن التعرض للمخاطر ومراجعة الدفاعات السيبرانية الحالية أول بأول.

3- دمج الأمن السيبراني في دورة حياة تطوير البرمجيات والمعلومات وعند وضع الأنظمة والتعليمات.

4- التأكيد على أهمية إصدار الإرشادات والقرارات المعنية بتعزيز الأمن السيبراني لدى مختلف المؤسسات بهدف تعزيز سلامة وكفاءة المدفوعات والتحويلات الالكترونية وتوفير خدمات مالية ومصرفية الكترونية أمنة وموثوقة ودعم التحول الرقمي الشامل والمتطور.

5- إنشاء تعاون وطني بين الحكومة والمؤسسات المالية لرفع الوعي حول القضايا المرتبطة بالأمن السيبراني وتحفيزه.

6- ضرورة إعداد استراتيجية وطنية وتشريعية للأمن السيبراني بشكل عملي وفعلي، لأجل التصدي لتهديدات الأمن الالكتروني الحالية والمتزايدة والحدد من مخاطرها. بالإضافة إلى الاستعانة بالاتفاقيات الدولية المرتبطة بتشريعات الفضاء السيبراني للاستفادة من التجارب والخبرات المختلفة، وتعزيز التعاون الدولي.

7- ضرورة مشاركة الكوادر الوطنية بالدولة الليبية في الدورات الدولية بما يساهم في اكسابهم الخبرة والمعرفة بكل ما هو جديد في عالم الفضاء المالي والسيبراني.

Abstract:

Technological developments and innovations have contributed to the significant impact on the financial sector, especially banks, which have witnessed a shift from traditional channels to electronic channels and the emergence of digital banks, and these transformations came with risks related to technology, which necessitated the need to focus on cyber security in general. The willingness of financial institutions to take measures to mitigate and address the risks associated with this development. Especially since the banking sector is linked to many other sectors with regard to financing, which makes it one of the most important parties that support various economic sectors within the country, and Libya is moving towards digital transformation, which requires it before doing so fully to strengthen its cyber security to be able to face its negative effects and the risks and cyber-attacks it contains that can expose its financial sector to many risks.

المراجع

1. اسماعيل، محمد، الأمن السيبراني في القطاع المصرفي عرض مقارن للمعايير والتجارب الدولية والعربية، الاجتماع الثالث لمجموعة العمل الاقليمية للتقنيات المالية الحديثة صندوق النقد العربي، ابوظبي 9-10 ديسمبر 2019.
2. إسماعيل، محمد، موجز سياسات (يونيو 2019)، الأمن السيبراني في القطاع المصرفي، العدد4 صندوق النقد العربي.
3. أمانة مجلس محافظي المصارف المركزية ومؤسسات النقد العربية، سلامة وأمن المعلومات المصرفية الالكترونية، اللجنة العربية للرقابة المصرفية، صندوق النقد العربي أبو ظبي- الامارات العربية المتحدة.

4. البغدادي، مروة فتحي السيد، اقتصاديات الأمن السيبراني في القطاع المصرفي، مجلة البحوث القانونية والاقتصادية، العدد 76 ، 2021.
5. الحديدي، أيمن أحمد، الأمن السيبراني في ظل الانفجار المعرفي، ط 1، دار اليازوري العلمية للنشر والتوزيع.
6. جغل، جميلة، زقرير، عادل، الأمن السيبراني والشمول المالي في ظل التحول الرقمي للقطاع المالي (التهديدات السيبرانية، آليات التحوط)، مجلة التنمية الاقتصادية جامعة الوادي، المجلد 8 العدد1، 2023.
7. رشوان، عبدالرحمن محمد، قاسم، زينب عبدالحفيظ، أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك، المؤتمر العلمي الدولي الأول بعنوان أثر الأمن السيبراني على الأمن الوطني، 20- 21 ديسمبر 2022. جامعة عمان العربية بالاشتراك مع مديرية الأمن العام.
8. السمحان، منى عبدالله، متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، مجلة كلية التربية- جامعة المنصورة العدد 111، 2020
9. سمير، علي، مركز الحضارة للدراسات والبحوث 2022، السيبرانية واقع وتحولات .
10. شادي، مهند حامد، عالم جديد شجاع ومخيف، عصر الاقتصاد السيبراني، مركز الحضارة للدراسات والبحوث، 2022.
11. شمران، عبيد خليف الأمير، أثر التحول الرقمي للمصارف التجارية العراقية على الإفصاح المحاسبي في ظل مخاطر الأمن السيبراني، مجلة الكوت للاقتصاد والعلوم الادارية، المجلد14، العدد54، 2022.
12. صواق، عبد القادر وآخرون، أثر جاهزية الأمن السيبراني على الخدمات المصرفية الالكترونية من خلال تقليل المخاطر المدركة دراسة حالة بنك BDL بغرداية، مجلة أبحاث اقتصادية معاصرة المجلد 6 العدد1، 2023.
13. علي، أحمد حامد، محمد، سالم عبدالله، الأمن السيبراني في دول مجلس التعاون لدول الخليج العربية بمنظور جيوبولتيكي معاصر، مجلة جامعة الأنبار للعلوم الانسانية، العدد 3 المجلد 1، 2020.
14. العمارات، فارس محمد، الحمامصة، ابراهيم محمد، الأمن السيبراني المفهوم وتحديات العصر، دار الخليج للنشر والتوزيع، 2022، ط1.
15. العمارات، فارس محمد، جرائم العصر من الرقمية إلى السيبرانية، دار الخليج للنشر والتوزيع، 2023.

16. قرزيز، نبيلة، زيدان، محمد، دور أمن المعلومات في تحقيق جودة الخدمات المصرفية، مجلة الاقتصاد والمالية المجلد 8 العدد 1، 2022

17. مركز الحضارة للدراسات والبحوث، 2022، السيبرانية واقع وتحولات

18. المنتدى العالمي للخبرات السيرانية، نظرة عامة حول أدوات تقييم القدرات السيرانية القائمة على الصعيد الوطني (GOAT).

19. مقترح استراتيجية التحول الرقمي الحكومي في دولة ليبيا، 2022.

20. يعقوب، ابتهاج اسماعيل وآخرون، مؤشر مقترح للإفصاح المحاسبي عن المخاطر السيبرانية في سوق العراق للأوراق المالية على وفق المتطلبات الدولية– دراسة اختبارية، مجلة الدراسات المالية والمحاسبية والإدارية المجلد 9 العد 1، 2022.

21. الشركة الليبية والبريد والاتصالات وتقنية المعلومات القابضة، دليل الاستراتيجية للأمن المعلومات والأمن السيبراني، 2023–2025.

22. هند مختار، 2023: https://www.youm7.com/6130353

23. Christian Calliess* and Ansgar Baumgarten. Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective, German Law Journal (2020), 21, pp. 1149–1179