مخاطر التكنولوجيا المالية وإدارتها في القطاع المصرفي –دراسة تنظيمية واحترازية

Financial technology risks and their management in the banking sector - a regulatory and precautionary study.

محمد قوجيل*[1]، عبد العزيز طيبة[2]

[1] مخبر الأنظمة المالية والمصرفية والسياسات الاقتصادية الكلية جامعة حسيبة بن بوعلي بالشلف (الجزائر)، mk.koudjil@univ-chlef.dz

[2] مخبر الأنظمة المالية والمصرفية والسياسات الاقتصادية الكليةجامعة حسيبة بن بوعلي بالشلف (الجزائر)، a.taiba@univ-chlef.dz

تاريخ الإرسال:2021/04/30 تاريخ القبول: 2021/05/17 تاريخ النشر: 2022/06/03

ملخص: تهدف هذه الدراسة الى ابراز المخاطر المختلفة الناشئة عن استخدام التكنولوجيا المالية بتقنيتها المتعددة في القطاع المصرفي، وهذا عن طريق التعرض مجموعة الاجراءات التنظيمية والاحترازية في المجال على غرار بنك نيقارا الماليزي، البنك الدولي، إدارة الخدمات المالية في نيويورك (NYDFS)....، هذا التنوع في الهيئات يعطى مفاهيم اكثر دقة واكثر شمول للأنواع المختلفة لتلك المخاطر المتعلقة بالتكنولوجيا المالية، ومن ثما عرض الحلول الاحترازية والتنظيمية التي فرضتها او اوصتها بها تلك الهيئات، والتي اجمعت على ان جميع الارشادات والتوجيهات التنظيمية تصب في نطاق وضع استراتيجيات متابعة وتدقيق مختلف العمليات المالية عبر تقنيات الفينتك، وكذا التحيين الدوري واجراء اختبارات الاداء المتعلقة بتلك الانظمة، وغيرها من النقاط الاحترازية التي قمنا بتفصيلها ضمن محتوى الدراسة.

الكلمات المفتاحية: التكنولوجيا المالية، إدارة المخاطر، الصناعة المصرفية، الأمن السيبراني.

تصنيفJEL: O33، E44، G21، G22.

Abstract: This study aims to highlight the various risks arising from the use of financial technology with its multiple technology in the banking sector, by examining the set of regulatory and precautionary measures in the field, such as the Malaysian Bank Nigara, the World Bank, and the New York Financial Services Department (NYDFS) ...., This diversity in the bodies gives more accurate and comprehensive concepts of the different types of those risks related to financial technology, and then presenting the precautionary and regulatory solutions imposed or recommended by these bodies, and which unanimously agreed that all the regulatory instructions and directives fall within the scope of developing strategies for monitoring and auditing various financial operations. Through Fintech techniques, as well as periodic updating and performance tests related to those systems, and other precautionary points that we have detailed within the content of the study

Keywords: Financial technology, risk management, banking industry, cyber security

Jel Classification Codes : O33, E44, G21, G22.

*المؤلف المرسل

توطئة (مقدّمة):

يعرف القطاع المصرفي ثورة جد متقدمة في ابتكار وتطوير منتجاته ومعاملاته المختلفة، إذ كان لظهور التكنولوجيا المالية اثر على تنويع وتوسيع استثمارات العاملين في القطاع، وكذلك ظهور مؤسسات غير مصرفية أصبحت تنافس وتدعم المصارف في هذا المجال من شركات التكنولوجيا المالية مثل شركة Anti Financial وAdyen وQudian وSofi وAvant وغيرها، فاحدث هذا التغيير في الابتكار والتطور ما يسمى بالثورة الرابعة والخامسة، والتي تجلت في تقديم منتجات وخدمات مالية ومصرفية بالاعتماد على التقنية الحديثة من أجهزة الحاسوب والشبكات العنكبوتية التي وطنت لبنية تحتية مبنية على تقنيات ومنصات للتداول والتعامل على غرار تقنية سلاسل الكتل كسجل للتوطين وحفظ وإجراء المعاملات المختلفة بالاعتماد على التشفير، وكذا تقنيات التمويل الجماعي، الذكاء الاصطناعي في المجال المصرفي، العقود الذكية، والعملات الرقمية المشفرة أشهرها البتكوين، فقد قللت هذه التقنيات من دور الوساطة المالية التي كانت تقوم بها البنوك وبعض المؤسسات المالية، إذ يمكن القول انه اليوم نحتاج إلي أعمال مصرفية دون الحاجة إلي بنوك بحكم الانتشار والتوسع الذي تعرفه تلك التقنيات وزيادة الانفتاح عليها واشتداد المنافسة فيها، وقد فرضت التكنولوجيا المالية تحديات إضافية على القطاع المصرفي وعلى قدرة الأنظمة المصرفية التعامل مع هذا المد العلمي الهائل، وتكييف الأنشطة وفق مخرجات التكنولوجيا المالية، بالإضافة إلى أن هذه التقنيات خلقت العديد من المخاطر واللاأمن، مما يجعل إدارة المخاطر المالية والمصرفية أمام تحدي دائم لمواكبة التطور والابتكار في مجال التكنولوجيا المالية، اذ أصبحت البنوك عرضة لمخاطر الاختراق والقرصنة نظير الاعتماد الكبير على البرمجة والأنترنت.

بناء على ما تقدم، يمكننا صياغة السؤال الرئيس للدراسة كما يلي: ما هي الإجراءات التنظيمية والاحترازية المتخذة في القطاع المصرفي للحد من مخاطر التكنولوجيا المالية؟

من السؤال الرئيس نطرح الأسئلة الفرعية لضبط الجوانب المحيطة بالموضوع كما يلي:

- ما هي الأنواع المختلفة للمخاطر الناتجة عن استخدام التكنولوجيا المالية في القطاع لمالي والمصرفي؟
- ما هي العوامل المساعدة على اختراق تقنيات التكنولوجيا المالية المختلفة؟
- فيما تكمن الإجراءات المتخذة من قبل الأنظمة المصرفية ومؤسسات التكنولوجيا المالية لمجابهة وإدارة تلك المخاطر عبر العالم؟

للإجابة على السؤال الرئيس والأسئلة الفرعية نطرح الفرضيات التالية:

- يوجد اثر او علاقة بين التوسع في استخدام تقنيات التكنولوجيا المالية وزيادة المخاطر في الصناعة المالية والمصرفية.
- زيادة استخدام تقنيات التكنولوجيا المالية زاد من قدرة البنوك والمؤسسات المالية على اتخاذ اجراءات وتدابير ادارة مخاطر التكنولوجيا والحد من آثارها.

أهمية وهدف الدراسة:

تتجلى أهمية الدراسة في تسليط الضوء على أهم المخاطر المرتبطة باستخدام تقنيات التكنولوجيا المالية وكيفية التعامل معها، والتي نهدف من خلالها لإبراز الأثر بين استخدام التكنولوجيا المالية والنشاط المالي والمصرفي ومدى الترابط بينهما، مع ضرورة إيجاد جملة الإجراءات والتدابير الاحترازية اللازمة لتجنبها والوقاية منها.

المنهج الدراسة:

اعتمدنا في دراستنا على المنهج الاستنباطي من خلال أداة الوصفي عرض الجانب النظري لمفاهيم التكنولوجيا المالية ومختلف تقنياتها، وكذا تعريف الخطر السيبراني ومخاطر التكنولوجيا المالية، وعلى اداة التحليل بهدف تحليل بعض المعطيات والنتائج المتعلقة بالبيانات الخاصة بأكثر المخاطر تأثيرا على القطاع المالي وتوزيعها عبر العالم،بالإضافة إلى تحليل البيانات الخاصة بالفئات التي يستهدفها الهجوم السيبراني خلال الفترة 2014-2021 ومختلف البرامج الضارة في العالم عام 2019.

الدراسات السابقة:

- دراسة (**Antoine Bouveret (June 2018** بعنوان **Cyber Risk for the financial sector.A Framework** **IMF Workingpaper**، وهي عبارة عن ورقة بحثية للمؤلف نشرها صندوق النقد الدولي تحت الرقم (WP/18/143)، تمثل دراسة قياسية لإبراز اثر الهجمات السيبرانية ومخاطر الانترنت على القطاع المالي والمصرفي العالمي، حيث نبهت الدراسة إلى ضرورة إيجاد إطار لتقييم

مخاطر الانترنت وتوحيد البيانات والمعلومات لأجل تقديم دراسات قادرة على إيجاد الحلول المشترك للخطر، من خلال إبراز تركز تلك المخاطر في مناطق مختلفة من العالم خاصة في الدول النامية والغير متطورة مقارنة بالدول المتقدمة، كما أعطت الدراسة مختلف الهجمات التي مست القطاع المالي والمصرفي شركات التكنولوجيا المالية عبر العالم، لتختم نتائج الدراسة بأن مخاطر الانترنت أو الأمن السيبراني أصبح مصدر قلق رئيسي للمشاركين في الأسواق العالمية وواضعي السياسات في العالم.

- دراسة **Lavinia Franco and All (May 2020)** بعنوان **Does Fintech Contribute to SYSTEMIC Risk? EVIDENCE FROM THE US AND EUROPE**، وهي سلسلة اوراق عمل نشرها معهد البنك الأسيوي للتنمية تحت الرقم(No1132)، تعرض المؤلفون إلى دراسة مدى صحة فرضية تأثير التكنولوجيا المالية على ظهور المخاطر النظامية من عدمها، في البداية نوهت الدراسة إلى مختلف تقنيات التكنولوجيا المالية المستخدمة مثل تقنية البلوك شين والعملات المشفرة،ثم تم التطرق إلىإجراء دراسة قياسية على عينة من شركات التكنولوجيا المالية فيأمريكاوأوروبا حيث تشكل 39 شركة أمريكية و53 أوربية ، دراسة حجم التغيرات للفترة جانفي 2010 إلى ديسمبر 2017، كما تم إجراء مقارنة لحجم نمو شركات الفينتيك بين المنطقتين مقارنة بشركات المالية التقليدية وحجم أصولهما، لتظهر نتائج الدراسة انه يستبعد اعتبار أن لتكنولوجيا المالية اثر في حدوث المخاطر النظامية، وان ساهمت فان مساهمتها ضئيلة جدا لا تتعدى 0.05 % فياروبا و 0.03% فيأمريكا.

- دراسة لـ **Milena ,Vučinić (January 2020)** تحت عنوان **Fintech and Financial Stability Potential Influence of FinTech on Financial Stability, Risks and Benefits**, مقال منشور في مجلة النظرية والتطبيق المصرفي المركزي، مونتنيغرو، 10-2478/jcbtp-2020-0013 ، سلطت الدراسة الضوء على التطور الكبير الذي عرفه المجال المالي والمصرفي العالمي، والذي انتقل من المعاملات التقليدية الى معاملات حديثة قائمة على تقنيات التكنولوجيا المالية المتعددة، والتي وضعت القائمين على القطاع المالي العالمي امام تحدي كبير للمحافظة على الاستقرار المالي وتجنب اثار استخدام التكنولوجيا المالية، لتظهر الدراسة كذلك مدى توسع مجال ونطاق استخدام الفينتك ومن ثم تغير التفضيلات الاستهلاكية للعملاء، لتخلص الدراسة الى انه يمكن ان تغير التكنولوجيا المالية صورة المعاملات المالية التقليدية، ولكنها تتميز بدرجة مخاطرة تهدد فعليا الاستقرار المالي العالمي.

1. ماهية التكنولوجيا المالية وتقنياتها الحديثة

يشهد العالم اليوم موجة من التطور والابتكار، والتي أصبحت جزء من حياة البشرية، وضرورة لا بد منها من اجل الاستمرار والمنافسة، لتحقيق الأهداف المبنية وفقا لاستراتيجيات البحث والتطوير، فأصبح مصطلح التكنولوجيا المالية الأكثر شيوعا وتداولا بين فئات مختلفة للمجتمعات، ولقي اهتماما منقطع النظير من قبل الباحثين والمستثمرين، والجهات الحكومية.

1.1.تعريف التكنولوجيا المالية (fini tech):

تعرّف التكنولوجيا المالية على أنها تلك الشركات أو ممثلي الشركات التي تجمع بين الخدمات المالية والتقنيات الحديثة والمبتكرة، كقاعدة تقدم للسوق عرضًا لمنتجات وخدمات قائمة على الإنترنت والتطبيق بهدف جذب العملاء بأكثر سهولة في الاستخدام وفاعلية وشفافية من تلك المنتجات والخدمات المتاحة من قبل(Gregor & Lars , 2016, p. 5)، ومصطلح "FinTech"، هو اختصار لعبارة " Financial technology".

وتعرّف كذلك بأنها تشير إلى مجموع الشركات التي تقدم الابتكار في الخدمات المالية باستخدام التقنيات الحديثة , AGUSTIN) (2017، كما يعرّفها مجلس الاستقرار المالي كذلك بأنها ابتكار ممكّن تقنيًا في الخدمات المالية يمكن أن ينتج عنه نماذج أعمال جديدة أو تطبيقات أو عمليات أو منتجات ذات تأثير مادي مرتبط على الأسواق المالية والمؤسسات المالية وتقديم الخدمات المالية Financial) (Stability Board, 2020،

في حين عرّفتها لجنة بازل على أنها أي تكنولوجيا او ابتكار مالي ينتج عنه نموذج أعمالأو عملية أو منتج جديد له تأثير على الأسواق والمؤسسات المالية، وعليه فان مصطلح التكنولوجيا المالية عبارة عن دمج الجانب المالي مع الجانب التكنولوجي لينتج عنه مجال جديد

يهتم بالمعاملات والخدمات المالية واعتمادا على مخرجات التكنولوجيا الجديدة من (هواتف ذكية، شبكات اتصالات، ذكاء اصطناعي، انترنت ، big data) وغيرها من تطبيقات الثورة الرابعة(مغربي و ثريا، 2020).

يمكن القول بأن التكنولوجيا المالية تمثل ذلك المزيج بين التقنيات والتطبيقات التكنولوجية الحديثة، والعمليات المالية والمصرفية، للحصول على منتجات وخدمات مالية جديدة تتميز بالحداثة والابتكار والجودة وكذا سهولة الوصول والاستخدام من كل مكان وفي أي وقت.

2.1. محتوى التكنولوجيا المالية وتقنياتها:

تتضمن التكنولوجيا المالية على وجه التحديد الإنترنت والبيانات الضخمة، الحوسبة السحابية،سلاسل الكتل والذكاء الاصطناعي،أي كل ابتكار في الخدمات المالية وفي منصات الإقراض القائمة على السوق، ابتكار في المدفوعات، تداول ذكي وابتكار مالي، من خلال استخدام التكنولوجيا المالية، يمكن أن تكون الصناعة المالية أكثر كفاءة في جانب واحد أو أكثر من العمليات، مما يقلل التكاليف ويزيد الكفاءة ويحسن تجربة المستخدم(Zhang & Yang , 2018).

يمكن تقسيم شركات صناعة التكنولوجيا المالية إلى أربعة قطاعات رئيسية وفقًا لنماذج أعمالها المميزة، من خلال القياس مع المجالات التقليدية ذات القيمة المضافة لبنك عالمي، يمكن تمييز استعمالات التكنولوجيا المالية على أساس، مشاركتها في التمويل وكذا عمليات الاقراض والاقتراض، إدارة الأصول، المدفوعات والتحويلات المالية الدولية واستخدامات مالية أخرى متمثلة في مجموعة كبيرة من الشركات التي تؤدي وظائف أخرى(Gregor & Lars , 2016, p. 6)، ومنها أنشطة التجارة والاستثمارات، تكنولوجيا التامين، المنتجات المالية لشركات الصغيرة، التمويل الجماعي، تحليل البيانات واتخاذ القرارات المالية، إدارة التمويل الشخصي، خدمات مصرفية عبر الجوال، تداول العملات المشفرة وتطبيقات سلاسل الكتل وغيرها(economyplus, 2020).

3.1. أنواع التقنيات المالية الحديثة واستخداماتها:

كان للابتكارات التكنولوجية والمعلوماتية الحديثة عدة تقنيات وتطبيقات استطاع القطاع المالي استغلالها والاستفادة منها، وهي متعددة نذكر منها:

– سلسلة الكتل او الثقة (BLOCKCHAIN) : عبارة عن سجل أو قاعدة بيانات موزعة عالميا وغير مركزية تعمل ضمن أجهزة كمبيوتر مختلفة، تنشأ عن طريق مجموع من الكتل غير قابلة للاستبدال وتظهر في جميع الأجهزة المستخدمة للنظام بتوقيت متزامن، لذلك فهي تتمتع بشفافية كبيرة لعدم تدخل إطراف خارجية في تشكيل كل كتلة أو تغييرها، لكونها تتمتع بنظام تشفير قوي، ويتم التأكيد على العمليات من خلال النظام بعد موافقة جميع الأجهزة المرتبط به(Keizer , 2017)، تعرف أيضا بأنها عبارة عن بنية بيانات لامركزية مع اتساق داخلي يتم الحفاظ عليه بإجماع المستخدمين بشان الحالة الآنية لشبكة أو السلسلة (سلسلة البيانات المخزنة نتيجة حدوث معاملات) , (Vikram David , & Max , 2017)

– العقود الذكية (Smart Contracts): عبارة عن عقد مبرمج الكترونيا يتم فيه التنفيذ التلقائي للبنودة عند استفاء الشروط التي حددها المتعاقدان على إحدى منصات التقنية المتاحة (بلوك شين او الايثريوم)(قندوز، 2019، صفحة 50) تستخدم مثلافي تنفيذ عقود الإيجار، دفع فواتير الخدمات المختلفة كالكهرباء..... .

– العملات المشفرة والرقمية: هي عبارة عن عملة غير مركزية وتستخدم التشفير لإنشاء وحدات منها والتحقق من صحة المعاملات بعيدا عن الحكومات والبنوك المركزية مثل البيتكوين، الريبل...الخ(قندوز، 2019، صفحة 52).

– الايثريوم(قندوز، 2019، صفحة 53): كعملة رقمية مشفرة وكتقنية مالية حديثة: هو عبارة عن نظام لامركزي متكامل يعتمد على تكنولوجيا البلوك شين، ويتيح العديد من الاستخدامات، يدار من قبل المنقبين الذين يسجلون العمليات والمعاملات عن طريقه سلسلة الكتل بمقابل عمولات، ليتم الحصول على عملات أيثر جديدة لمحافظهم، من أشهر الشركات استخداما لهذه التكنولوجيا مايكرو سوفت وانتل.

– الذكاء الاصطناعي: ابتكار يستخدم أجهزة الكمبيوتر والخوارزميات لزيادة محاكاة الذكاء البشري، وهو يعتمد على البيانات الضخمة والأساليب الإحصائية الحديثة لإعطاء التخمين والإجابة الدقيقة والمحددة، كما يسمح بعملية الأتمتة لتحقيق اكبر فعالية وكفاءة (Jayant &Rachel , 2019).. من أهم استخدامات الذكاء الاصطناعي في المعاملات المالية والمصرفية عديدة منها عمليات السوق وقرارات التسعير والتحوّط، العمليات الاستشرافية، إدارة المخاطر ، التفاعل الذكي مع العميل والتعرف على متطلباته(اتحاد المصارف العربية، 2020)

– **نظم المدفوعات:** عبارة عن تقنية من التقنيات المالية، تسمح للمستخدم القيام بدفع قيمة مشترياته والتزاماته المختلفة، وكذا تحويل مدفوعاته الكترونيا وعن بعد، هناك أيضا تقنية التكنولوجيا التنظيمية RegTech التي تتجلي في إدارة العمليات التنظيمية ضمن الصناعة المالية من خلال التكنولوجيا مع التوافق لقواعد الامتثال، والتي تشمل المراقبة التنظيمية وإعداد التقارير وكذا الالتزام، وأيضا تقنية إدارة الأصول والثروة تكنولوجيا التامين، الخدمات المصرفية المفتوحة (Open Banking) او خدمة الطرف الثالث هي السماح لطرف ثالث (شركات متخصصة في التقنيات المالية)من البنك ببناء تطبيقات وخدمات مبتكرة للعملاء باستخدام بيانات البنك (– Third Party Providers TTPs)(قندوز، 2019، صفحة 61).

2. مخاطر استخدام التكنولوجيا المالية في البنوك والمؤسسات المالية:

تتعرض الأنشطة المالية إلى جملة من المخاطر والتهديدات صنفها الاقتصاديون والمختصون إلى عدة أصناف منها المخاطر النظامية والمخاطر غير النظامية، منها مخاطر التكنولوجيا المالية التي اعتبرها الأغلبية كمخاطر تشغيلية باعتبارها تتعلق بالأجهزة والأنظمة المستخدمة وكذا العنصر البشري في بعض الأحيان، ولهذا فان الانفتاح على تلك التقنيات التكنولوجيا المالية الحديثة، وضع القطاع المصرفي في مواجهة ضد مخاطر تشغيلية جديدة تهدد نشاطه تزيد من حساسيته للمخاطر، نظرا لكون هذه التقنيات مبنية على أسس افتراضية عبر شبكات، غالب ما تكون سهلة الاختراق والوصول من قبل القراصنة، ما لم تخضع لإجراءات الرقابة والمتابعة المستمرة.

1.2.تعريف مخاطر التكنولوجيا المالية:

تشير مخاطر التكنولوجيا إلى المخاطر الناشئة عن استخدام تكنولوجيا المعلومات والإنترنت، تنشأ هذه المخاطر من إخفاقات أو خروقات في أنظمة تكنولوجيا المعلومات أو التطبيقات أو المنصات أو البنية التحتية، مما قد يؤدي إلى خسارة مالية أو اضطراب في الخدمات أو العمليات المالية أو ضرر على سمعة مؤسسة مالية(Bank NEGARA MALAYSIA, 2020).

تعرف كذلك على أنها كل خطر ناتج عن ابتكار وتقديم او تسويق منتج او خدمة جديدة تعتمد على التكنولوجيا المالية، وتخضع للمعالجة الالية وهي التي تتميز بسرعة الظهور او الاكتشاف(RSA security LLC, 2020)، وتسمى أيضا بمخاطر الانترنت والتي تصنف ضمن المخاطر التشغيلية التي تستهدف أصول المعلومات والتكنولوجيا مما يؤثر على سرية وعلى توافر وسلامة تلك المعلومات والأنظمة(Antoine , 2018, p. 6).

من خلال التعاريف السابقة، يمكن اعتبار مخاطر التكنولوجيا المالية كل خسارة، اختراق او تأثير تتعرض لها الأنظمة والتطبيقات والتقنيات التكنولوجية الحديثة المعتمدة في تقديم المنتجات والخدمات المالية مما يكون له الأثر السلبي على الأداء المالي للبنوك والمؤسسات المالية بما يتعارض وأهدفها المسطرة، وعليه يمكن اعتبارها ضمن المخاطر التشغيلية التي تعترض العمل المصرفي والمالي.

2.2. أهم مخاطر التكنولوجيا المالية:

يمكننا ذكر أهم المخاطر الممكنة لاستخدامات التكنولوجيا في الخدمات المالية، التي حذرت منها الأنظمة المصرفية والمنظمات المالية الدولية، والعديد من الهيئات التي سعت لتجنب مخاطرها وامن الانترنت، وهي كما يلي:

– **مخاطر أمن معلومات المستخدم:** تعتمد الخدمات المالية التي تقدمها منصات الفنيتك بشكل كبير على التكنولوجيا الرقمية، اذ تؤثر سرية وموثوقية وأمن التكنولوجيا الرقمية بشكل مباشر على جودة الخدمات المالية وأمن المستخدمين، ويتم من خلال ظاهرة الاحتيال المالي وتسريب معلومات العملاء. بإلحاق ضرر لا يمكن إصلاحه لمعلومات المستخدم وممتلكاته وكذلك يؤثر أيضًا على استقرار السوق المالية بأكملها (Bank NEGARA MALAYSIA, 2020).

– **خطر الطرف الثالث:** هو الخطر الناشئ عن تفويض البنك لطرف ثالث يتمثل في شركات التكنولوجيا المالية لتقديم خدمات ومعاملات باستخدام بيانات البنك، نيابة عنه للعملاء(Milena , 2020, p. 52).

– **مخاطر زيادة ائتمان الفينتك:** هو الخطر الناتج عن تقديم الائتمان او الإقراض و الاقتراض باستخدام منصات الفينتك مثل الإقراض من نظير إلى نظير P2Pاو منصات التمويل الجماعي مما يسبب ضعف في معايير الإقراض، كما يمكن أن تؤدي إلى حدوث مخاطر نظامية،

– **خطر المساس بالاستقرار المالي**: من خلال خطر عدم توافق الأنظمة المستخدمة للتكنولوجيا عبر الحدود مثلا عدم السماح للشركات حماية البيانات بالعمل في بلد الطرف الثالث وهذا لعدم إخضاع الشركات نفسها للوائح ذلك البلد(Milena , 2020, p. 55).

– **مخاطر افتقار المستعملين للمعرفة الكافية** بتعاملات الفينتك مما يؤثر على قدرات تحديد المخاطر والوقاية منها، ومخاطر ضعف الرقابة المالية على استخدامات ومنتجات التكنولوجيا المالية، و مخاطر ضعف موظفو الخدمات المالية، لان الافتقار إلى المعرفة يعوق الاستخدام لتعزيز التنمية واتساع نطاق التعاملات المالية الحديثة(Bank NEGARA MALAYSIA, 2020).

– **مخاطر الاحتكار وقتل المنافسة**: اذ بمجرد إنشاء نظام بيئي مقيد، لن يكون لدى المنافسين المحتملين مجال كبير لبناء منصات منافسة يمكن للمنصات المهيمنة أن تعزز موقعها من خلال رفع حواجز الدخول، يمكنهم استغلال قوتهم في السوق والشبكات الخارجية لزيادة تكاليف تغيير المستخدم أو استبعاد المنافسين المحتملين(RSA security LLC, 2020).

كما أن زيادة الإنفاق على إجراءات الأمن والحماية قد يؤثر على أداء المؤسسات المالية من خلال استغلال الفرص الاستثمارية المتاحة(Deloitte, 2018)، وعليه يجب على المؤسسات المالية الموازنة بين استراتيجياتها لاستخدامات التكنولوجيا المالية وإدارة مخاطرها مع محيطها الاستثماري.

– **مخاطر أنظمة التشغيل ومنصات التكنولوجيا المستخدمة لقنوات الدفع الرقمية** على غرار محطة الخدمة الذاتية SST، والخدمات المصرفية عبر الانترنت وتطبيقات أجهزة الجوال...(Bank NEGARA MALAYSIA, 2020) هذا بسبب الاعتماد الكبير على التكنولوجيا المالية في البنى التحتية للسوق المالية والمصارف، والعلاقة المتبادلة في تعاملاتها مع أطراف متعددة محليا ودوليا، هو ما يزيد من تعقيد تعرض القطاع إلى الهجوم او الخطر الالكتروني.

– **خطر منصات القرض من نظير الى نظير**: يكمن في قلة المعلومات عن المقترضين وكذلك عدم تحمل المستثمرون لمخاطر الائتمان وبالتالي عدم دقة نظام تسجيل الدرجات بمقترضي P2Pحول التخلف عن السداد، وكذا عدم القدرة لنفس النظام على قياس المخاطر النظامية الناشئة عن آليات العدوى بين المقترضين لترابط الشبكات على لصعيد العالمي(Paolo, 2018).

– **الخطر السيبراني**: الذي يعبر عن احتمال حدوث الخسائر التي قد تنتج عن مخاطر الانترنت المتعلقة بالمؤسسة المالية كفقدان البيانات او الخسارة المالية او الاضطراب والإضرار بسمعة المنظمة بسبب فشل أنظمة التكنولوجيا، من بين هذه المخاطر الأكثر شيوعا هجمات القرصنة، خرق البيانات، نقل الفيروسات، الابتزاز السيبراني، تعطيل الشبكة، وكذا الأخطاء البشرية كالموظفين (Martin & Jan Hendrik , 2016).

ومن اهم المخاطر السيبرانية نذكر ما يلي:

- **خطر حجب الخدمة الموزعةDDoS (DistributedDenial of Service)**: عبارة عن هجوم يغمر الموارد أو النطاق الترددي لنظام ما بحركة مرور غير مرغوبة (ارسال بيانات من المخترق غير ضرورية لتأثير على اداء النظام) ويمنع الاستخدام المصرح به لهذا النظام(Zarka , Moin , & Karuna , 2016)، من امثلة هذا الهجوم ما حدث في سبتمبر 2012 بالولايات المتحدة الامريكية اين تم استهداف موقع Bank of America و PNC و JPMorgan و US Bancorp و Wells Fargo وبعد شهر واحد مواقع BBTوCapital OneوHSBCو Region Financial ، كما تم تعطيل SunTrust وفي جمهورية التشيك بتاريخ 6 مارس 2013، وتعطلت المواقع الإلكترونية للبنك المركزي وثلاثة بنوك كبيرة والبورصة، مع أضرار محدودة تقدر بنحو نصف مليون دولار. أما في النرويج، فتعرضت سبع مؤسسات مالية كبرى للهجوم في 8 يوليو 2014، مما أدى إلى تعطيل الخدمات خلال النهار. وكذلك فنلندا في نهاية عام 2014، عانت ثلاثة بنوك (Op Pohjolaو Danske BankوNordea) من هجمات DDoS التي جعلت خدماتها عبر الإنترنت غير متاحة، كما منع أحد البنوك العملاء من سحب النقود وإجراء مدفوعات البطاقات(Antoine , 2018, p. 15).

– **خطر التهديد المستمر المتقدم (Advanced Persistent Threat)APT**هجوم الكتروني يبقى صاحبه غير مرئي يهدف الى الترصد ومراقبة نشاط الشبكة والبيانات دون السعي إلي إتلاف الجهاز او النظام (Zarka , Moin , & Karuna , 2016).

– **خطر التصيدPhishing**:باستخدام رسائل البريد الالكتروني والتظاهر كهيئة رسمية ولكنها مزيفة من اجل الحصول على بيانات المستخدم من خلال توجيهه الى المواقع الاحتيالية(Zarka , Moin , & Karuna , 2016).

– **خطر بريد مؤذيSPAM:** إرسال بريد الكتروني غير مطلوب كالإعلان عن منتجات وخدمات مواقع الكترونية، وكذلك تسليم البرامج الضارة والتهديدات السيبرانية الأخرى(NURUL AFSER , 2019).

– **خطر البرامج الضارة**:كالفيروسات والديدان وأحصنة طروادة وبرامج التجسس المصممة لإتلاف أجهزة الكمبيوتر والبرامج والتطبيقات.

– **خطر الروبوتBotnet:** يستخدم لتوزيع البرامج الضارة والرسائل غير المرغوب فيها والخداع، تسمح للمتسلل بالتحكم في النظام.

– **خطر الخداع**: يعني التقليد او النسخ والتزوير كأنواع كثيرة من الانتحال .

– **التهديدات من الداخل**: كالموظفين او العملاء الذين لديهم إمكانية الوصول إلى المعلومات الداخلية(NURUL AFSER , 2019).

إن الهدف من وراء المخاطر السيبرانية له مبرراته بطبيعة الحال، فإما ان يكون الهجوم بدافع الحصول على الأموال عن طريق التحويل او الدفع كفدية، او من اجل الوصول الى معلومات النظام وتحصيل المعلومات السرية الخاص بالمنشاة، كما يمكن ان يكون لأغراض خروقات سياسية لأجل الجوسسة والتنصت، وبالتالي للخطر السيبراني عدة توجهات مالية واقتصادية وأمنية، وإستراتيجية.

كما أن لهذا النوع من المخاطر سواء ما تعلق بالمخاطر السيبرانية او مخاطر التكنولوجيا المالية عامة اثر كبير على المبادئ الأساسية الثلاثة لتكنولوجيا المعلومات وهي السرية والنزاهة والتوافر، كما لها تأثير على سمعة العلامة التجارية- يمكن للعملاء ان يفقدوا الثقة في مصرفهم او مؤسستهم المالية، والخسائر المالية وخسائر البيانات الهامة، وعليه يجب مراعاة جميع المسائل المتعلقة بإدارة التهديد او الخطر من خلال تتبعه واسترداد البيانات وغيرها من الاجراءات التي سنتعرض لها لاحقا.

3.2. الأهمية النسبية للمخاطر المؤثرة على الأداء المالي والمصرفي :

في استبيان قامت به مؤسسة الودائع والمقاصة DTCCحول أكثر المخاطر التي تتعرض لها البنوك والمؤسسات المالية، خلال الفترة 2014-2021 خاصة بعد توسع استخدام تقنيات وتطبيقات التكنولوجيا المالية، والتي قدمت للاختصاصين والقائمين على النشاط المالي اذ كانت نتائج الفئة التي استجابة للاستبيان كما هو موضح في الجدول الموالي:

الجدول رقم (01): المخاطر الأكثر تأثيرا على النشاط المالي والمصرفي وفقا لاستبيان DTCC خلال الفترة2014-2021.

(كنسبة مئوية من إجمالي المخاطر%)

المخاطر	2014	2015	2016	2017	2018	2019	2020	2021
الأمراض المعدية والأوبئة	...	...	...	...	...	...	...	67
المخاطر السيبرانية	84	70	56	71	78	69	63	54
المخاطر الجيوسياسية	64	50	38	52	69	55	59	45
تباطؤ النمو الاقتصادي الأمريكي	31	28	22	27	18	22	44	31
تأثير خروج بريطانيا من الاتحاد الأوربي	...	...	33	34	38	49	43	23
اضطرابات الأسواق المالية	62	25	24	32	25	18	22	16
تأثير اللوائح الجديدة	64	41	35	40	45	26	17	16
تباطؤ النمو الاقتصادي الأوربي	27	17	18	19	7	17	17	14
تباطؤ الاقتصاد الآسيوي	...	...	24	16	17	26	30	12
مخاطر السيولة	26	30	23	25	18	16	21	10
الامتثال والحوكمة	19	16	16	21	18	14	13	4

... : عدم توفر البيانات

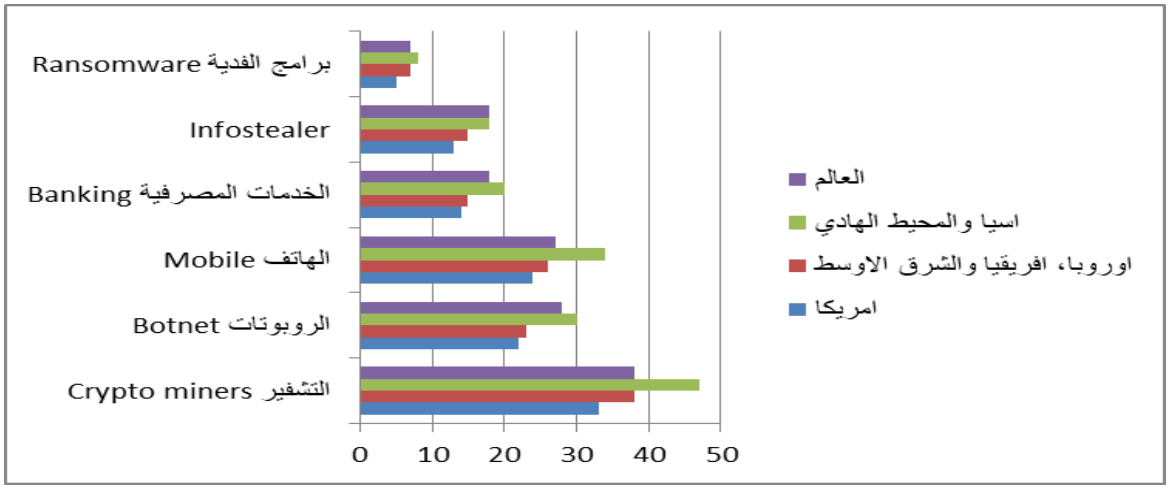
المصدر: من إعدادالباحثين بالاعتماد على نتائج استبيان مؤسسة الودائع والمقاصةDTCC للفترة 2014-2021 (SYSTEMIC RISK BAROMETER , 2021).

نلاحظ من خلال نتائج الاستبيان المبينة في الجدول رقم (01) أعلاه انه خلال السنوات الثمانية كان الإجماع على أن أكثر المخاطر اثرا على القطاع المالي والمصرفي هي مخاطر الأمن السيبراني، ويفسر ذلك بأنه خلال هذه الفترة عرفت المؤسسات المالية والمصرفية توسعا كبيرا في استخدام تقنيات وتطبيقات التكنولوجيا المالية في معاملاتها، مما زاد من احتمالية تعرضها لتلك المخاطر النظامية التشغيلية المتعلق بالاختراق والاحتيال عبر الانترنت، ويعود الأمر الثاني الى ظهور الشركات المتطورة والناشئة في مجال استخدام التكنولوجيا المالية وممارسة بعض الأنشطة التي كانت حكرا على البنوك والمؤسسات المالية، مما زاد من احتمالية تعرضها لتلك المخاطر.

كما نلاحظ أن النسبة تتراوح ما بين 54 % - 84 % خلال الفترة 2014 -2021 من الأشخاص الذين قدموا إجاباتهم كانت تعتبر مخاطر الأمن السيبراني الأكثر تهديدا للنشاط المالي والمصرفي على طول الفترة المذكورة سابقا، لتليها نسبة تتراوح ما بين 38% و 69% كانت إجابتهم حول مخاطر جيوسياسية، وفي المرتبة الثالثة تأتي المخاطر المتعلقة بتباطؤ النمو الاقتصادي بأوروبا وأمريكا بنسبة ما بين 18 % و44% ، فتحول هاجس القطاع المالي والمصرفي من مخاطر السيولة والائتمان وغيرها من المخاطر التقليدية إلى هاجس أكثر خطورة منه وهو مخاطر التكنولوجية الحديثة باعتبارها شكل جديد من أشكال المخاطر التشغيلية.

الشكل (1): توزيع فئات الهجوم السيبراني على مناطق العالم خلال العام 2019 .

(كنسبة مئوية من إجمالي الهجمات)



المصدر: من إعداد الباحثين بالاعتماد على معطيات تقرير الأمنالسيبراني CYBER SECURITY REPORT 2020).
(https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf, 2020،

ويبرز الشكل (1) أعلاه أن فئة الهجوم السيبراني المتعلقة بالتشفير من أكثر الفئات انتشارا عبر العالم، والتي تتركز بالدرجة الأولى في آسيا والمحيط الهادي، وهي منطقة تتركز فيها جميع الفئات المذكورة في الشكل، باعتبارها أكثر المناطق انفتاحا على التقنية الرقمية والتكنولوجيا المالية، ثم امريكا بدرجة اقل، لتليها دول اوروبا وافريقيا والشرق الأوسط مجتمعة.

الجدول رقم (02): البرامج الضارة المستخدمة في الهجمات السيبرانية

(كنسبة المئوية لشبكات الشركات المتأثرة بكل مجموعة من مجموعات البرامج الضارة%)

البرامج الضارة	أمريكا	أوروبا، إفريقيا والشرق الأوسط	أسيا والمحيط الهادي	العالم
EMOTET	16	21	17	18
JSECOIN	14	16	14	15
XMRIG	11	13	22	14
CRYPTOLOOT	12	14	14	14
COINHIVE	11	12	13	12
TRICKBOT	12	10	14	11
LOKIBOT	5	12	13	10

AGENT TESLA	6	11	13	10
HAW KEYE	…	10	11	8
FORMBOOK	7	…	…	7
GANDCRAB	6	8	…	…
RAMNIT	…	…	14	…

… : عدم توفر البيانات

المصدر: من إعداد الباحثين بالاعتماد على معطيات تقرير الأمن السيبراني CYBER SECURITY REPORT 2020)
https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf, 2020)

من خلال الجدول رقم (02) والشكل (1) اعلاه، يظهر لنا توزيع الهجمات السيبرانية وكذا الأنواع المخلفة لتلك البرامج المستخدمة في الهجوم، اذ تعرف منطقة اسيا والمحيط الهادي نسبة كبيرة للهجمات وتليها منطقة الشرق الأوسط وشمال افريقيا في البرامج الضارة ومن ثم امريكا، وهذا يعود لتركز الكبير لاستخدامات تقنيات التكنولوجيا المالية الحديثة في دول اسيا المتطورة تكنولوجيا، وكثافة الاستخدام للأنترنت هناك، اما منطقة الشرق الاوسط وشمال افريقيا فهي مبتدئة في معاملات الانترنت مما يجعلها عرضة للهجمات لقلة الإجراءات الاحترازية وضعف القدرة على التحكم فيها، وامريكا الاقل ضررا نظرا لتوسع الاستخدام لهذه التكنولوجيا واكتساب خبرة في مجال ادارة امن المعلومات والتقنيات مع تشديد إجراءات الوقاية وحوكمة الاستخدام لمختلف أنواع تقنيات ومعاملات التكنولوجيا المالية.

3. تدابير وإجراءات إدارة مخاطر التكنولوجيا المالية في البنوك والمؤسسات المالية:

يتعين على البنوك والمؤسسات المالية المنفتحة في تعاملاتها على التكنولوجيا المالية لمنتجاتها وخدماتها أن تمتثل للمتطلبات إدارة المخاطر مع العمل على تحديد تلك المخاطر بدقة وباستمرار نظرا لتنوعها وتعددها بالإضافة لحجم تعاملات تلك المؤسسات وتعقيد عملياتها.

فيمكن اعتبار إدارة مخاطر التكنولوجيا المالية هي تلك الإجراءات والتدابير المنظمة لاستخدام تقنيات التكنولوجيا المالية، والتي تهدف للحد من الاختراقات والتجاوزات التي تمس بموثوقيتها من خلال حماية بيانات ومعاملات العملاء والمنشئات المختلفة المستثمرة في المجال والمستخدمة له.

1.3. اجراءات وتدابير ادارة مخاطر التكنولوجيا المالية وفقا لتوصيات بنك نيقارا بماليزيا وإدارة الخدمات المالية في نيويورك (NYDFS) ومجموعة البنك الدولي:

من أهم الإجراءات الواجب اتخاذها من طرف مجالس الإدارة ومسؤولياتهم، وكذا الإدارة العليا، والقائمين على ادارة المخاطر في البنوك والمؤسسات المالية تجاه مخاطر التكنولوجيا المالية وفقا لتوجيهات وتوصيات جهات دولية مختصة في المجال المالي والمصرفي مختلفة نذكر ما يلي:

- وضع مؤشرات الأداء الرئيسية وكذا مؤشرات التنبؤ بالمخاطر منها مخاطر التكنولوجيا المالية للمنشاة مع التحديثات الدورية لها تسهيلا لاتخاذ القرارات الإستراتيجية اللازمة، توفر مثلا منصة LogRhythm (عبارة عن منصة لشركة رائدة تعمل على مساعدة وتمكين المؤسسات في العالم لتقليل المخاطر عن طريق الكشف السريع لتهديدات الالكترونية الضارة والاستجابة لها وتحديدها) إدارة كاملة لدورة حياة التهديد، من خلال النظام المركزي للإنذار والتبليغ في الانتهاكات الأمنية، وعبارة عن محرك ذكاء اصطناعي (Smart Response)، اذ تساعد هذه الإجراءات المؤسسات المالية للاستجابة لحوادث الأمن السيبراني، وكذا تقليل متوسط الكشف MTTD ومتوسط الاستجابة MTTR(Logrhythm the security intelligence company, 2018).

- الإشراف على الخطط الإستراتيجية للتكنولوجيا المعلومات والأمن السيبراني للمؤسسات المالية مع المراجعة الدورية لها، من خلال وضع متطلبات البنى التحتية والموارد اللازمة وتدابير الرقابة للحد من المخاطر، ثم الإشراف على التنفيذ الفعال لإطار إدارة مخاطر التكنولوجيا المالية مع وجود أعضاء من ذوي الخبرة والكفاءة في مجال استخدامات التقنية الحديثة، ناهيك عن دراسة ومناقشة المخاطر السيبرانية والإستراتيجية ومخاطر السمعة المتعلقة بحادث الكتروني(World Bank Group, 2018)، وكذا إقامة لجان تدقيق داخلي مسؤولة عن ضمان وظيفة تدقيق التكنولوجيا الداخلية بضمان الكفاءة الكافية لموظفي المراجعة(Logrhythm the security intelligence company, 2018).

– ضرورة إنشاء لجنة متعددة الوظائف لتقديم التوجيه بشأن الخطط والاستخدامات التكنولوجية للمؤسسة المالية، وتقديم تحديثات في الوقت المناسب مع الموافقة على أي انحراف عن السياسات المتعلقة بالتكنولوجيا بعد تقييم للمخاطر ذات الصلة(Deloitte, 2018)وضرورة الإبلاغ، مع ضمان التخصيص الكافي للموارد للحفاظ على أنظمة التكنولوجيا القوية والموظفين ذوي المهارات والكفاءة المناسبة لدعم الإدارة الفعالة لمخاطر التكنولوجيا(Bank NEGARA MALAYSIA, 2020).

– يجب على المؤسسة المالية إنشاء وظيفة مستقلة لإدارة مخاطر التكنولوجيا على مستوى المؤسسة بتشكيل خلايا لأمن المعلومات وتعيين رئيس لأمن المعلومات CISO، ومنحها السلطة الكافية والموارد، والاستقلال عن العمليات التكنولوجية اليومية مع البقاء على اطلاع بالمخاطر التكنولوجية الحالية والناشئة من خلال وضع سياسة مكتوبة للأمن السيبراني ومحفوظة تتضمن امن المعلومات، حوكمة البيانات، عمليات الأنظمة واستمرارها (Logrhythm the security intelligence company, 2018).

– إدارة العمليات التكنولوجية عن طريق تحديد وتقييم ومعالجة المخاطر التي تهدد التنفيذ الناجح للمشروع او تؤدي الى فشله، ومراقبة تعقيدات الأنظمة كاستخدام التكنولوجيا غير المثبتة او غير المألوفة او مخاطر دمج تكنولوجيا جديدة في أنظمة حالية، وعمليات ترحيل البيانات...، الحفاظ على ضوابط أمنية كافية طوال حياة المشروع لتجنب مخاطر الأمن السيبراني، والحد من مخاطر أخطاء النظام غير المكتشفة وأخطاء الوظائف ومشكلات استقرار النظام الطويلة عن طريق اخذ إستراتيجية متينة ومرنة(Bank NEGARA MALAYSIA, 2020).

– التزام الهيئات المعنية بتلقي ومراجعة التقارير في الوقت المناسب حول إدارة هذه المخاطر باستمرار وطول مدة تنفيذ المشاريع، وتطوير النظام واكتسابه، مع ضرورة إجراء التقييمات الدورية لمخاطر أنظمة المعلومات (Logrhythm the security intelligence company, 2018).

– إتخاذ سياسات وممارسات واضحة لإدارة المخاطر خلال مرحلة تطوير الأنظمة، مع التنوع في التكنولوجيا لتعزيز المرونة وهذا بضمان عدم تعرض البنية التحية للأنظمة بشكل مفرط لمخاطر التكنولوجيا.

– مراقبة الأنظمة الحرجة والمطورة او التي تم صيانتها مع ضمان استمرارية سهولة الوصول الى التعليمات البرمجية المصدرة وتأمينها، عن طريق فصل بيئة الانتاج عن بيئة التطوير والاختبار للأنظمة الحيوية(Logrhythm the security intelligence company, 2018).

– التأكد من الالتزامات الخاصة بمقدمي الخدمة من الطرف الثالث وهذا بتقديم إشعار للمؤسسة قبل إجراء أي تغييرات قد تؤثر على الأنظمة التكنولوجية(Bank NEGARA MALAYSIA, 2020)، واعتماد سياسة تشفير قوية ومرنة لحماية البيانات والمعلومات باعتماد معايير لخوارزميات التشفير، ومصادقة الرسائل، ووظائف التجزئة والتوقيعات الرقمية، ... (Logrhythm the security intelligence company, 2018).

– مرونة مركز البيانات، أي تصميم بنية تحتية مرنة وآمنة وقابلة للتطوير، لا تؤدي في حالة الفشل او الانقطاع المحتمل في مركز البيانات الى تدهور كبير في تقديم الخدمات وإعاقة العمليات الداخلية بوضع إجراءات تحكم مناسبة لعمليات مركز البيانات الخاص بها.

– مرونة الشبكة لا بد من تصميم شبكة موثوقة وقابلة للتوسيع وآمنة وقادرة على دعم أنشطتها التجارية بما في ذلك خطط النمو المستقبلية، وتنفيذ إجراءات وقائية مناسبة لتقليل مخاطر اختراق النظام في كيان واحد يؤثر على الكيانات الأخرى داخل المجموعة.

– إدارة مقدم خدمة الطرف الثالث عن طريق الانتقاء المناسبة لكفاءة مقدم خدمة الطرف الثالث، وإجراء تقييم لقدرات هذا الطرف في إدارة مخاطر مثل تسرب البيانات والكشف غير المسرح به عن معلومات العميل والطرف المقابل، انقطاع الخدمة، معالجة الأخطاء، التهديدات السيبرانية، الاعتماد المفرط على الموظفين الرئيسين، سوء التعامل مع المعلومات السرية أثناء نقل او معالجة او تخزين المعلومات، مخاطر التركيز(World Bank Group, 2018).

– خدمات سحابية والتي يتجسد خطرها في تعقيد نموذج النشر، ومخاطر ترحيل النظم الحالية الى البنية التحية السحابية، ومخاطر موقع البنية التحتية السحابية، إضافة الاختلاط المتعدد او دمج البيانات، أيضا الهجمات السيبرانية عبر مزودي الخدمات السحابية، ولهذا لا بد من تحديد الأنظمة الحرجة وغير الحرجة قبل استخدام اي خدمات سحابية.

– صلاحية التحكم او الدخول وضع ضوابط وصول مناسبة لتحديد هوية مستخدمين ومصادقتهم و تفويضهم لتجنب خطر الوصول او الدخول غير المصرح به الى الأنظمة مع استخدام عمليات توثيق قوية لضمان هويات المستخدمين، مما يمتلكه مثل البطاقة الذكية، ومما هو مستخدم مثل الخصائص البيومترية كالبصمة او نمط الشبكية... (Logrhythm the security intelligence company, 2018)

– امن الخدمات الرقمية لمجابهة مخاطر الاحتيال في المعاملات، والتصيد الاحتيالي، من خلال ضمان الاحتفاظ بسجلات خدمة رقمية كافية وذات صلة لأغراض التحقيقات، مع إجراء تقييم شامل لمخاطر التقنيات المتقدمة والتأكد من صحتها بالانتظام (Bank NEGARA MALAYSIA, 2020).

2.3. ادارة مخاطر التكنولوجيا المالية وفقا لتوصيات مجلس الاستقرار المالي:

عرض مجلس الاستقرار المالي عشرة قضايا للإدارة مخاطر التكنولوجيا المالية (Financial Stability Board, 2020):

- إدارة المخاطر التشغيلية من جانب مقدمي الخدمات من الأطراف الثالثة.
- التخفيف من مخاطر الانترنت.
- رصد المخاطر المالية الكلية.
- المسائل القانونية عبر الحدود والترتيبات التنظيمية
- كشف اطر وتحليلات البيانات الكبيرة
- تقييم المحيط التنظيمي وتحديثه في الوقت المناسب.
- التعلم المشترك مع مجموعة متنوعة من أطراف القطاع الخاص.
- تطوير خطوط مفتوحة للاتصالات عبر السلطات المختصة.
- بناء قدرات الموظفين في مجالات جديدة من الخبرات المطلوبة.
- دراسة مكونات بديلة للعملات الرقمية.

3.3. إدارة المخاطر السيبرانية في القطاع المالي والمصرفي لهيئات دولية متخصصة:

بما أن الخطر السيبراني يعتبر من أهم وأكثر المخاطر المرتبطة بتقنيات التكنولوجيا المالية المرتبطة بالأنترانت والتطبيقات المختلفة، تولي له العديد من الهيئات والمنظمات المالية والمصرفية الدولية وحتى الامنية اهمية كبيرة، وتضعه ضمن الاستراتيجيات الامنية الواجبة متابعتها ومراقبتها، ولذلك يطلق عليها بالأمن السيبراني والذي يعرّفه المعهد الوطني للمعايير والتقنية الأمريكيNIST على انه النشاط او العملية التي يتم بموجبها حماية نظم المعلومات والاتصالات والدفاع عنها ضد الضرر او الاستخدام او التعديل غير المصرح به او الاستغلال(حلف شمال الاطلسي NATO، 2016)، والذي تتجلى وظيفته فيما يلي:

– تامين جميع جوانب التحول الرقمي والبيانات والقدرة على المقاومة، من خلال سرية المعلومات الحساسة، وسلامة المعالجة، وتوافر الأنظمة ومخازن البيانات والشبكات الضرورية لتوفير خدمة مستمرة(Jayant & Rachel , 2019).

– إدارة مخاطر الانترنت من خلال تطوير نموذج الإبلاغ الموحد الذي يوضح حوكمة المؤسسة لإدارة المخاطر.

– إجراء اختبارات الاختراق دوريا بناء على سيناريوهات الهجوم السيبراني مع إشراك مختبري الاختراق المعتمدين (Logrhythm the security intelligence company, 2018).

من عوائق إقامة امن سيبراني قيود الميزانيات، نقص المهنين والخبراء، والتهديدات الداخلية، وعلى هذا الأساس وجدة بعض الشركات والمؤسسات المختصة في المجال واوصت بضرورة:

– ضمان مفاتيح، وجرد البيانات الشخصية والحساسة، الاحتكاك بالمنظمات الاخرى لفهم طرق تعاملها في مواجهة الجرائم الالكترونية.

– دراسة معهد SANA مختص في امن المعلومات عام 2015 ذكر خمس مراحل أساسية لحماية المنظمة من الهجمات وهي : عناصر التحكم في الشبكة، مكافحة الفيروسات، السمعة والتحليل السلوكي، الكشف والمعالجة.

وقدّم مجلس الاستقرار المالي ايضا حزمة من التوصيات عن بناء وظيفة امن سيبراني فعالة لدى المؤسسات والشركات الكبرى على غرار المؤسسات المالية والبنوك نذكر(Financial Stability Board, 2020):

– ممارسة الأمن السيبراني الفعال من خلال تحديد وظيفة خلية الأمن السيبراني في تلك المؤسسات وتحديد وظائفها وما يجب حمايته لاختلاف طبيعة العمليات والوظائف للمؤسسات المالية والشركات.

– التنظيم والإشراف الفعالان عن طريق الالتزام بالامتثال والتنسيق بين المؤسسات والشركات العاملة في مجال التكنولوجيا المالية.

– بناء القدرات والتوظيف الأمثل مع التدريب للموظفين مع استمرار عمليات الفحص والمراقبة في المؤسسات المالية والبنوك..

اما المعهد الوطني الأمريكي لمعايير التكنولوجية (NIST) أنشأ إطار أكثر إتباعا لتصنيف عالي المستوى لنتائج الأمن السيبراني ومنهجية لتقييم تلك النتائج وإدارتها، يحدد Cyber Security Framework خمس وظائف اساسية وهي: تحديد، كشف، حماية، استجابة واسترداد يجب على المؤسسات معالجتها لإدارة مخاطر الأمن السيبراني بشكل استباقي لأعمالهم (Logrhythm the security intelligence company, 2018).

– للحد من خطر رفض خدمة الموزع DDoS يجب وضع إستراتيجية واضحة لمنع فقدان البيانات وعملياتها لضمان تحديد معلومات الملكية والعملاء والأطراف المقابلة وتصنيفها وتأمينها(Bank NEGARA MALAYSIA, 2020).

– لا بد من ان يتميز مركز العمليات الأمنية بالقدرة على الرصد الاستباقي لوضع امن التكنولوجيا الخاص بها، والاشتراك في خدمات استخبارات التهديدات لتحديد التهديدات السيبرانية الناشئة.

– الاستجابة والاسترداد السيبراني من خلال وضع سياسات واستراتيجيات شاملة لإدارة الأزمات السيبرانية بالاعتماد على وضع خطط اتصال واضحة لإشراك المساهمين والهيئات التنظيمية والعملاء والموظفين في حالة وقوع حادثة الكترونية (Bank NEGARA MALAYSIA, 2020).

– التدقيق التكنولوجي: يجب ان تمتلك المؤسسة موظفي مراجعة داخلية لتكنولوجيا مؤهلين مهنيا ولهم القدرة الكافية ودراية بالتطور للأنظمة التكنولوجيا مع إنشاء وظيفة مخصصة للتدقيق الداخلي للتكنولوجيا.

– الوعى الداخلي والتدريب حول أهمية الأمن السيبراني مع توفير التدريب الكافي والمستمر للموظفين المشاركين في العمليات التكنولوجيا وإدارة المخاطر(Financial Stability Board, 2020).

وقدّمت كذلك مجموعة من المعايير الدولية المنظمة للمخاطر السيبرانية نذكر منها:

– الحوكمة الالكترونية (Cyber –governance) من خلال وضع استراتيجية للأمن السيبراني في المؤسسات المالية الخاصة بها تتوافق مبادئ وممارسات ادارة المخاطر، كما تقوم الجهات الرقابية بمراجعتها وتقييمها.

– فهم إدارة المخاطر واختبارها وطرق التغلب عليها (Approaches to risk management ; testing and incident response and recovery) يتمحور حول أربعة نقاط أساسية ممثلة في الرقابة على الأمنالسيبراني (cyber-resilience) ، ضوابط امن المعلومات وطرق اختبارها وضمان استقلاليتها، مدى الاستجابة للتغلب على الخطر، مقاييس الأمنالسيبراني والمرونة.

– التواصل وتبادل المعلومات(Communication and sharing of information) من خلال مشاركة المعلومات مع العاملين في القطاع وكذا مع الأجهزةالأمنية .

– إسناد امن المعلومات والأنظمة الالكترونية الى جهات ثالثة (Interconnection Withthird parties) من اجل توسيع الرؤية الشاملة لتلك الضوابط المعمول بها ومستوى المخاطر من خلال الاستعانة بمصادر خارجية كخدمات الحوسبة السحابية cloud computing services والاتصالات السلكية واللاسلكية(محمد ، 2019)

كما كان لصندوق النقد العربي جملة من الاقتراحات او الاجراءات الواجب الالتزام بها لحد من مخاطر الأمن السيبراني المهدد الأول للاستقرار المالي من خلال(محمد ، 2019):

– وضع لائحة من التعليمات لتأمين التطبيقات الالكترونية كتثبيت البرامج المضادة للاختراق.

– الزام المصارف بإجراء اختبارات الضغط (Stress Testing) لتحديد الآثار الممكنة في حالة حدوث قرصنة للأنظمة الالكترونية.

– تعزيز امكانات الرقابة والإشراف على مخاطر الأمن السيبراني وبناء العنصر البشري المتخصص فيها.

خاتمة:

تعرضت العديد من الدراسات والأبحاث الى موضوع التكنولوجيا المالية في القطاع المالي والمصرفي، أين أظهرت العديد منها مدى القفزة النوعية التي عرفها القطاع المالي، من خلال توسع الابتكار والرفع من مستوى المنافسة العالمية بين البنوك والمؤسسات المالية وكذا الشركات العملاقة في التكنولوجيا المالية والشركات الناشئة، بحيث أصبح هناك ترابط وتداخل بين العمليات وكذا بين العملاء، اذ يمكن الاستثمار عن بعد فقط من خلال فتح حساب على الشبكة او الولوج الى المنصات المختلفة، ونفس الأمر بالنسبة لإجراء المعاملات المالية والمصرفية المختلفة.

إن كل ما ذكرناه في مقالنا عن أهمية التكنولوجيا المالية وتقنياتها المتعددة يحفز القطاع المالي والمصرفي من جهة، ويضعه أمام تحدي اكبر من جهة اخرى وهو تحدي امن التقنية وتجنب المخاطر المحيطة بها، مما يثبت العلاقة والأثر الكبيرين بين التوسع في استخدامات التكنولوجيا المالية والمخاطر التي يمكن أن تسببها للقطاع المالي والمصرفي، وتوصلنا إلى مجموعة من النتائج لهذه الدراسة نذكرها فيما يلي:

نتائج الدراسة:

- تمثل التكنولوجيا المالية ذلك المزيج بين التقنيات والتطبيقات التكنولوجية الحديثة، والعمليات المالية والمصرفية، للحصول على منتجات وخدمات مالية جديدة تتميز بالحداثة والابتكار والجودة وكذا سهولة الوصول والاستخدام من كل مكان وفي أي وقت.

- تعبر مخاطر التكنولوجيا المالية عن كل احتمال للخسارة او اختراق او تأثير تتعرض لها الأنظمة والتطبيقات والتقنيات التكنولوجية الحديثة المعتمدة في تقديم المنتجات والخدمات المالية مما يكون له الأثر السلبي على الأداء المالي للبنوك والمؤسسات المالية بما يتعارض واهدفها المسطرة، وعليه يمكن اعتبارها ضمن المخاطر التشغيلية لكنها تختلف الى حد ما عن المخاطر التشغيلية التقليدية التي تعترض العمل المصرفي والمالي ومن أهمها الخطر السيبراني او خطر الانترنت.

- تتضمن التكنولوجيا المالية مجموعة معتبرة من التقنيات والمنصات التي تستخدم في تقديم المنتجات والخدمات المالية والمصرفية على غرار تقنية البلوك شين، تقنية التمويل الجماعي، وتقنية التمويل النظير للنظيرp2p، وهي جميعها تقنيات تعتمد على الانترنت والأجهزة الحاسوبية مما يجعلها عرضة للاختراق والقرصنة ما لم يتم حمايتها بشكل دائم ومستمر.

- حذرت أغلب بلدان العالم المستخدمة للتكنولوجيا المالية والهيئات الدولية المشرفة على القطاع المالي والمصرفي من مخاطر متشابهة تتعلق بالتكنولوجيا المالية سواء في امريكا او اسيا او اوروبا، مما يفرض ضرورة بناء تكتل او تحالف دولي مختص في مجال امن التقنية المالية الحديثة، وإدارة مخاطرها.

- لقيت إدارة مخاطر التكنولوجيا المالية اهتماما واسعا من العديد من الهيئات والمنظمات العالمية والسلطات المركزية على غرار مجلس الاستقرار المالي، البنك المركزي الماليزي، البنك الدولي وإدارة الخدمات المالية في نيويورك (NYDFS)، لأهميتها الكبيرة في الحد من الانزلاقات والخرقات التي قد تعصف بالقطاع ككل نتيجة الانفتاح الكبير على التقنية في المحال المالي والمصرفي، وهو الأكثر حساسية وعرضة للمخاطر .

توصيات الدراسة:

بناء على نتائج الدراسة التي توصلنا إليها، يمكن طرح مجموعة من التوصيات التي تخدم موضوع الدراسة لاحقا نذكرها فيما يلي:

- إن قلة الإفصاح ونشر المعلومات المتعلقة بحجم الخسائر المتعلقة باستخدام التكنولوجيا المالية في القطاع المصرفي، وعدد الهجومات السيبرانية والاختراقات الأمنية لتلك التقنيات يعتبر عائق للعمل المشترك بين الهيئات والمنظمات العالمية في مجال إدارة التكنولوجيا المالية ومخاطرها، لذلك لابد من إقامة قاعدة بيانات مشتركة بين الهيئات التنظيمية والامنية الدولية.

- ضرورة إدراج مخاطر التكنولوجيا المالية ضمن توصيات اللجان والمواثيق المالية والمصرفية الدولية، على غرار توصيات لجنة بازل، وميثاق الحوكمة والامتثال المصرفيين.

- صياغة قوانين وتوجيهات إرشادية داخل الأنظمة المصرفية للدول المنفتحة على التكنولوجيا المالية، وتشديد إجراءات الرقابة والتدقيق.

- مراقبة استخدام التكنولوجيا المالية كوسيلة لتبييض الأموال الإرهاب، التجارة غير المشروعة عبر العالم، من خلال تضافر الجهود الدولية وخارج الحدود الإقليمية لكل دولة.

- أصبح لزاما على الأنظمة المصرفية إقامة مخابر ومراكز للبحث في التقنية وأمنها، مع السعي الدائم لإجراء الاختبارات للأنظمة، وتدريب الإطار البشرية في المجال مع مواكبة التطورات الحديثة، وتبادل الخبرات في المجال الأمن السيبراني.

افاق الدراسة:

ان موضوع التكنولوجيا المالية واستخداماتها المختلفة عن طريق تقنياتها المتعددة، والمخاطر المحيط بها، يبقى موضوعا حديثا نسبيا، مما يفتح المجال لتقديم دراسات وابحاث جديدة تتعلق به، فموضوع ادارة مخاطر التكنولوجيا المالية الذي تطرقنا اليه في هذه الدراسة يفتح المجال لأفاق دراسة مستقبلية متعددة، على غرار:

- دراسة قياسية لأثر مخاطر التكنولوجيا المالية على مؤشرات الاداء المالي للمؤسسات المالية والمصرفية.
- دراسة مدى فعالية اجهزة قياس المخاطر المستخدمة في القطاع المالي والمصرفي في الكشف وقياس مخاطر التكنولوجيا المالية.
- دراسة كفاءة مؤشرات التنبؤ بالمخاطر المصرفية في تحديد المخاطر الناتجة عن استخدام التكنولوجيا المالية والحد منها.
- دراسة مدى ترابط الانظمة المالية والمصرفية العالمية نتيجة استخدام التكنولوجيا المالية، والمخاطر المرافق لها.

مراجع باللغة العربية:

1. حلف شمال الاطلسي NATO. (27 09، 2016). تاريخ الاسترداد 25 12، 2020، من الامن السيبراني مرجع عام: www.nato.int/nato static
2. اتحاد المصارف العربية. (2020). تاريخ الاسترداد 18 12، 2020، من اتحاد المصارف العربية: www.uabonline.org
3. اسماعيل محمد . (01، 2019). الامن السيبراني فى القطاع المصرفي موجز سياسات. تأليف الامن السيبراني فى القطاع المصرفي موجز سياسات العدد 04. الامارات العربية المتحدة: صندوق النقد العربي.
4. عبد الكريم قندوز. (2019). التقنيات المالية وتطبيقاتها فى الصناعة المالية الاسلامية. تأليف التقنيات المالية وتطبيقاتها فى الصناعة المالية الاسلامية (صفحة 50). الامارات العربية المتحدة: صندوق النقد العربي.
5. م مغربي، و م.ح ثريا. (2020). ثورة التكنولوجيا المالية. مصر: معهد التخطيط القومي المصري.

مراجع باللغةالأجنبية

1. *Deloitte*. (2018). Retrieved 01 15, 2021, from Deloitte: www2.Deloitte.com.articles
2. *Logrhythm the security intelligence company*. (2018, 03). Retrieved 04 13, 2021, from LOGRHYTHM SUPPORT FOR THE NYDFS CYBERSECURITY REGULATION (23 NYCRR 500): WWW.LOGRHYTHM.COM
3. *World Bank Group*. (2018). Retrieved 03 23, 2021, from Financial Sectore Cyber Security: www.pu bdocs.worldbank.org/en
4. *Bank NEGARA MALAYSIA*. (2020). Retrieved 03 10, 2020, from Bank NEGARA MALAYSIA: www.bnm.gov.my/index.php
5. *CYBER SECURITY REPORT https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf*. (2020). Retrieved 02 20, 2021, from CYBER SECURITY REPORT: https://www.ntsc.org/assets/pdfs/cyber-security-report-2020.pdf
6. *Financial Stability Board*. (2020). Retrieved 12 15, 2020, from fsb : www.fsb.org/work-of-the-fsb/financial-innovation-and-structural-change/fintech
7. *RSA security LLC*. (2020). Retrieved 12 29, 2020, from RSA security LLC: www.rsa.com
8. *SYSTEMIC RISK BAROMETER https://www.dtcc.com/systemic-risk/systemic-risk-barometer-surveys*. (2021). Retrieved 02 22, 2021, from SYSTEMIC RISK BAROMETER: https://www.dtcc.com/systemic-risk/systemic-risk-barometer-surveys
9. AGUSTIN , R. (2017). FINTACH IN A FLASH. In R. AGUSTIN , *FINTECH IN A FLASH - FINANCIAL TECHNOLOGY MADE EASY* (p. 15). LONDON : www.fintechflash.co.uk.

10. Antoine , B. (2018, 06). *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment* . Retrieved 02 25, 2021, from International Monetary Fund: www.imf.org
11. Gregor, D., & Lars , H. (2016). *The FinTech Market in Germany.* Germany: Matthias Schmitt and Martina Weber.
12. Jayant , R., & Rachel , L. (2019). *ARTIFICIAL INTELLIGENCE APPLICATIONS IN FINANCIAL SERVICES-ASSET MANAGEMENT, BANKING AND INSURANCE.* Retrieved 12 17, 2020, from www.oliverwyman.com
13. Keizer , S. (2017). BLOCKCHAIN Novice to Expert. In *BLOCKCHAIN Novice to Expert* (p. 43). 2 manuscripts by Keizer Söze.
14. Martin , E., & Jan Hendrik , W. (2016, 03 16). *University of Gallen.* Retrieved 03 14, 2021, from University of Gallen: www.unisg.ch
15. Milena , V. (2020, 01 28). Fintech and Financial Stability Potential Influence of FinTech on Financial Stability, Risks and Benefits. *Journal of Central Banking Theory and Practice*, p. 54.
16. NURUL AFSER , S. (2019). *A FRAMEWORK FOR THE MOBILIZATION OF CYBER SECURITY AND RISK MITIGATION OF FINANCIAL ORGANIZATIONS IN BANGLADESH: A CASE STUDY.* DHAKA, BANGLADESH : DEPARTMENT OF INDUSTRIAL AND PRODUCTION ENGINEERING (IPE) BANGLADESH UNIVERSITY OF ENGINEERING AND TECHNOLOGY (BUET.
17. Paolo, G. (2018, 11 27). Fintech Risk Management A Researche challenge for artificial intelligence in finance. *SPECIALTY GRAND CHALLENGE* .
18. Vikram , D., David , M., & Max , H. (2017). Blockchain Enabled Applications . In *Blockchain Enabled Applications Understand the Blockchain Ecosystem and How to Make it Work for You* (p. 15). USA: Library of Congress Control Number.
19. Zarka , Z., Moin , U.-d., & Karuna , S. (2016, 06). Challenges in Privacy and Security in Banking Sector and Related Countermeasures. *International Journal of Computer Applications* , p. 32.
20. Zhang, M., & Yang , J. (2018). Research on financial Technology and inclusive finance Development. *6th international education; economics, social science, art, sport and management conference* (p. 67). CHINA: ATLANTIS PRESS.