# تهديدات الأمن السيبراني للمصارف الإلكترونية وآلية مواجهاتها

**إعداد**
**الأستاذ الدكتور / غريب جبر جبر**
**أستاذ المحاسبة والمراجعة**
**عميد المعهد العالي للحاسبات والمعلومات وتكنولوجيا الإدارة ـ طنطا**

**تاريخ الإرسال: 16 سبتمبر 2022؛ تاريخ المراجعة: 12 ديسمبر2022؛ تاريخ القبول: 20 ديسمبر2022؛ تاريخ النشر:1 فبراير2023.**

**المستخلص**
يهدف البحث إلى عرض أهم التحديات التي تواجه المجتمع المصرفي من أجل تحقيق الأمن السيبراني والذي يلعب دوراً محورياً في معالجة التحديات المستقبلية نظراً لاستخدامه كتكنولوجيا لإدارة الشبكات، وذلك لمحاولة وضع اليات للحد من هذه المخاطر، واتخاذ كافة الإجراءات الاحترازية التي يمكن ان تزعزع سلامة ونزاهة واستقرار القطاع المصرفي والمالي، حيث تمثل التكنولوجيا المالية وتطبيقاتها المالية المختلفة فرصاً وتحديات في الوقت الراهن، وذلك بما يدعم أهداف التنمية المستدامة في ظل رؤية 2030.
**الكلمات المفتاحية: الأمن السيبرانى، المصارف الإلكترونية .**

## Abstract
This paper aims to pinpoint the most important challenges facing the banking sector in order to achieve cyber security; which plays a pivotal role in addressing future challenges due to its use as a technology for networks management, in an attempt to develop mechanisms that would help in mitigating these risks, and to take all precautionary measures that could destabilize the safety, integrity and stability of the banking sector; where financial technology and its various financial applications represent opportunities and challenges at the present time, in a way that supports the goals of sustainable development in light of Vision 2030.
***Keywords: Cyber Security, Electronic Banks***

**التوثيق المقترح وفقاً لنظام APA:**
**جبر**، غريب جبر (2023). تهديدات الأمن السيبراني للمصارف الإلكترونية وآلية مواجهاتها . **المجلة الأكاديمية للعلوم الاجتماعية**، الأكاديمية الدولية للهندسة وعلوم الإعلام،1(1)،53-70.

**1. طبيعة ومشكلة البحث:**

في ظل التطور التكنولوجي الحالي أصبحت الرقمنة مطلباً أساسياً لجميع القطاعات على اختلاف أنشطتها وأهميتها لما يشهده العالم اليوم من تحولات جذرية تعتمد على الافتراضية والترابط كمتطلب أساسي لما يعرف بـ عصر الثورة الصناعية الرابعة وقد شهدت الصناعة المصرفية تحولاً جوهرياً في النظام المصرفي، اشتمل علي الانتشار السريع للتقنيات مثل الهواتف المحمولة الذكية، الذكاء الاصطناعي، الروبوتات الذكية، الحوسبة السحابية، تعميم الحواسيب والإنترنت وتحليلات البيانات الضخمة وغيرها، وفي هذا السياق فقد أحدث تغلل الإنترنت تحولاً عميقاً في عادات وتفضيلات المستخدمين ،حيث أثبتت الدراسات أن حوالي ما يقرب من 59% من سكان العالم يستخدم تطبيقات الإنترنت وذلك في نهاية عام 2021، ولقد أصبحت عملية تبادل المعلومات عبر الوسائط الرقمية وإجراء تعاملات عديدة كالتسوق عبر الإنترنت أو الوصول إلى خدمات مصرفية جديدة سمة من سمات ما نعيشه الآن، وذلك نظراً لسرعة الأداء والقدرة علي التحكم في تلك الأمور من قبل المستخدمين

وفي إطار متصل فقد طرأت على الساحة المصرفية تغيرات متسارعة ومتلاحقة بشكل غير مسبوق على نحو أن أصبح الشكل التقليدي للبنوك مهدد بشكل قوي، حيث أصبحت الأعمال التي تقوم بها البنوك تتميز بدرجة كبيرة من التعقد بشكل واضح، حيث ظهرت مجموعة من المخاطر تستدعي تقيمها وإدارتها، حيث أن القطاع المالي المصرفي من أكثر القطاعات الاقتصادية تعرضاً للمخاطر لاسيما المخاطر المستقبلية، ومن هنا دعت الحاجة إلي أهمية سلامة النظام المصرفي واستقراره.

وفي هذا الاطار يشهد قطاع الخدمات المالية المصرفية هجمات سيبرانية تفوق القطاعات الأخرى بنسبة 71% وذلك وفق تقديرات البنك الدولي الصادرة في ديسمبر 2021 وقد تصل تكلفة الهجمات السيبرانية في قطاع الخدمات المالية إلى ما يقدر بنحو 360 مليار دولار سنوياً حال اتساع نطاق انتشارها وفقاً لتقديرات صندوق النقد الدولي، الأمر الذي دفع المصارف المركزية العربية إلى تشديد التعليمات الرقابية والتي تلزم المصارف بوضع لائحة من التعليمات لتأمين التطبيقات الإلكترونية ومن أهمها تثبيت برامج الحماية ضد الاختراق

ومع استمرار تقنيات المعلومات والاتصالات في الابتكار في

إيجاد وتقديم طرق جديدة للوصول إلى المستخدمين فإن تلك المصارف خاصة الإلكترونية منها تتعرض لمجموعة من المخاطر حيث أن الاستخدام الضار لتقنية المعلومات والاتصالات يمكن أن يؤدي إلى تعطيل الخدمات المالية الضرورية للأنظمة المالية الوطنية والدولية وتقويض الأمن والثقة وتعريض الاستقرار المالي للخطر، حيث تمثل الهجمات السيبرانية تهديداً للنظام المالي بأكمله وهي حقيقة تؤكدها التقارير الصادرة في هذا الشأن على المستوى الدولي والإقليمي والمحلي، حيث بلغت نسبة المستخدمين الذين عانوا من الهجمات السيبرانية خلال عام 2016 نحو 65% بنسبة زيادة قدرها حوالي 29% مقارنة بالعام 2015، وذلك وفقاً للتقرير الصادر عن البنك الدولي في هذا الشأن.

وكنتيجة لما سبق واعترافا بالتهديدات الناجمة عن المخاطر السيبرانية دعت الحاجة إلي السعي بشكل متواصل نحو مواجهه هذه المخاطر والحد منها، ومحاولة وجود آليات فعلية تعمل علي تعزيز قدرة الأجهزة المصرفية على تحمل هذه المخاطر والتحوط منها، خاصة بعد ان اتخذت السلطات الرقابية على مستوى العالم خطوات تنظيمية وإشرافية تهدف إلى تجنب أثر تلك المخاطر السيبرانية على المصارف في هذا الصدد، حيث قامت المصارف المركزية العربية بإصدار التعليمات المصرفية التي تحث فيها البنوك على تعزيز قدراتها لمواجهة تلك الهجمات الإلكترونية

**2. هدف البحث:**

يستهدف البحث عرض اهم التحديات التي تواجه المجتمع المصرفي من أجل تحقيق الأمن السيبراني والذي يلعب دوراً محورياً في معالجة التحديات المستقبلية نظراً لاستخدامه كتكنولوجيا لإدارة الشبكات، مما يدعم أهداف التنمية المستدامة في ظل رؤية 2030.

**3. أهمية البحث:**

تعتبر فكرة البحث من الموضوعات الهامة وذلك نظرا لأنها تمثل عنصراُ هاماً من عناصر التكنولوجيا المالية Fintech ومستقبل الخدمات المصرفية الإلكترونية في ظل مجموعة من مخاطر الأمن السيبراني ، ومحاولة وضع اليات للحد من هذه المخاطر، واتخاذ كافة الإجراءات الاحترازية التي يمكن ان تزعزع سلامة ونزاهة واستقرار القطاع المصرفي والمالي، حيث تمثل التكنولوجيا المالية وتطبيقاتها المالية المختلفة فرصاً وتحديات في الوقت الراهن.

**وبناء علي ما سبق يمكن استعراض الورقة البحثية من خلال المحاور التالية:**

المحور الأول: الأمن السيبراني ( المفهوم – المحددات ).
المحور الثاني: طبيعة وأنواع المخاطر السيبرانية.
المحور الثالث: مخاطر الأمن السيبراني في المصارف الإلكترونية.
المحور الرابع: إدارة مخاطر العمليات المصرفية الإلكترونية.
المحور الخامس: معوقات تعزيز الأمن السيبراني في المصارف الإلكترونية.
المحور السادس: اليات تعزيز الأمن السيبراني في المصارف الإلكترونية.
المحور السابع: رؤية جمهورية مصر العربية في مجال الأمن السيبراني طبقا 2030
النتائج والتوصيات.

**أولا: الأمن السيبراني ( المفهوم – المحددات ).**

**المفهوم**

طبقا لما ورد في التقرير الصادر عن الاتحاد الدولي للاتصالات بشأن الأمن السيبراني حول اتجاهات الإصلاح في الاتصالات للعام 2014 – 2015 حيث يمثل مجموعة من المهمات مثل تجميع وسائل وسياسات وإجراءات أمنية ومبادئ توجيهية ومقاربات لإدارة المخاطر وتدريبات وممارسات فضلي وتقنيات يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين

ويمكن تعريف الأمن السيبراني طبقاً لما جاء بدراسة( البغدادي، 2021 ) بأنه النشاط الذي يؤمن حماية الموارد البشرية والمالية المرتبطة بتقنيات الاتصالات والمعلومات ويضمن إمكانات الحد من الخسائر والإضرار التي تترتب في حال تحقق المخاطر والتهديدات كما يتيح إعادة الوضع إلى ما كان عليه بأسرع ممكن بحيث لا تتوقف عجلة الإنتاج وبحيث لا تتحول الإضرار إلى خسائر دائمة

ويري الباحث ان الأمن السيبراني عملية حماية المعلومات من خلال معالجة التهديدات التي تتعرض لها هذه المعلومات التي تتم معالجتها وتخزينها ونقلها بواسطة أنظمة المعلومات المتداخلة بين الشبكات.

**المحددات:**

يمتد الأمن السيبراني ليشمل جميع المجالات الاقتصادية والاجتماعية والسياسية والقانونية لكافة المجتمعات المعاصرة واستنادا لما سبق فإن الأمن السيبراني يرتبط ارتباطا وثيقاً بسلامة مصادر الثروة والتقدم فالوقت الراهن والتي تشمل القدرة على الاتصال والتواصل والبيانات والمعلومات التي يستند عليها الإنتاج والإبداع والقدرة على المنافسة لذلك تتمثل محددات الأمن السيبراني في الاتي:

**1- البعد العسكري:**

إن بدء استخدام الإنترنت قد تم في بيئة عسكرية ثم تطور الأمر ليشمل البعد الأكاديمي لها بهدف تطوير القدرات العسكرية والإنجازات العلمية التي تضمن تقدم دولة على أخرى خاصة في مجال تطوير الأسلحة النووية ومن أبرز الأمثلة التي يمكن عرضها في هذا المجال لتوضيح الأبعاد العسكرية للأمن السيبراني وخطورة الهجمات السيبرانية ما حدث في جورجيا وكوريا الجنوبية وإيران مثال على بعض الهجمات والاختراقات والتي انتهت بالصراع المسلح لاحق أو بانقطاع الاتصال بالفضاء السيبراني داخل الدولة أو التشويش على الإدارات الحكومية.

**2- البعد الاجتماعي:**

تسمح طبيعة الفضاء السيبراني المفتوحة عبر وسائل التواصل الاجتماعية لكل مواطن بالتعبير عن تطلعاته السياسية وطموحاته الاجتماعية، كذلك تعتبر فرص ميسرة للاطلاع على الأفكار والمعلومات المتباينة مما يسمح بتبادل الخبرات وتحقيق التعاون والتقارب بين المجتمعات المختلفة كما أنه لا يمكن تجاهل الدور الفضاء السيبراني في تبادل المعلومات في المجالات العلمية والثقافية والخدمية وفي أوقات الأزمات والكوارث.... إلخ إذ لا تقف الأبعاد الاجتماعية عند هذه الحدود فقط بل تتعداها إلى صيانة القيم الجوهرية في المجتمع كالانتماء والمعتقدات إضافة إلى العادات والتقاليد.

**3- البعد السياسي:**

تتمثل الأبعاد السياسية للأمن السيبراني في حق الدولة في حماية نظامها السياسي ومصالحها في وقت تؤثر التقنيات على موازين القوى داخل المجتمع نفسه حيث أصبح من حق المواطن الاطلاع على خلفيات ومبررات القرارات السياسية داخل بلادة والاطلاع على نظيرتها في الدول الأخرى بالمقابل يحاول العاملون في الشأن السياسي الإفادة مما تقدمه هذه التقنيات والترويج لسياساتهم في العالم.

**4- البعد الاقتصادي:**

يرتبط الأمن السيبراني ارتباطا وثيقاً بالاقتصاد فالتلازم واضح بين اقتصاد المعرفة وتوسع استخدام تقنيات المعلومات والاتصالات كما تتيح تقنيات المعلومات والاتصالات تعزيز التنمية الاقتصادية لدول كثيرة عبر إفادتها من فرص الاستخدام التي تقدمها الشركات الدولية التي تبحث عن إدارة تكلفة إنتاجها بأفضل الشروط إلا أن هذا الواقع يطرح مسائل مختلفة تتعلق بحماية مقدم الخدمة أو حماية المستهلك على الإنترنت.

**5- البعد القانوني:**

يرتب النشاط الفردي والحكومي في الفضاء السيبراني نتائج قانونية تتطلب اهتماما لحل النزاعات التي يمكن أن تنشأ عنها ونظراً لنشأة مجتمع المعلومات وتطوره السريع فقد أضيف إلى قائمة الحقوق الأساسية والحريات المعترف بها في الدساتير والتشريعات الدولية حقوقاً أخرى كحق النفاذ إلى الشبكة العالمية للمعلومات كما توسعت بعض المفاهيم لتشمل أساليب ممارسة واستخدام تقنيات المعلومات والاتصالات كالحق في إنشاء المدونات الإلكترونية والحق في إنشاء التجمعات على الإنترنت والحق في حماية ملكية البرامج المعلوماتية.

**المحور الثاني: طبيعة وأنواع المخاطر السيبرانية.**

في عالم يشوبه الكثير من التعرض للمخاطر على جميع المستويات وتزايد حدة أشكال الحرب السيبرانية تحتاج بيئة الأعمال إلى تكييف أدواتها في الحد من مخاطر الأمن السيبراني والاستجابة لها في مراحل مختلفة وأصبحت التغييرات والتحسينات التي تأتي مع التكنولوجيا الجديدة والابتكار واعتمادها من قبل المنظمات أكثر تعقيداً عما سبق.

مفهوم الجريمة السيبرانية:

يتطلب الأمر بداية التعرف على طبيعة الجريمة السيبرانية التي تشكل الخطر الأساسي الواجب مكافحته واستنادا إلى مبدأ لا جريمة ولا عقاب دون نص عمدت العديد من الدول إلى وضع نصوص قانونية خاص بهذه الجرائم التي يمكنها أن تشمل قطاع واسع من الأعمال غير الشرعية كتلك التي تستخدم أجهزة الكمبيوتر والشبكات كوسيلة لتنفيذ الجريمة أو كهدف لها بدءا من عمليات اختراق الأنظمة المعلوماتية وأنظمة الاتصالات وصولاً إلى الهجمات التي تعطل الخدمات.

إلا أن عدم وجود تعريف شامل للجريمة السيبرانية يجعل من

الأفضل أن نستند إلى التعريفات التي اعتمدتها الهيئات والمنظمات الدولية المتخصصة ففي ورشة عمل متخصصة حول المسائل التي تثيرها الجرائم المتصلة بالشبكات قسمت هذه الجرائم إلى مجموعتين

المجموعة الأولي: وضمنت حسب المفهوم الضيق كل تصرف غير شرعي موجه بالوسائل الإلكترونية نحو أمن أنظمة المعلومات والبيانات التي تحويها

المجموعة الثانية: والتي ضمنت حسب المفهوم الأوسع كل تصرف غير شرعي يرتكب بواسطة الأنظمة المعلوماتية أو بطريقة متصلة بها ويشمل جرائم كالحيازة غير المشروعة أو عرض الخدمات وتوزيع المعلومات بواسطة أنظمة معلومات أو شبكات معلومات

ومن جهة أخرى عمدت الاتفاقية الأوروبية لمكافحة الجريمة السيبرانية إلى إيراد ما تعتبره أعمالاً غير شرعية تناولت الجرائم ضد سرية الأنظمة والبيانات سلامتها وتوفرها والجرائم المتصلة بالأجهزة والجرائم الخاصة بالمحتوى والجرائم الخاصة بالملكية الفكرية

أنواع المخاطر السيبرانية

يتمثل تأثير الهجمات السيبرانية من خلال المساس بالجوانب الرئيسية الثلاثة لأمن المعلومات والتي تتمثل في السرية والنزاهة واستمرارية الأداء

السرية: حيث تنشأ عندما يتم الكشف عن المعلومات الخاصة داخل الشركة إلى أطراف ثالثة كما في حالة حدوث اختراق البيانات.

النزاهة: والتي تتعلق بإساءة استخدام الأنظمة كما هو الحال بالنسبة للاحتيال

استمرارية الأداء: والتي تتلخص في تعطل أو التوقف عن ممارسة الأعمال

وتتمثل خطوط الدفاع الثلاثة للحد من المخاطر السيبرانية في الاتي Sergejq Slapni cara et al., 2022

خط الدفاع الأول: يتمثل في مديرو وحدات الأعمال ووظيفة تكنولوجيا المعلومات الذين يمتلكون ويديرون البيانات والعمليات والمخاطر والضوابط وينفذون الإجراءات التصحيحية لمعالجة أوجه القصور في العمليات والتحكم

خط الدفاع الثاني: يتمثل في وظيفة إدارة مخاطر تكنولوجيا المعلومات والالتزام وتلعب دوراً رئيسياً في أمان المؤسسة وتصميم البرامج وتشتمل على وظائف المخاطر والرقابة والإشراف على الالتزام

المسؤولة عن ضمان وجود عمليات وضوابط خط الدفاع الأول وتشغيلها بفعالية.

خط الدفاع الثالث يتمثل في وظيفة المراجعة الداخلية IAF التي توفر لمجلس الإدارة ولجنة المراجعة / المخاطر توكيد شامل بناء على أعلى مستوى من الاستقلالية والموضوعية داخل المنظمة بأن استراتيجية وسياسات وإجراءات وضوابط إدارة المخاطر السيبرانية فعالة وهذا ينطوي على مراجعة مدى كفاية العمل الذي قام به خطى الدفاع الأول والثاني والتنسيق معهم.

المحور الثالث: مخاطر الأمن السيبراني في المصارف الإلكترونية.

تواجه المخاطر الإلكترونية مجموعة من مخاطر الأمن السيبراني حيث يصاحب تقديم العمليات المصرفية الإلكترونية مخاطر متعددة وقد أشارت لجنة بازل للرقابة المصرفية إلى أنه ينبغي قيام البنوك بوضع السياسات والإجراءات التي تتيح لها إدارة هذه المخاطر من خلال تقييمها والرقابة عليها ومتابعتها وقد سبق وأشرنا إلى أن المخاطر السيبرانية تندرج تحت مسمى المخاطر التشغيلية التي تواجه المصارف وتتمثل تلك المخاطر وطبقا لما جاء بدراسة ( البغدادي ،2021) في الاتي:

1- استهداف البنية التحتية للمصرف الإلكتروني أو تعطيل عملها

2- استغلال الثغرات

3- اختراق البيانات

4- استهداف الهواتف الذكية

المحور الرابع: إدارة مخاطر العمليات المصرفية الإلكترونية.

أشارت لجنة بازل للرقابة المصرفية إلى أهمية قيام البنوك بوضع السياسات والإجراءات التي تتيح إدارة مخاطر العمل المصرفي الإلكتروني من خلال تقييمها والرقابة عليها ومتابعتها تندرج إدارة مخاطر العمليات المصرفية الإلكترونية تحت طائفة مخاطر التشغيل risk operational التي أصدرتها لجنة بازل للرقابة المصرفية في مارس 1998 ومايو 2001 ولا يمنع ذلك من توافر بعض أنواع المخاطر الأخر كمخاطر السمعة والمخاطر القانونية وفيما يلي عرض موجز لهذه المخاطر

1- مخاطر التشغيل Risk operatinal

تنشأ مخاطر التشغيل من عدم التأمين الكافي للنظم أو عدم ملاءمة تصميم النظم أو إنجاز العمل أو أعمال الصيانة وكذا نتيجة إساءة

الاستخدام من قبل العملاء وذلك على النحو التالي

- عدم التأمين الكافي للنظم system security
- عدم ملاءمة تصميم النظم أو إنجاز العمل أو أعمال الصيانة:
- إساءة الاستخدام من قبل العملاء customer misuse of services

2- مخاطر السمعة:

تنشأ مخاطر السمعة نتيجة عدم مقدرة البنك على إدارة أنظمته بكفاءة أو حدوث اختراق مؤثر لها ومن أجل حماية البنك يتعين عليه تطوير ورقابة ومتابعة معايير الأداء بالنسبة إلى عمليات المصارف الإلكترونية بحيث أنه

- تقدم البنوك المعلومات المناسبة عن مواقعها على الإنترنت للعملاء المحتملين بالتوصل إلى استنتاجات مدروسة حول هوية البنك ومركزه القانوني وذلك قبل الدخول بتنفيذ معاملات مصرفية إلكترونية
- تتخذ البنوك الإجراءات المناسبة للتأكد من الوفاء بمتطلبات سرية العميل حسب الدول التي يقدم فيها البنك منتجاته وخدماته المصرفية إلكترونيا
- أن تتوفر للبنوك القدرة على استمرار النشاط وعمليات التخطيط للطواري للمساعدة على ضمان توافر النظم والخدمات من خلال العمليات الإلكترونية
- تلتزم البنوك بإعداد خطط مناسبة تتضمن الاستجابة للحوادث والحد منها وخفض المشكلات الناتجة عن الحوادث غير المتوقعة بما في ذلك أنواع الهجوم الداخلي والخارجي التي قد تعوق تزويد النظم والخدمات المتعلقة بالعمليات المصرفية الإلكترونية

3- المخاطر القانونية

وهي تلك المخاطر الناجمة عن عدم التحديد الواضح للحقوق والالتزامات القانونية الناتجة عن العمليات المصرفية الإلكترونية وتبرز أهم التحديات القانونية في تحدي قبول القانون لحجية التعاقدات الإلكترونية في الإثبات وسائل الدفع والتحديات الضريبية وإثبات الشخصية والتواقيع الإلكترونية أنظمة الدفع النقدي والمال النقدي أو الإلكتروني سرية المعلومات وأمنها من مخاطر إجرام التقنية العالية خصوصية العميل وعلاقة وتعاقدات المصرف مع الجهات المزودة

للتقنيـة أو المـوردة لخـدمات أو مشـاريع الانـدماج والمشـاركة والتعـاون المعلوماتي.

الضوابط الأساسية في إدارة العمليات المصرفية الإلكترونية:

هنـاك مجموعـة مـن الضـوابط الأساسـية فـي إدارة العمليـات المصرفية الإلكترونية سواء لكل من البنك والعملاء.

بالنسبة للبنك عند تقديم خدماته عبر شبكات الاتصال الإلكترونية

1- موافقـة مجلـس إدارة البنـك علـى استراتيجية تتضـمن قيـام البنـك بتقـديم خدماتـه عبـر الشـبكات علـى أن يحـاط المجلـس بكافـة المخاطر الناشئة عن ذلك
2- موافقة مجلس إدارة البنك على سياسة الإدارة التنفيذية للبنك فيما يتعلق بأسلوب إدارة المخاطر وتدعيم نظم الرقابة الداخلية بشأن تلك المخاطر
3- تصـميم نمـاذج عقـود لتأديـة مختلـف الخـدمات المصـرفية التـي تـؤدي عبـر شـبكات الاتصـال الإلكترونيـة وأن يتأكـد البنـك مـن تـوافر القـوى البشـرية المؤهلـة للتعامـل مـع عمـلاء البنـك عبـر الشبكات مع تحديد ساعات تقديم هذه الخدمات
4- في حالة وجود طرف آخر تقدم من خلاله الخدمة فيتعين على مجلس إدارة البنك إقرار اتفاقية التشغيل التي تنظم العلاقة بين البنك مع هذا الطرف وتحديد مسئوليته في الحفاظ على سرية التعليمـات والمعـاملات التـي تـتم عبـر الشـبكات وأيـة معلومـات تتاح له
5- إفصاح على صفحة الـWeb الخاصة بـه بمـا يفيد حصـوله علـى تـرخيص بتقـديم خدماتـه عبـر الشـبكات مـن البنـك المركـزي المصـري ورقـم وتـاريخ الحصـول علـى التـرخيص والخـدمات التـي يجـوز للبنـك تقديمها عبـر الشـبكات مـع ربـط هـذا الموقـع بصفحة البنك المركزي المصري المعلن فيها عن أسماء البنـوك المرخص لها بذلك من خلال Hypertext links حتـى يتحقق العملاء من صحة التصريح
6- إفصاح البنك عن أن القوانين المصرية هي التـي تحكم الخـدمات التي يقوم بتأديتها للعملاء عبر الشبكات
7- ضـرورة أن يتحقـق البنـك مـن شخصـية طالـب / متلقـي الخدمـة بأساليب قانونية ثابتة تضمن الحقوق المتبادلة

بالنسبة للعميل عند تلقي خدماته عبر شبكات الاتصال الإلكترونية

1- يتحمل العميل مسئولية صحة المعلومات التي يقوم بإدخالها عبر الشبكات باعتباره مستخدماً للخدمات التي تؤدي من خلالها ويقر العميل بأن التعليمات والمعاملات التي يدخلها يتم التعامل عليها بدون أية مراجعة إضافية من البنك أو إشعارات خطية أو التأكد منها بطرق أخرى.
2- لا يلتزم البنك بقبول أية تعديلات أو إلغاء تعليمات أو معاملات سبق أن أرسلها العميل عبر الشبكات
3- يتحمل العميل مسئولية إعداد البيانات الخاصة بالمستفيد أو الإضافة أو التعديل عليها.
4- يلتزم العميل بمراعاة إجراءات الحماية في التعامل عبر الشبكات مع البنك
5- يتحمل العميل مسئولية سوء استخدام الخدمة الناتج عن عدم الالتزام بإجراءات الحماية والشروط والأحكام الواردة في العقد الذي يتم إبرامه مع البنك بشأن العمليات المصرفية الإلكترونية أو الناتج عن قيامه بالكشف عن إجراءات الحماية أو مخالفتها لدى الاستخدام
6- عدم تحمل البنك مسئولية تعطل الخدمة لظروف خارجة عن إرادته
7- تعتبر سجلات البنك حجة قاطعة ملزمة قانوناً على صحة المعاملات والتعليمات
8- يلتزم العميل في حالة فقد أو سرقة جهاز الشفرة بإخطار البنك لكي يقوم بإبطال هذا الجهاز
9- تعتبر أدوت الحماية وسيلة للتعرف والتحقق من شخصية العميل وبمجرد إتمام إدخالها بنجاح يعتبر العميل هو مصدر جميع التعليمات والمعاملات

استراتيجية إدارة مخاطر العمليات المصرفية الإلكترونية

تشتمل استراتيجية إدارة المخاطر على التقييم والرقابة والمتابعة وذلك على النحو التالي

- تقييم المخاطر
- إعداد خطط طوارئ بديلة في حالة إخفاق النظم عن أداء الخدمات.
- متابعة المخاطر

- التأكد من فاعلية إجراءات المراجعة الداخلية والخارجية

المحور الخامس: معوقات تعزيز الأمن السيبراني في المصارف الإلكترونية.

إن غياب الأمن السيبراني وهو ما يمكن تسميته بالإرهاب الإلكتروني هو نموذج جديد لهذا العصر التكنولوجي القائم على العولمة، إن الإرهاب الإلكتروني سوف يكون عدو للحكومة الإلكترونية وإن كان هذا التطور موجود فقط في الدول المتقدمة ومازال فكرة أو مشروع بالنسبة للدول النامية لأن الإرهاب الإلكتروني يرى في هذا النوع من التطور عرقلة لمشاريعه غير المشروعة وبالتالي يصعب عليه كل التصرفات من غسيل وتحويل وتبيض الأموال أو حتى اختراق هذا النظام، وتتمثل معوقات تعزيز الأمن السيبراني في الآتي:-

معوقات تعزيز الأمن السيبراني

بالنظر إلى طبيعة مخاطر وتهديد الأمن السيبراني يمكن تحديد المشكلات التي تواجهها الدول وخاصة في العالم العربي كما يلي

- نقص وعدم وضوح البيئة التشريعية
- عدم وجود بيئة تنفيذية ملائمة

المحور السادس: آليات تعزيز الأمن السيبراني في المصارف الإلكترونية.

دعت الحاجة إلى وجود مجموعة من الآليات التي يكمن الغرض منها في تعزيز الأمن السيبراني في المصارف الإلكترونية والتي ضمت الآتي:- **(البغدادي، 2021 )**

أولا استراتيجيات التغلب على التحديات في مجال أمن نظم المعلومات والفضاء الإلكتروني

تتمثل أهم استراتيجيات التغلب على التحديات في مجال أمن نظم المعلومات والفضاء الإلكتروني في فيما يلي:

- أهمية قيام الأجهزة الرقابية والمؤسسات بتوفير الدورات التدريبية عالية المستوى وتنظيم الندوات وورش العمل والمؤتمرات بمشاركة الشركات والمؤسسات الدولية المتطورة في مجال تقنية المعلومات لاطلاع الكوادر الفنية على أحدث التقنيات لمواكبة التطور السريع والتعرف على التقنيات الحديثة في مجال الخدمات الإلكترونية على المستوى العالمي وذلك بهدف خلق كوادر فنية عالية المستوى قادرة على التصدي للتحديات الجديدة المرتبطة بهذه التقنيات وكيفية التغلب عليها

- أهمية وضع الأجهزة الرقابية العربية الآلية رقابية وضحة على البنوك والمؤسسات المالية للتأكد من وجود ضوابط وسياسات لتحقيق المن السيبراني
- أهمية حصول المؤسسات المالية والمصارف بالدول العربية على أحدث التقنيات سواء فيما يتعلق بالأجهزة Hardware أو البرامج software لمواجهة أحدث التطورات والأساليب المتبعة في مجال الهجمات والقرصنة الإلكترونية الدولية بهدف اقتناء جدار أمني أكثر فعالية قادر على التصدي لأحدث الأساليب المتعبة في هذا الشأن
- أهمة استحداث تخصص الأمن السيبراني في الجامعات العربية المتخصصة في مجال تقنيات المعلومات أسوة بالجامعات العالمية بهدف خلق الكوادر العربية المتخصصة ذات المستوى العالي في هذا المجال
- قيام الهيئات والجهات الرقابية في الدول العربية بإصدار التعليمات والقواعد المنظمة الخاصة بقيام المصارف والمؤسسات المالية بإجراء عقود لأطراف ثالثة تختص بأمن نظم المعلومات على أن تخضع تلك الشركات التي يتم التعهد إليها للرقابة الصارمة من قبل الأجهزة الأمنية العربية للقضاء على عمليات الاحتيال والقرصنة على الأنظمة الإلكترونية في تلك البنوك والمؤسسات
- مدى أهمية قيام المصارف والمؤسسات المالية العربية بتخصيص الموارد والمخصصات الكافية للحصول على أحدث التقنيات في مجال أمن نظم المعلومات والفضاء السيبراني حيث تتسم تلك التقنيات بالارتفاع الملحوظ في تكلفة اقتناءها
- العمل على تكثيف التوعية لدى العملاء من خلال البرامج المسموعة والمرئية والندوات التثقيفية لرفع المستوى الخاص بثقافة الأمن السيبراني لدى المتعاملين بالقطاع المالي والمصرفي بهدف تفهم الضوابط والتعليمات الخاصة بأمن نظم المعلومات والفضاء السيبراني

**ثانيا الجوانب المتعلقة بأمن الفضاء الإلكتروني في إطار المخاطر التشغيلية للبنوك المركزية العربية [1]**

وتتمثل أهم هذه الجوانب المتعلقة بأمن الفضاء الإلكتروني في إطار المخاطر التشغيلية للبنوك المركزية العربية فيما يلي:

1-الإطار الرقابي العام للمخاطر المرتبطة بأمن نظم المعلومات والفضاء السيبراني

2-تنظيم وإدارة الحسابات والخدمات المصرفية المقدمة عبر الإنترنت

3-وسائل إثبات الهوية عبر الإنترنت

المحور السابع رؤية جمهورية مصر العربية في مجال الأمن السيبراني طبقا 2030

عندما ننظر إلى رؤية جمهورية مصر العربية 2030 والتي تؤكد من خلالها على أهمية التوسع في الاستخدام الإلكتروني في الأعمال الحكومية والعلمية والتجارية فقد أشارت كثير من التقارير العالمية والمحلية إلى تعرض مصر إلى العديد من الهجمات اسيبرانية ولكن تم اتخاذ إجراءات الأمان والتحصين وبحسب ما أعلنت عنه إحدى الشركات الأمنية السيبيرية الفرنسية فإن هذا الهجوم يشل عمل الأجهزة الإلكترونية ويستغل ثغرة موجودة في نظام تشغيل ويندوز

وسوف يتم استعراض جهود الحكومة المصرية بشأن تعزيز الأمن السيبراني في الآتي:

1-إنشاء الجهاز القومي لتنظيم الاتصالات التابع لوزارة الاتصالات ( المركز المصري للاستجابة للطوارئ المعلوماتية ) ( سيرت ) وذلك لتعزيز أمن البنية المعلوماتية وبنية الاتصالات في مصر

2- جمع المعلومات حول الحوادث الأمنية وتحليلها والسعي الدائم نحو إيجاد حلول لتلك الحوادث

3- التنسيق بين الهيئات الحكومية والمالية المتعددة بهدف توفير إنذار مبكر ضد انتشار البرمجيات الخبيثة والهجمات السيبرانية التي تحول دون اكتمال البنية التحتية للاتصالات في مصر

4- عدم الإخلال بأي عقوبات جنائية قد تنشأ نتيجة وقوع أضرار جسيمة تتعلق بعدم الالتزام بتأمين البنية التحتية الحرجة للاتصالات وتكنولوجيا المعلومات حيث يسأل تأديبياً كل موظف أو عامل يخالف قرارات المجلس الأعلى للأمن السيبراني

5- تطوير الضوابط الأساسية للأمن السيبراني بعد دراسة عدة معايير وأطر وضوابط للأمن السيبراني من خلال التنسيق بين عدة جهات ومنظمات محلية ودولية مختلفة، ودراسة متطلبات التشريعات والتنظيمات والقرارات الوطنية ذات العلاقة

**نتائج البحث وتوصياته**

**وفي ضوء ما سبق انتهى البحث إلى النتائج التالية:**

1- التطور الحادث في المخاطر السيبرانية يحفز المؤسسات المالية على البحث المستمر والمكثف نحو اتخاذ إجراءات وقائية من تلك المخاطر من خلال لوائح تجعل تلك الإجراءات أكثر وضوحاً أمام مجالس إدارات تلك المؤسسات الأمر الذي يؤدي إلى خلق حافز أكبر على الاستثمار بشكل مستمر في تحسين الأمن السيبراني

2- محاولة إضافة المخاطر السيبرانية ضمن المخاطر التشغيلية للمؤسسات المالية يعتبر غير كافي حيث أن المعايير الرقابية على المصارف تتطلب أهمية تضمين الاستراتيجيات والسياسات الخاصة بتلك المصارف جزء خاص بإدارة المخاطر السيبرانية

3- هناك جهود تبذل في كافة المصارف على المستوى المحلي والعالمي بهدف تعزيز آليات الأمن السيبراني في المصارف الإلكترونية وذلك بهدف الحد من المخاطر السيبرانية على المستوى العالمي

توصيات البحث

نظرً لما يصاحب إجراء العمليات المصرفية التقليدية والإلكترونية وإصدار وسائل دفع النقود الإلكترونية من مخاطر متعددة فإن البحث يوصي بالتالي

1- وضع إطار عام لمراجعة وإدارة المخاطر السيبرانية وتحديد مسئوليات مختلف الجهات ذات الصلة بها وما يستلزم ذلك من الحصول على ترخيص من البنك ومواقته بالبيانات اللازمة

2- عقد الدورات التدريبية ذات الصلة وتنظيم ورش العمل والمؤتمرات بمشاركة الشركات والمؤسسات الدولية المتطورة في مجال تقنيات المعلومات

3- العمل على تكثيف التوعية لدى المستخدمين من خلال البرامج المسموعة والمرئية والندوات التثقيفية لرفع المستوى الخاص بثقافة الأمن السيبراني
4- ضرورة الاطلاع على التجارب الرائدة في مجال عمليات البنوك الإلكترونية وإدارة مخاطرها ومحاولة استخراج نقاط القوة والضعف ومعرفة الاستفادة منها
5- التوجه نحو المزيد من الاستثمار في مجال الأمن السيبراني من خلال توطين التكنولوجيا والبني التحتية السيبرانية

المراجع

1- د/ أحمد جمال الدين موسى: النقود الإلكترونية وتأثيرها على المصارف المركزية في إدارة السياسة النقدية الجديد في أعمال المصارف من الوجهتين القانونية والاقتصادية أعمال المؤتمر العلمي السنوي لكلية الحقوق جامعة بيروت العربية الجزء الأول، الجديد في التقنيات المصرفية منشورات الحلبي الحقوقية، بيروت 2002
2- الاتحاد الدولي للاتصالات: دليل الأمن السيبراني للبلدان النامية 2007 الموجز التنفيذي المعلومات والاتصالات
3- د/ خالد ممدوح العزي: الجرائم المالية الإلكترونية الجرائم المصرفية نموذجا بحث مقدم في المؤتمر الدولي الرابع عشر: الجرائم الإلكترونية طرابلس لبنان، 24 – 25 مارس 2017
4- حمدون أ. توريه وآخرين: البحث عن السلام السيبراني الاتحاد الدولي للاتصالات والاتحاد العالمي للعلماء يناير 2011
5- صندوق النقد العربي: سلامة وأمن المعلومات المصرفية الإلكترونية، اللجنة العربية للرقابة المصرفية أمانة مجلس محافظي المصارف المركزية ومؤسسات النقد العربية، العدد 72 أبو ظبي الإمارات العربية المتحدة 2017
6- حسن بن علي العجمي: الثورة الصناعي الرابعة وتغييرات الحياة الإنسانية المجلة العربية العدد 498 أبريل 2018
7- صندوق النقد العربي: سلامة وأمن المعلومات المصرفية الإلكترونية، اللجنة العربية للرقابة المصرفية أمانة مجلس محافظي المصارف المركزية ومؤسسات النقد العربية، العدد 72 أبو ظبي الإمارات العربية المتحدة 2017

8- د/ هبة أحمد عبد الدايم & د/ منار محمد شعبان: الهجمات السيبرانية، دراسات دورية بنك الاستثمار القومي قطاع الاستثمار والموارد – الدعم الفني للاستثمار العدد التاسع يوليو 2017
9- مروة فتحي السيد البغدادي، 2021، اقتصاديات الأمن السيبراني في القطاع المصرفي، مجلة البحوث القانونية والاقتصادية – كلية الحقوق، جامعة المنصورة، المجلد 76.

ثانيا المراجع الأجنبية:

1- Antoine Bouveret: Cyber Risk for the financial sector: A Framework for Quantitative assessment working paper IMF June 2018
2- Cebula J.J and L.R Young: A taxonomy of operational Cyber security Risks Technical Note CMU/SEI-2010-TN-028 software Engineering Institute Carnegie Mellon University 2010
3- Eling M. And J.H. wirfs: Cyber Risk: too big toinsure ? Risk transfer options for a mercurial risk class institute of Insurance Economics University of St. Gallen 2016
4- Emanuel Jopp Lincoln Kaffenberger and christopher wilson: cyber risk market failures and financial stability working paper No 17/185 IMF 2017
5- Price water house Coopers Cyber security M&A: decoding deals in the Global cyber security industry Nov. 2018
6- S. Friedman Taking cyber risk management to the next level – lessons learned from the front lines at financial institutions Deloite insight June 2019
7- World Bank: cyber security Cyber risk and financial sector Regulation and supervision Feb 2020.