

أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك

ملخص: هدفت الدراسة إلى التعرف على أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك المدرجة في بورصة فلسطين، وتقديم تشخيص لواقع إدارة مخاطر الأمن السيبراني من أجل دعم تطبيق الشمول المالي لتعزيز الاستقرار المالي لهذه البنوك، وللإجابة على التساؤلات البحثية واختبار فرضيات الدراسة أعتمد الباحثان على المنهج الوصفي التحليلي، واستخدمت الاستبانة كاداه لجمع المعلومات ووزعت بعد تقييمها وتحكيمها من عدد من المتخصصين على عينة الدراسة والتي بلغت (90) مفردة والمكونة من المدراء العاميين، ومدراء الفروع، ومدراء الدوائر المالية، ومدراء إدارات المخاطر في البنوك المدرجة في بورصة فلسطين. وأثبتت نتائج الدراسة أنه يوجد أثر لإدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك المدرجة في بورصة فلسطين، كما تقوم البنوك المدرجة في بورصة فلسطين بالتصدي للمخاطر السيبرانية من خلال توفير بيئة مناسبة للأمن السيبراني بهدف دعم الشمول المالي. كما أوصت الدراسة بضرورة قيام البنوك المدرجة في بورصة فلسطين باتخاذ إجراءات للأمن السيبراني لضمان سلامة ومتانة نظم المعلومات المالية والإدارية والحفاظ على الاستقرار والشمول المالي وبما يحقق أهدافها، كما ضرورة وضع نماذج فعالة لإدارة المخاطر السيبرانية المصاحبة لتكنولوجيا المعلومات وهو ما يتطلب الرقابة المستمرة لتحديد هذه المخاطر التي قد تهدد الاستقرار المالي في القطاع المصرفي.

مقدمة:

تعتبر البنوك هدفاً رئيسياً لمجرمي الإنترنت، سواء من الأفراد أو الجهات الحكومية، ولا يوجد كيان حكومي له مصلحة أكبر في حماية أداء المؤسسات المالية من البنك المركزي في أي الدولة. علاوة على ذلك، عند ممارسة سلطاتها الإشرافية والإنفاذ، تتمتع البنوك المركزية برؤية فريدة حول ما إذا كانت المؤسسات المالية الخاضعة للتنظيم، وحتى المؤسسات غير المنظمة في بعض الأحيان، قد اتخذت الخطوات المناسبة لتكون أكثر مرونة ضد الهجمات الإلكترونية. نظرًا لأن البنوك المركزية هي مستودعات للمعلومات الحساسة للغاية المتعلقة بالنظام المالي، فإن لديهم أيضاً مصلحة قوية في الدفاع ضد اختلاس بياناتهم الخاصة

وتشكل الحوادث السيبرانية تهديداً كبيراً للنظام المالي حيث تشير التقديرات إلى أن الهجمات الإلكترونية على المؤسسات المالية التقليدية وعمليات تبادل العملات المشفرة على حد سواء أدت إلى سرقة مليارات الدولارات. وأدت عمليات اختراق الشركات المالية الكبرى ووكالات الإبلاغ عن ائتمان المستهلكين وتجار التجزئة والوكالات الحكومية إلى اختراق المعلومات الشخصية لمئات الملايين من الأفراد، تعرض خرق البيانات لمقدمي الخدمات من الأطراف الثالثة الملكية الفكرية والمعلومات السرية لشركاتهم المالية المخدومة لمخاطر كبيرة. أصابت هجمات برامج الفدية مئات الآلاف من أنظمة الكمبيوتر على مستوى العالم.

يساهم عدد من العوامل في المخاطر السيبرانية في البنوك، بما في ذلك الاتجاه المتزايد في العولمة، والاستخدام والاعتماد المبكر للتكنولوجيا سريعة التطور، والاعتمادات الكبيرة والترابط داخل كل من النظام المالي والبنية التحتية لتكنولوجيا المعلومات، والتطور المتزايد لمجرمي الإنترنت، والطبيعة الجوهرية لأعمال وخدمات المؤسسات المالية. وإدراكاً منهم للمخاطر المرتبطة بالأمن السيبراني، بدأ المشرفون والمنظمون في جميع أنحاء العالم في اتخاذ خطوات تهدف إلى التخفيف من المخاطر الإلكترونية في المؤسسات المالية، بما في ذلك تعزيز قدرات المرونة وتنفيذ خطط للاستجابة الفعالة للهجمات الإلكترونية والتعافي منها.

لقد أتاح التطور المتسارع الذي شهده قطاع التكنولوجيا المالية الكثير من الفرص أمام البنوك والمؤسسات المالية تحولاً كبيراً لتحسين مستوى الخدمات المقدمة للعملاء من خلال قنوات جديدة ومبتكرة، والتي أحدثت مؤخراً تغيير ملموس في الخدمات المقدمة من قطاع البنوك، حيث ساهم هذا التطور التقني في قيام البنوك بتقديم الخدمات المالية الرقمية بشكل أكبر وخاصةً تعزز من إمكانية الوصول إلى الخدمات المالية الرقمية بيسر وكفاءة وأمان، الأمر الذي أدى إلى توفير الوقت والجهد والمال، لكن بنفس الوقت فإن هذه التطورات التكنولوجية المتسارعة قد تؤدي إلى زيادة تعرض البنوك إلى مخاطر جديدة (مخاطر الأمن السيبراني)، وقد تؤدي إلى تعطل الخدمات المالية الضرورية للأنظمة المالية، وتقويض

الأمن والثقة بالنظام المصرفي، وعدم قيام البنوك بوضع الشمول المالي ضمن أولوياته، وتعرض الاستقرار المالي للخطر، حيث أن الشمول المالي له أثر إيجابي على الاستقرار المالي ووجود علاقة سببية بين مؤشرات الشمول المالي والاستقرار المالي، ويعد الشمول المالي عاملاً هاماً للاستقرار المالي.

حيث أسفرت مخاطر الأمن السيبراني بالفعل عن اختراقات للبيانات التي تم من خلالها الوصول إلى معلومات سرية، الأمر الذي أدى إلى زعزعة أمن المعلومات ناهيك عن الخسائر المالية التي تكبدتها البنوك، كما أن قدرة النظام المصرفي على التصدي للمخاطر السيبرانية يكون من خلال توفير بيئة مناسبة للأمن السيبراني بهدف دعم الشمول المالي لتعزيز الاستقرار المالي. ولغرض ضبط المخاطر السيبرانية وتخفيف الأثر المالي والتحوط منها فإن كثير من البنوك في العالم قامت بتحسين ضوابطها الأمنية ووضع الإجراءات والتدابير والأمن السيبراني التي قد تتعرض لها، حيث شكلت فريق للاستجابة لحوادث الأمن السيبراني لقطاع البنوك بما يساهم في تكثيف الجهود والاستغلال الأمثل للطاقت لتطوير منظومة الأمن السيبراني على مستوى قطاع البنوك، وإصدار تعليمات لكيفية إدارة المخاطر السيبرانية، ووضع السياسات لإدارة أمن المعلومات والأمن السيبراني.

حيث من الضروري على البنوك تكوين مخصصات مالية لمواجهة الخسائر الناتجة عن المخاطر السيبرانية، بالإضافة إلى معالجة نقاط الضعف في أنظمة الرقابة الداخلية، وإعداد خطة لإدارة المخاطر السيبرانية تتضمن تحديد المهام وزيادة سرعة الاستجابة للهجمات والتعافي منها في زمن قياسي لاسترجاع البيانات ومعالجة الأحداث التشغيلية، حيث أن عملية إعداد وتصميم معالجات للمخاطر السيبرانية تتم من خلال تحديد مصادر بداية هذه المخاطر واحتمالية حدوثها.

مشكلة الدراسة:

تعتبر البنوك من أكثر المؤسسات المالية التي تولي عناية خاصة وكبيرة لإدارة مخاطر الأمن السيبراني؛ لأن الآثار المحتملة للاختراق السيبراني تنطوي على تعرض البنوك لخسائر مالية مباشرة وغير مباشرة ناجمة عن الهجمات السيبرانية، وتعطيل الأعمال، والضرر على السمعة، وغيرها، ولا يمكن بأي حال من الأحوال إغفال المخاطر المتزايدة للهجمات السيبرانية التي تعتبر البنوك هدفاً جذاباً لها نظراً لدورها الحيوي في الوساطة المالية، ما قد يهدد الاستقرار والشمول المالي، ومن هذا المنطلق تمكن مشكلة الدراسة من خلال طرح التساؤلات التالية:

السؤال الرئيس:

ما أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك المدرجة في بورصة فلسطين؟

ومن السؤال الرئيس تتفرع التساؤلات الفرعية التالية:

1. ما أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار المالي في البنوك المدرجة في بورصة فلسطين؟

2. ما أثر إدارة مخاطر الأمن السيبراني على تعزيز الشمول المالي في البنوك المدرجة في بورصة فلسطين؟

أهداف الدراسة:

تهدف الدراسة أساساً للتأصيل العلمي من خلال التعرف على أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك المدرجة في بورصة فلسطين، وفي سبيل تحقيق هذا الهدف الرئيس لابد من تحقيق الأهداف الفرعية التالية:

1. بيان أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار المالي في البنوك المدرجة في بورصة فلسطين.

2. التعرف على أثر إدارة مخاطر الأمن السيبراني على تعزيز الشمول المالي في البنوك المدرجة في بورصة فلسطين.

أهمية الدراسة:

تكمن أهمية هذه الدراسة في كونها محاولة علمية حديثة في توضيح أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك، وتتأكد أهمية هذه الدراسة من خلال ما يمكن أن تقدمه من تشخيص لواقع إدارة مخاطر الأمن السيبراني من أجل دعم تطبيق الشمول المالي لتعزيز الاستقرار المالي للبنوك المدرجة في بورصة فلسطين، وتنقسم أهمية الدراسة إلى قسمين:

الأهمية العلمية: تتبع الأهمية العلمية للدراسة في كونها من الدراسات المثيرة والتي تبحث في أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك المدرجة في بورصة فلسطين، وبالتالي قد تساهم هذه الدراسة في زيادة المعرفة للباحثين بحيث يستطيع الباحثين الاعتماد عليها واستقصاء المعلومات اللازمة في إعداد دراساتهم المستقبلية ذات العلاقة.

الأهمية العملية: تبرز الأهمية العملية للدراسة من خلال مساهمة نتائج الدراسة في معرفة كيفية إدارة مخاطر الأمن السيبراني، بالإضافة إلى ما تحققه تقدمه من توصيات لدعم الاستقرار والشمول المالي في البنوك المدرجة في بورصة فلسطين.

فرضيات الدراسة: بناءً على مشكلة وأهداف الدراسة يمكن صياغة الفرضيات كما يلي:-

الفرضية الرئيسية:

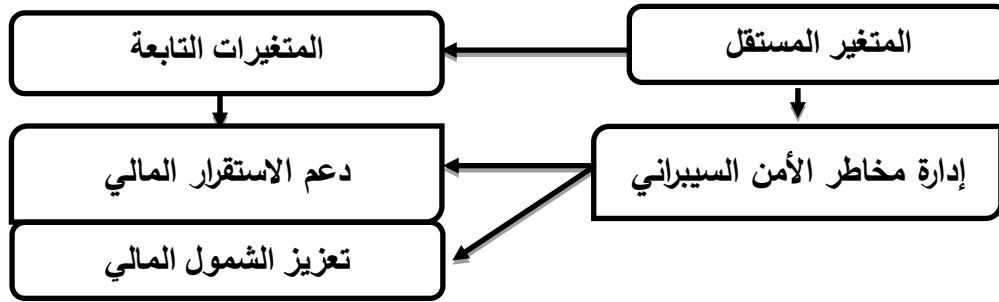
يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) بين إدارة مخاطر الأمن السيبراني ودعم الاستقرار والشمول المالي في البنوك المدرجة في بورصة فلسطين؟

ويتفرع من الفرضية الرئيسية الفرضيات الفرعية التالية:

الفرضية الأولى: يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) بين إدارة مخاطر الأمن السيبراني ودعم الاستقرار المالي في البنوك المدرجة في بورصة فلسطين.

الفرضية الثانية: يوجد أثر ذو دلالة إحصائية عند مستوى معنوية ($\alpha \leq 0.05$) بين إدارة مخاطر الأمن السيبراني وتعزيز الشمول المالي في البنوك المدرجة في بورصة فلسطين.

نموذج الدراسة:



شكل رقم (1) أنموذج الدراسة

حدود الدراسة:

تمثلت حدود الدراسة فيما يلي:

1. الحدود الزمانية: تم إعداد هذا الدراسة خلال عام 2022.
2. الحدود المكانية: يطبق هذا الدراسة على البنوك المدرجة في بورصة فلسطين.
3. الحدود البشرية: تتكون من مدير عام، مدير فرع، مدير الدائرة المالية، مدير إدارة المخاطر.
4. الحدود العلمية: دراسة أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك.

الدراسات السابقة والإطار الفكري

أولاً: الدراسات السابقة

1. دراسة (Saon, Miglanic, 2019):

هدفت هذه الدراسة إلى دراسة كيفية تمكين تقنيات الذكاء الاصطناعي والبلوك تشين للمساهمة في تدعيم الشمول المالي. في حين أن إمكانيات تقنية block chain، بشكل عام والعقود الذكية، على وجه الخصوص، لجعل الخدمات المالية أكثر كفاءة وفعالية من حيث التكلفة وشاملة لا جدال فيها، فهناك قلق فيما يتعلق بقابلية التوسع وقابلية التشغيل البيئي وتأثير التكلفة والتنظيم. يؤدي أيضاً إلى الانتقال إلى للفهم والخبرة وخلق حواجز ثقافية تجعل الابتعاد عن النظام القديم أكثر صعوبة. ويمكن لتقنية Block chain أن تغير قواعد اللعبة إذا تم تبنيها على نطاق واسع وكان هناك اتفاق على بنية التكنولوجيا التي يجب وضعها لتبنيها. بقدر ما يتعلق الأمر بالذكاء الاصطناعي، فهي تقنية ناشئة وهناك تحديات مثل

سرعة المعاملات وعملية التحقق وحدود البيانات. وضعها التنظيمي غير مؤكد وهناك مخاوف تتعلق بالتكامل (داخل المنظمة، بسبب النظام البيئي الحالي)، وندرة المواهب، والتكاليف المتضمنة. إن إمكانات هاتين التقنيتين في تحقيق قدر أكبر من الشمول المالي واضحة بلا شك. ويعتمد ما إذا كان ذلك سيحدث على العديد من العوامل بالإضافة إلى مدى سرعة اعتماد هذه التقنيات من قبل معظم لاعبي التكنولوجيا المالية.

2. دراسة (Vucinic, 2020):

هدفت الدراسة إلى دراسة الآثار المحتملة لتطورات التكنولوجيا المالية على الاستقرار المالي، وتأثير التكنولوجيا المالية على هيكل السوق بالإضافة إلى فوائد ومخاطر الابتكارات المالية المدفوعة تقنيًا على الاستقرار المالي. وتؤكد نتائج الدراسة على أهمية التعاون الدولي للمنظمين من أجل الحفاظ على الاستقرار المالي في العالم الحديث من التغيرات والابتكارات التكنولوجية، حيث قامت FinTech بتغيير توقعات المستهلكين وتفضيلاتهم مع زيادة عدد المستخدمين الذين يتوقعون خدمات سريعة وسهلة الوصول متاحة على الهواتف المحمولة والأجهزة الإلكترونية الأخرى. كما أظهرت نتائج الدراسة أن التكنولوجيا الجديدة توفر مساحة لتوسيع الخدمات المالية ولكنها تشكل أيضاً مخاطر إضافية على النظام المالي من حيث مخاطر التمويل الأصغر والمخاطر المالية الكلية.

3. دراسة (Khan, Malaika, 2021):

بحثت هذه الدراسة في التكنولوجيا المالية ومجال الأمن السيبراني ذي الصلة من منظور إدارة مخاطر البنك المركزي، واعتمدت هذه الدراسة على النتائج المستخلصة من قاعدة بيانات المادة الرابعة لصندوق النقد الدولي، وخيارات تقييم البنوك المختارة، حيث سلطت الدراسة الضوء على ضرورة معالجة المخاطر المتعلقة بالتكنولوجيا المالية والأمن السيبراني للبنوك المركزية من خلال تفعيل الإدارة السليمة للمخاطر الداخلية من خلال إنشاء وتعزيز نهج متكامل لإدارة المخاطر في جميع أنحاء المنظمة، بما في ذلك وحدة مخصصة لإدارة المخاطر، والتوعية والتدريب المستمر لأعضاء مجلس الإدارة والموظفين، وخطوط إبلاغ واضحة، وتقييم المرونة السيبرانية والوضع الأمني، وربط إدارة المخاطر بالتخطيط الاستراتيجي. وبالنظر إلى الطبيعة سريعة التطور لمثل هذه المخاطر، ويمكن للبنوك المركزية الاستفادة من المدخلات المنتظمة وفي الوقت المناسب من الخبراء الخارجيين.

4. دراسة (Varga, et al., 2021):

هدفت الدراسة إلى التحقيق في الوعي بالوضع السيبراني في البنوك في السويد، من خلال فحص عناصر المعلومات اللازمة لصورة تشغيلية مشتركة، واستكشاف كيفية إدراك الجهات الفاعلة الرئيسية للتهديدات السيبرانية، تم جمع البيانات من خلال المقابلات مع الجهات الفاعلة الرئيسية في القطاع بالتزامن مع ممارسة إدارة الأزمات على المستوى الوطني. وتم تحليل البيانات ومقارنتها بالنظرية. وأظهرت النتائج أن الجهات الفاعلة في البنوك السويدي لديها مفهوم عمل متطور لإدارة الأزمات. ومع ذلك، فإن المعلومات

حول الخصوم العقلانيين الذين يتسببون في اضطرابات طويلة الأمد ربما لا يتم جمعها وتحليلها واستخدامها بشكل منهجي. وان القطاع البنوك يدرك التهديدات السيبرانية ضد البنية التحتية المالية الأساسية، وكذلك ضد توافر خدمة تكنولوجيا المعلومات وسرية البيانات، إلى جانب المالية والمخاوف الخاصة بشأن احتمال فقدان السمعة بسبب الهجمات الإلكترونية. وهناك أيضاً مخاوف خاصة بشأن التهديد من الداخل.

5. دراسة (Inoussa, 2021):

هدفت الدراسة إلى دراسة تأثير التكنولوجيا المالية على الشمول المالي من خلال بناء مقياسين منفصلين لتقييم الشمول المالي التقليدي والرقمي ولتقديم ثلاثة مؤشرات جديدة للشمول المالي. والتحقيق في آثار الشمول المالي المدفوع بالتكنولوجيا المالية على النمو الاقتصادي وعدم المساواة في الدخل باستخدام مجموعة من 16 دولة من دول أفريقيا الواقعة جنوب الصحراء الكبرى مع بيانات من FAS وقاعدة بيانات Findex العالمية عبر عامي 2014 و2017، وعلى وجه التحديد استخدمت المؤشرات لتقييم تأثير الشمول المالي المدفوع بالتكنولوجيا المالية على النمو الاقتصادي وعدم المساواة في الدخل، وظهرت النتائج ثلاثة استنتاجات رئيسية من نتائج الدراسة. أولاً، يعد الشمول المالي القائم على التكنولوجيا المالية استراتيجية أفضل من الشمول المالي التقليدي لإدخال الفقراء وسكان الريف في النظام المالي. ثانياً، يمكن أن يساهم الشمول المالي المدفوع بالتكنولوجيا المالية في النمو الاقتصادي في أفريقيا جنوب الصحراء الكبرى. ثالثاً، يقلل الشمول المالي القائم على التكنولوجيا المالية من عدم المساواة في الدخل. مع تزايد اعتبار الشمول المالي أداة أساسية في تنفيذ أهداف التنمية المستدامة، كما تساهم نتائج هذه الدراسة في أدبيات الشمول المالي، وإلقاء الضوء على دور الشمول المالي القائم على التكنولوجيا المالية في تعزيز التنمية الشاملة والمستدامة. كما أن الأفكار المكتسبة من هذه الدراسة تضع الأساس للبحث المستقبلي في محددات الشمول المالي والطرق المختلفة التي قد تدعم بها التكنولوجيا المالية التنمية المستدامة المتوازنة.

6. دراسة (Eisenbach, Lee, 2022): هدفت الدراسة إلى توضيح كيف يمكن أن تنتقل الهجمات الإلكترونية على بنك كبير واحد أو مجموعة من البنوك الصغيرة أو مزود خدمة مشترك من خلال نظام المدفوعات، حيث من المرجح أن يتم تضخيم أي هجوم إلكتروني على أكثر البنوك الأمريكية نشاطاً والذي يضعف من قدرات تلك البنوك على إرسال المدفوعات للتأثير على السيولة في العديد من البنوك الأخرى في النظام. سيكون مدى التضخيم أكبر إذا استجابت البنوك بشكل استراتيجي، وهو ما من المرجح أن يفعلوه إذا كان هناك عدم يقين بشأن الهجوم. قد يكون التأثير على المناطق الجغرافية ذات البنوك المركزية أكبر، وحددت أيضاً طرقاً أخرى يمكن أن يصبح بها النظام معطلاً والتي تسلط الضوء على أهمية جميع البنوك في الشبكة، وليس فقط البنوك الكبرى، وإذا تم توصيل عدد من البنوك الصغيرة أو متوسطة الحجم من خلال نقطة ضعف مشتركة، مثل مزود خدمة مهم، فقد يؤدي ذلك إلى انتقال

صدمة عبر الشبكة. وبالمثل، فإن البنوك التي لديها أصول قليلة نسبياً ولكن تدفقات مدفوعات كبيرة لديها أيضاً القدرة على إضعاف النظام.

التعقيب على الدراسات السابقة:

– أوجه الاختلاف بين الدراسة الحالية والدراسات السابقة:

1. من حيث الموضوع:

تناولت الدراسات السابقة مناقشة موضوع " أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك"، ولكنها ركزت على دراسة واقع الأمن السيبراني ومخاطره في البنوك المدرجة في بورصة فلسطين العاملة في قطاع غزة بدولة فلسطين وأثرها في دعم الاستقرار والشمول المالي.

2. من حيث المكان: تنوعت أماكن تطبيق الدراسات السابقة (السويد، أمريكا، جنوب أفريقيا، كندا).

3. من حيث المنهج: اعتمدت الدراسات السابقة المنهج الوصفي التحليلي.

4. من حيث الأدوات: استخدمت معظم الدراسات المنهج الوصفي كأداة للدراسة.

5. من حيث العينات: تنوعت عينات الدراسات السابقة فبعض الدراسات كانت على الشركات ومنها على البنوك، أما الدراسة الحالية فكانت العينة من البنوك المدرجة في بورصة فلسطين.

– ما يميز الدراسة الحالية عن الدراسات السابقة: تتميز الدراسة الحالية في عدة نقاط؛ أهمها:

– تعتبر الدراسة الحالية بناءً معرفياً وتراكيمياً للدراسات السابقة حول الموضوع، وتأتي استكمالاً لما بدأه الباحثون؛ فهي تُبنى على ما توصلوا إليه من نتائج، وما قدموه من توصيات.

– تركز الدراسة الحالية على دراسة أثر مخاطر الأمن السيبراني على دعم وتعزيز الاستقرار والشمول المالي، وهي بذلك تعتبر أكثر تخصصاً من الدراسات السابقة، كونها تناولت دراسة الأثر بين متغيرين في موضوعها وهي مخاطر الأمن السيبراني والاستقرار والشمول المالي.

– تضع الدراسة الحالية حلولاً عملية لمخاطر الأمن السيبراني في البنوك المدرجة في بورصة فلسطين لدعم وتعزيز الاستقرار والشمول المالي.

ثانياً: الإطار الفكري

1. الامن السيبراني وإدارة مخاطره

1-1. مخاطر الأمن السيبراني

الأسواق المالية أهدافاً جذابة بشكل متزايد لمجرمي الإنترنت مع تعزيز الدول المتقدمة لدفاعاتها الإلكترونية. ويؤدي انتشار الخدمات المالية الرقمية وزيادة الترابط بين الأنظمة والأسواق المالية إلى تفاقم التهديد الذي تشكله الهجمات الإلكترونية على القطاعات المالية في البلدان النامية وكذلك على الصعيد العالمي، ويعد بناء مرونة قوية على الإنترنت أمراً بالغ الأهمية لاستقرار الأسواق المالية وكذلك لتحقيق الشمول المالي، ويمكن للهجمات السيبرانية أن تثبط جهود الشمول المالي لأنها، إذا نجحت، قد تردع العملاء عن تبني منتجات وخدمات مالية جديدة.

وتعتبر المخاطر الإلكترونية شكلاً من أشكال المخاطر التشغيلية وتعرف على أنها مخاطر الخسارة الناتجة عن الحوادث الرقمية الناجمة عن الحوادث الداخلية والخارجية. أو أطراف ثالثة، بما في ذلك السرقة أو النزاهة المعرضة للخطر أو تلف المعلومات أو أصول التكنولوجيا، والاحتيال الداخلي والخارجي، وتعطيل الأعمال. وهذا التعريف يتوافق إلى حد كبير مع جهود القطاع الخاص المتزامنة المعروفة لتحديد المخاطر السيبرانية، على سبيل المثال، مبادرة مخاطر الأمن السيبراني والمعلوماتية الخاصة بشركة ORX. وقد تؤدي حوادث المخاطر السيبرانية إلى إضعاف سرية وسلامة وتوافر البيانات والمعلومات، والتشغيل السليم للبنية التحتية لتكنولوجيا المعلومات.

حيث أن أنظمة الأمن السيبراني هي أنظمة مدعومة بالذكاء الاصطناعي للحماية من الانتهاكات الأمنية المحتملة ومنعها، ويستخدم الذكاء الاصطناعي لتطبيق الخدمات المصرفية عبر الهاتف المحمول وتطوير حلول الذكاء الاصطناعي لدعم العملاء وأتمتة العمليات والموارد البشرية والأمن واكتشاف الاحتيال. (Saon, Miglanic, 2019)

وقد عرف مخاطر الأمن السيبراني على أنه المخاطر التشغيلية لأصول المعلومات والتقنية التي تؤثر على سرية أو توافر أو سلامة المعلومات أو أنظمة المعلومات. (Kumar, Thomas, 2022)، وإن سرقة بيانات وهوية المستهلك، وكذلك والتلاعب بها، باعتبارها تهديدات إلكترونية رئيسية تؤثر على أعمال البنوك. والتهديدات التي تتعرض لها البنية التحتية المالية، والمخاطر التي تشكلها البرامج الضارة المدمرة (Piotrowski, 2022)، وإن تصنيف المخاطر السيبرانية والمحفزات الكامنة وراءها يمكن أن يؤدي إلى وجود تعريف وفهم مشترك عبر البنوك، بما في ذلك بين السلطات والمشاركين من القطاع الخاص، وإلى زيادة تسهيل تبادل المعلومات والتعاون المناسب في إدارة المخاطر الإلكترونية. حيث يتم تنظيم تصنيف المخاطر الإلكترونية للأمن السيبراني إلى :

1. **مسببات المخاطر السيبرانية:** الطريقة التي يتم من خلالها تنفيذ هجوم إلكتروني ضار من خلال:
 - **رفض الخدمة:** هو هجوم يغمر الأنظمة أو الخوادم أو الشبكات بحركة مرور لاستنفاد الموارد وعرض النطاق الترددي. نتيجة لذلك، النظام غير قادر على تلبية الطلبات المشروعة. ورفض الخدمة الموزع (DDoS) هو عندما يستخدم المهاجمون عدة أجهزة مختربة لتنفيذ الهجوم.

- **هجوم التنصت:** يدخل المهاجمون أنفسهم في معاملة ثنائية الأطراف وذلك بمجرد مقاطعة المهاجمين لحركة المرور، يمكنهم تصفية البيانات وسرقتها.
 - **التصيد الاحتيالي:** هو ممارسة إرسال اتصالات احتيالية التي تبدو أنها واردة من مصدر حسن السمعة، عادةً عبر البريد الإلكتروني. والهدف منه سرقة البيانات الحساسة مثل بطاقة الائتمان ومعلومات تسجيل الدخول أو تثبيت برامج ضارة على جهاز الضحية.
 - **هجوم كلمة المرور:** يحدث عندما تحصل أطراف غير مصرح لها على حق الوصول إلى كلمة مرور الشخص من خلال النظر حول مكتب الشخص، و"استنشاق" الاتصال بالشبكة للحصول على كلمات مرور غير مشفرة، واستخدام الهندسة الاجتماعية، والحصول على إمكانية الوصول إلى قاعدة بيانات كلمة المرور أو التخمين المباشر (القوة الغاشمة أو هجوم القاموس).
 - **حقن SQL:** يحدث حقن لغة الاستعلام الهيكلية (SQL) عندما يقوم المهاجم بإدراج تعليمات برمجية ضارة في خادم يستخدم SQL ويجبر الخادم على الكشف عن المعلومات الخاصة به عادة لا.
 - **البرمجة النصية عبر المواقع:** تستخدم هجمات البرمجة النصية عبر المواقع موارد ويب تابعة لجهات خارجية لتشغيل البرامج النصية في متصفح الويب الخاص بالضحية أو التطبيق القابل للبرمجة.
 - **البرامج الضارة:** برنامج مصمم بقصد ضار يحتوي على ميزات أو قدرات يمكن أن تسبب ضررًا مباشرًا أو غير مباشر للكيانات أو أنظمة المعلومات الخاصة بها.
 - **استغلال Zero-day:** ثغرة أمنية في الأجهزة أو البرامج الثابتة أو البرامج غير المعروفة سابقاً.
 - **أخرى:** أي نوع آخر من الهجمات الإلكترونية التي لم يتم تعريفها. ستعمل هذه الفئة كفتة "النقاط الكل" للهجمات الإلكترونية ذات النوع المعروف ولكن لم يتم التقاطها بواسطة فئة أخرى موجودة.
 - **غير معروف:** عندما يكون نوع الهجوم الإلكتروني غير معروف للمؤسسة.
2. **نتيجة الحادث السيبراني: نتيجة حادث إلكتروني يؤدي إلى:**
- **اضطراب الأعمال وفشل النظام والتنفيذ:** هي الحوادث الداخلية أو الخارجية التي تعطل العمل أو تتسبب في فشل البرامج / الأجهزة / تكنولوجيا المعلومات.
 - **خرق البيانات:** تعني فقدان البيانات أو التعرض الذي يتضمن معلومات التعريف الشخصية.
 - **سرقة أو فقدان معلومات غير معلومات:** تعني سرقة أو فقدان التكنولوجيا أو الملكية الفكرية أو المعلومات التجارية أو أي معلومات أخرى ليست معلومات تحديد الهوية الشخصية.
 - **سرقة الأموال:** هي الحوادث التي أدت إلى خسارة فورية ومباشرة للأموال وتم تنفيذها عبر قناة رقمية.
3. **النية: مؤشر لمعرفة ما إذا كان الحادث الإلكتروني متعمدًا أم عرضيًا:**

- **متعمد:** عندما يكون الحادث الإلكتروني كيداً / متعمداً.
- **غير مقصود:** عندما يكون الحادث السيبراني غير مقصود.
- 4. **المنشأ:** مؤشر لمعرفة ما إذا كانت الحادثة الإلكترونية قد نشأت في المؤسسة أو في جهة خارجية:

- **طرف خارجي:** عند وقوع الحادث السيبراني لدى طرف ثالث / بائع أو أي كيان خارجي آخر.
- **طرف غير خارجي:** عندما بدأ الحادث الإلكتروني في المؤسسة أو الشركة التابعة لها.
- 5. **فئة حدث بازل (II): فئة حدث بازل المخصصة للحادث السيبراني:**
- **الاحتيال الداخلي:** خسائر ناجمة عن أفعال من نوع الاحتيال أو اختلاس الممتلكات أو التحايل على اللوائح أو القانون أو سياسة الشركة، باستثناء أحداث التنوع / التمييز، والتي تشمل طرفاً داخلياً واحداً على الأقل.

- **الاحتيال الخارجي:** خسائر ناجمة عن أفعال من النوع المقصود بها الاحتيال أو اختلاس الممتلكات أو التحايل على القانون من قبل طرف ثالث.

ويستخلص الباحثان أنه يمكن تعريف مخاطر الأمن السيبراني على أنه حدث يمكن ملاحظته في نظام المعلومات، حيث أن الخطر السيبراني يهدد المعلومات التي يعالجها النظام أو يخزنها أو ينقلها. أو ينتهك السياسات أو الإجراءات الأمنية أو سياسات الاستخدام المقبولة، سواء كان ذلك نتيجة لنشاط ضار أم لا. ويمكن أن يؤدي الحادث الإلكتروني إلى خسارة مالية. ويمكن ملاحظته في نظام معلومات لا ينتج عنه بالضرورة خسارة مالية. وهناك تهديدان لتقنيات ناشئة جديدة غير مثبتة وربما مليئة بنقاط الضعف، وانتشار المعلومات المضللة واستخدامها بشكل عام، كما أن التعامل مع المخاطر السيبرانية، والقضايا السيبرانية بشكل عام، يتم النظر إليه بطريقة مختلفة عن إدارة الأنواع الأخرى من المخاطر.

1-2. مخاطر الامن السيبراني في الخدمات المالية عبر الحدود

تثير الابتكارات الرقمية لخدمات الدفع عبر الحدود باستخدام FinTechs مخاطر جديدة، لا سيما فيما يتعلق بالأمن السيبراني. إن الطبيعة المتغيرة للهجمات الإلكترونية ونمو المخاطر السيبرانية مدفوعة بعوامل تشمل التقنيات المتقدمة، وزيادة الترابط بين المؤسسات المالية والأطراف الخارجية، والحوافز الأكثر أهمية لمجرمي الإنترنت لاستهداف الهيئات المالية (Huang, Madnick, 2020) على سبيل المثال، أدى الهجوم الإلكتروني على بنك (Banco de Chile) في عام 2018 إلى تدمير 9000 محطة عمل و500 خادم، بالإضافة إلى تعرض نقاط النهاية للتعامل مع المعاملات على شبكة SWIFT للخطر، كما يتم استخدام الخوارزميات التي تعمل خلف الشاشة لأتمتة الموافقات أو الاستشارات الائتمانية، وتسهيل الامتثال التنظيمي واكتشاف الاحتيال وأتمتة تداول الأصول المالية، وتلعب أدواراً أساسية لخدمات الدفع عبر الحدود. ومع ذلك، فإن سلامة الخوارزميات، والضعف المتأصل في

الخوارزميات المعتمدة، والمسائل الأخلاقية للحكم الذاتي، وما إلى ذلك، تزيد من المخاطر النظامية داخل نظام الدفع عبر الحدود. نظرًا للاعتماد الواسع النطاق للتداول الخوارزمي هذه الأيام، يمكن أن تؤدي هذه التقلبات إلى مزيد من "الانهيارات السريعة"

ويعتبر النظام المالي بنية تحتية مهمة ويتم تعريف أمنه السيبراني على أنه جزء من الأمن السيبراني الوطني. "الاستثناء الأمني" هو مبدأ مهم في بيئة التجارة الدولية، والذي يسمح للحكومات باتخاذ الإجراءات عند الضرورة في حالات "المصلحة الأمنية الأساسية". ومع ذلك، يعتبر هذا الاستثناء الأمني محدودًا ذاتيًا، أو ما يسمى "الحكم الذاتي" أو "التفسير الذاتي" ومن المتوقع أن يظل غير واضح في المستقبل القريب. حيث يثير العديد من النزاعات في مجال الأمن السيبراني بين الدول (Tzoneva, Stoyanov, 2022)، ولتغلب على خسائر الأمن السيبراني لابد من وجود مبادئ أساسية مهمة لإنشاء مخطط لتصنيف تأثير الخسائر السيبرانية في إنشاء فئات تجمع تأثيرات الخسارة المتشابهة نسبيًا في طبيعتها وتحتوي على دوافع مماثلة من أجل تسهيل الخطوات القابلة للتنفيذ من منظور إدارة المخاطر، خاصة

1-3. إدارة مخاطر الأمن السيبراني في البنوك

إدارة المخاطر هي عمل أساسي للبنوك، فمن المهم التمييز بين الأنواع المختلفة من المخاطر، حيث أن التمييز الأساسي هو التمييز بين المخاطر المالية وغير المالية. على سبيل المثال، المخاطر التي يتعين على البنوك الاحتفاظ برأس مالها: مخاطر الائتمان (تقصير الأطراف المقابلة)، ومخاطر السوق (انخفاض قيمة الأصول المتداولة)، ومخاطر التشغيل (تلك العمليات الداخلية أو فشل الأنظمة أو أن الأحداث الخارجية المعاكسة تتحقق)، حيث أن المخاطر الأولى والثانية في هذا التصنيف مالية في الأصل، في حين أن الأخطار الأخيرة، التي تشمل المخاطر السيبرانية، غير مالية في الأصل (Varga, Brynielsson, Franke, 2021)، وتعتمد البنوك على التكنولوجيا السيبرانية (CyberTech)، ولكنها تصبح عرضة للأمن السيبراني. وبالتالي، تصبح زيادة الاستثمار في CyberTech وضرورة استراتيجية للبنوك لمكافحة مخاطر الأمن السيبراني.

وتعد إدارة المخاطر السيبرانية مجالاً تقنياً 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 نادراً ما يتم جمعها جنباً إلى جنب مع مقاييس التأثير. كما أن معظم مصادر البيانات الموضحة أعلاه هي من مصادر مختلفة ويتم توفيرها من قبل بائعين مختلفين (Herrera, Munera, Williams, 2021).

التوجيهات التنظيمية المتعلقة بإدارة المخاطر الإلكترونية. يمكن أن يعزز التصنيف المشترك لعمل الوكالات التنظيمية والإشرافية في توفير التوجيه المتعلق بالأمن السيبراني والمرونة الإلكترونية، بما في ذلك تحديد الممارسات الفعالة أو التهديدات الناشئة. على سبيل المثال، والمساعدة في استخدام لغة مشتركة لتعزيز الأساليب التنظيمية الفعالة مع تقليل مخاطر المتطلبات التنظيمية والإشرافية المتكررة والمتضاربة. (Curti, Gerlach, et al., 2019)، وقد تم تطوير معايير جديدة للإبلاغ عن معلومات المخاطر السيبرانية في السنوات الأخيرة عن طريق ORX للمخاطر الإلكترونية 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 (Herrera, Munera, Williams, 2021).

ويرى الباحثان أن الافتقار إلى قدرات الحماية الكافية يمكن أن يعرض البيانات لخطر انتهاكات البيانات. في ضوء ذلك، هناك متطلبات من اتفاقية بازل وحوكمة البنوك تتعلق بالأمن السيبراني وتدبير 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 الإلكترونية من مزودي الخدمة الخارجيين، بما في ذلك المصدر الأجنبي، ويعتبر هذا أمراً بالغ الأهمية عند التخفيف من المخاطر الإلكترونية من سلاسل التوريد ويقترح أيضاً اختبار رموز المصدر كأحد أفضل الإجراءات لإدارة مخاطر الإنترنت في سلسلة التوريد. ومع ذلك، فإن الكشف عن أكواد المصدر يمكن أن يثير مخاوف بشأن حماية الملكية الذكية، وهي ميزة نسبية للعديد من الشركات الدولية.

1-4. أثر استخدام التكنولوجيا المالية على الاستقرار والشمول المالي في قطاع البنوك:

تلعب التكنولوجيا المالية دوراً متزايداً لتعزيز نظام الدفع عبر الحدود بينما تظهر مخاطر التهديد السيبراني. ومع ذلك، ينبغي أن يقترن الاستخدام المتزايد لهذه التقنيات بتعزيز الرقابة التنظيمية على الأنشطة المالية لحماية الاستقرار المالي، حيث قد تظهر مخاطر جديدة تزيد اتجاهات الرقمنة المالية من

الحاجة إلى الأمن السيبراني لحماية المستهلكين والمنتجين الماليين. ومن ثم، إلى جانب تنفيذ اللوائح ذات الصلة لحماية الأنظمة المالية والتخفيف من مخاطر الأمن السيبراني المحتملة، حيث فرضت العديد من الدول قيوداً على حواجز التجارة الإلكترونية، بهدف تصنيفها في الفئات التالية، التوطين، ويتكون أول تقييد للتجارة من متطلبات التوطين، بما في ذلك البيانات أو توطين النظام ذي الصلة. على سبيل المثال، تتطلب الهند أن يتم وضع جميع بيانات الدفع التي تحتفظ بها شركات الدفع في منشآت محلية داخل الدولة ولا يسمح بتصديرها خارج البلاد، ولا حتى للمعالجة. إلى جانب متطلبات البيانات، Huang, (Madnick, 2020).

وعلى الرغم من أن FinTech تخلق فوائد للاستقرار المالي، إلا أنه من المحتمل أن يكون لها تأثير نظامي سلبي على الأخير ويمكن أن تنتج آثاراً سلبية خطيرة يمكن أن تعرض الاقتصاد الحقيقي للخطر، وتعتبر التكنولوجيا المالية إحدى التقنيات الهامة التي يمكن أن تقوض الاستقرار المالي من خلال قنوات التمويل الأصغر والقنوات المالية الكلية. لذلك يمكن أن تخلق التكنولوجيا المالية مخاطر مالية صغيرة وكبيرة على الاستقرار المالي. بينما يعمل رأس المال والسيولة من جانب على تعزيز المرونة المالية، من ناحية أخرى، وتدعم الحوكمة والضوابط القوية المرونة التشغيلية. وتتبع مصادر المخاطر التشغيلية من الحوكمة ومراقبة العمليات، والمخاطر الإلكترونية، والاعتماد على الأطراف الثالثة، والمخاطر القانونية ومخاطر الأعمال المتعلقة بالبنية التحتية الحيوية للأسواق المالية (Vucinic, 2020).

ويشير الشمول المالي إلى عدد المستفيدين الذين يمكنهم الوصول إلى الخدمات المصرفية أو المالية، حيث أن الخطوة الأولى نحو الشمول المالي هي امتلاك حساب على نحو متزايد، يتم استخدام المدفوعات الرقمية في المعاملات المالية. كما يعد إجراء المدفوعات الرقمية أو تلقيها أحد الاستخدامات المهمة لحساب الادخار. مع ذلك، أفاد عدد قليل من الأشخاص باستخدام حساباتهم للادخار ولكن ليس أيضاً لإجراء مدفوعات رقمية أو تلقيها في العام الماضي، كما ساعدت التكنولوجيا في تحقيق التكافؤ بين الجنسين وقلصت الفجوة بين البالغين الأكثر ثراءً والفقراء (Saon, Miglanic, 2019).

وان أحد المنتجات التي تم إنشاؤها من نموذج Fintech هو منصة الإقراض من شخص إلى شخص (P2P)، على الرغم من أن إقراض P2P يقدم خدمات أفضل بتكاليف منخفضة، إلا أنه زاد أيضاً من مخاطر الائتمان. وبالتالي ظهور المخاطر النظامية، ومما لا شك فيه أن الوسائط الرقمية قد زادت من مستوى الشمول المالي عالمياً من 51 بالمائة عام 2011 إلى 69 بالمائة في 2017 والتحدي الذي يواجه البنوك هو تحديد أنسب نموذج للاتصال للتفاعل مع شرائح مختلفة من العملاء من أجل إقناعهم ببنية قنوات مصرفية رقمية. ونظراً للاضطرابات غير النقدية، لا تستطيع المؤسسات المالية التحكم في تجربة العملاء في المعاملات بسبب التكامل وتفتت المؤسسات المالية الرؤية وسيتمكن عليها أن تهدف إلى تأمين مكان البطاقة الافتراضية في السوق. (Yadav, Shanmugam, 2022).

أن التطورات السريعة في التكنولوجيا المالية على الأسواق المالية ونماذج

الأعمال للمؤسسات المالية التقليدية من أجل متابعة الاتجاهات الحالية والمنافسة في منافستها سريعة النمو، للوصول إلى الشمول المالي. حيث تتبنى المؤسسات المالية التقليدية التغييرات من أجل تلبية احتياجات السوق. ويمكن أن تكون عوامل جانب العرض والطلب بمثابة محركات للابتكارات المالية، وتبحث للأجيال الجديدة بشكل خاص عن خدمة مالية سريعة وسهلة الوصول يمكن الوصول إليها في أي وقت وفي أي مكان. وفيما يتعلق بذلك، من المرجح أن يستخدموا المدفوعات الإلكترونية أو الخدمات المصرفية عبر الهاتف المحمول أو ائتمانات FinTech أو غيرها من المنتجات بدلاً من استخدام أساليب الخدمات المالية التقليدية. والشاغل الرئيسي هو التأثير الرقمي على استقرار وسلامة أسواق والأنظمة المالية الأوسع.

1-5. اثر مخاطر الامن السيبراني على الاستقرار والشمول المالي للبنوك:

تتنبت البنوك بشكل متزايد دورها في تعزيز الشمول المالي إلى جانب أهدافها التقليدية المتمثلة في الحفاظ على استقرار الأسعار والاستقرار المالي. ولتحقيق هذه الغاية، لا تستخدم بعض البنوك المركزية القواعد واللوائح فحسب، بل تستخدم أيضًا الابتكار من خلال التدخل المباشر في نظام المدفوعات الفورية المدعوم من البنك المركزي. والذي يمكن أن يحدثه البنك المركزي على تحقيق الإدماج والمنافسة في صناعة المدفوعات. وأن دور البنك في المدفوعات يمكن أن يكون أداة فعالة لتعزيز الإدماج وتعزيز المنافسة، لا سيما عندما يبدو الفاعلون الخاصون غير راغبين أو غير قادرين على القيام بذلك بأنفسهم. ومع ذلك، فإن شرعية التدخلات المبتكرة للبنك المركزي في المدفوعات والذي يمكن للبنوك أن تمضي فيه في إجراءاتها المبتكرة دون المبالغة في تقدير أيديها أو إزاحة المبادرة والبراعة الخاصة، Bolzani (2022)، وتغطي البنوك خمس وظائف واسعة. وهي من أجل (Saon, Miglanic, 2019):

- إجراء المدفوعات واستلامها، بما في ذلك عبر الحدود.
- الادخار لتتمكن من الاستهلاك أو الاستثمار لاحقاً.
- الاقتراض لتتمكن من الاستهلاك أو الاستثمار الآن.
- إدارة المخاطر على الدخل والمدخرات والمعاملات.

قد تحفز Fintech مكاسب الكفاءة في البنوك، وتقدم منتجات وخدمات أفضل وأكثر استهدافاً، وتعمق الشمول المالي. ومع ذلك، قد يشكل أيضاً مخاطر إذا كان تطبيقه يقوض المنافسة والثقة ونقل السياسة النقدية والاستقرار المالي. على الرغم من الاعتراف بأن المخاطر السيبرانية تشكل تهديداً كبيراً لاستقرار المالي، إلا أن قياس وتحليل المخاطر الإلكترونية في البنوك لم ينضج إلى الحد الذي يمكن فيه قياسها وإدارتها باستمرار مقابل تقبل المخاطر المؤسسية والنظر إليها من منظور النظام من خلال المنظمون والمشرّفون. وهذا يعيق الجهود المبذولة لقياس وإدارة هذه المخاطر بشكل فعال، مما يقلل من

استعداد المؤسسات الفردية والجماعية للتعامل مع التهديدات الإلكترونية على مستوى النظام ومعالجة تكنولوجيا المعلومات أو أبعاد هندسة النظام للمخاطر السيبرانية، بل التركيز على جوانب إدارة المخاطر المالية للمخاطر السيبرانية (Tzoneva, Stoyanov, 2022).

أن المخاطر السيبرانية تمتد إلى جميع المجالات الرئيسية لعمليات البنوك، والاستقرار المالي، والنزاهة المالية، والشمول المالي، وأنظمة الدفع، وإدارة العملات النقدية. على الرغم من أن هذه المخاطر المتعلقة بالأمن السيبراني تؤثر في المقام الأول على المؤسسات الخاضعة للإشراف والمشاركين في الأسواق المالية، إلا أنها تؤثر أيضاً على التعرض للمخاطر التي يواجهها البنك نفسه. بالإضافة إلى ذلك، يمكن أن تتفاقم المخاطر التشغيلية المتعلقة بالنظام الداخلي، بما في ذلك تكنولوجيا المعلومات (والأمن السيبراني) والموارد البشرية وإدارة استمرارية الأعمال، من خلال زيادة استخدام أدوات التكنولوجيا المالية أيضاً. لذلك، تحتاج إدارة المخاطر السيبرانية للبنك إلى تشكيل خط دفاع مناسب للمخاطر المتعلقة بالتكنولوجيا المالية.

وعلى الرغم من أن مخاطر الأمن السيبراني ليست جديدة على الإطلاق، فإن السرعة والميل الذي تحدث به تطورات في البنوك إلا أن إدارات تكنولوجيا المعلومات والمشرفين الماليين هم أول "وحدات عمل" داخل العديد من البنوك لتحديد مخاطر الأمن السيبراني. لذلك تحتاج البنوك إلى تعزيز إدارتها الداخلية للمخاطر لتشمل مساعدة شاملة على مستوى البنك في تحديد المخاطر المتعلقة بالتكنولوجيا ومخاطر الأمن السيبراني وتخفيفها والإبلاغ عنها ومراقبتها بالنسبة للبنك، حيث أن حوكمة المخاطر وثقافة المخاطر القوية أمران حاسمان. هذه تتطلب توعية قوية من البنك. وأن يكون المحافظين وأعضاء مجلس الإدارة على دراية بالمخاطر المتعلقة بالأمن السيبراني التي تديرها البنك، وكيف أن هناك حاجة واضحة لإطار عمل لإدارة المخاطر السيبرانية. ويشمل ذلك الوصول إلى موظفي البنك المركزي وتدريبهم (لا يقتصر على المشرفين ومتخصصي تكنولوجيا المعلومات - على الرغم من أن برنامج التدريب على التكنولوجيا المالية وإدارة المخاطر وتدريب موحد ومتسق ومركّز على التكنولوجيا والالكترونية)، بالإضافة إلى تعزيز فهم أعضاء مجلس الإدارة أنفسهم لتطورات التكنولوجيا المالية على مستوى أكثر دقة، حيث أن إدارة المخاطر يجب أن تأخذ في الحسبان دمج العاملين السيبرانيين في فرق إدارة الأزمات.

الدراسة الميدانية:

أولاً: منهج الدراسة:

تم استخدام المنهج الوصفي التحليلي في إجراء الدراسة لكونه من أكثر المناهج استخداماً في الدراسات الاجتماعية والإنسانية، وكذلك تم استخدام المصادر الثانوية والتي تشمل الأبحاث التي كتبت في موضوع الدراسة، وكذلك ما تم نشره من أبحاث علمية ومقالات في الدوريات المتخصصة وكذلك

القوانين والتشريعات المرتبطة بموضوع الدراسة. وفيما يتعلق بالمصادر الأولية اعتمد الباحثان على استبانة تم تصميمها وتوزيعها خصيصاً لغرض الدراسة، وكذلك تم تفريغ الاستبانة من خلال استخدام برنامج SPSS الإحصائي، كما تم حساب الاختبارات الإحصائية المناسبة والضرورية لموضوع الدراسة.

ثانياً: مجتمع وعينة الدراسة:

1. **مجتمع الدراسة:** بلغ مجتمع الدراسة (120) مدراء عامين، ومدراء الفروع، ومدراء الدوائر المالية، ومدراء إدارات المخاطر في البنوك المدرجة في بورصة فلسطين.

2. **عينة الدراسة:** تم توزيع الاستبانة على عينة عشوائية بلغت (90) مدراء عامين، ومدراء الفروع، ومدراء الدوائر المالية، ومدراء إدارات المخاطر في البنوك المدرجة في بورصة فلسطين، وكانت النتائج على النحو التالي:

المتغير	البيان	العدد	النسبة المئوية
المؤهل العلمي	بكالوريوس	70	%77.8
	ماجستير	17	%18.9
	دكتوراه	3	%3.3
	المجموع	90	%100.0
المسمى الوظيفي	مدير عام	20	22.3
	مدير فرع	31	34.5
	مدير مالي	22	24.5
	مدير دائرة المخاطر	17	18.9
	المجموع	90	%100.0
سنوات الخبرة	أقل من 5 سنوات	13	%14.4
	5-10 سنوات	17	%18.9
	10-15 سنة	33	%36.7
	أكثر من 15 سنوات	27	%30.0
	المجموع	90	%100

ثالثاً: أداة الدراسة:

لقد تم تقسيم الاستبانة إلى جزأين كما يلي:

- **الجزء الأول:** ويتكون من البيانات الديمغرافية لعينة الدراسة ويتكون من 3 فقرات.
- **الجزء الثاني:** ويتناول أثر إدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك، وقد تم تقسيم هذه الاستبانة إلى ثلاثة محاور.

وقد اعتمد الطالبان على المقياس الخماسي للإجابة عن الفقرات ، حسب ما هو موضح في الجدول رقم (2).

جدول رقم (2) مقياس ليكرت الخماسي

التصنيف	موافق بدرجة كبيرة جدا	موافق بدرجة كبيرة	محايد	غير موافق	غير موافق بدرجة كبيرة
الدرجة	5	4	3	2	1

رابعاً:

صدق الاتساق الداخلي:

يقصد بصدق الاتساق الداخلي مدى اتساق كل فقرة من فقرات الاستبانة مع المجال الذي تنتمي إليه هذه الفقرة، وقد قام الطالبان بحساب الاتساق الداخلي للاستبانة وذلك من خلال حساب معاملات الارتباط بين كل فقرة من فقرات مجالات الاستبانة والدرجة الكلية للمجال نفسه.

جدول (3) معامل الارتباط بين كل فقرة من فقرات المجال الأول (إدارة مخاطر الأمن السيبراني ودعم الاستقرار المالي) والدرجة الكلية للمجال

الرقم	الفقرة	معامل الارتباط سبيرمان	القيمة الاحتمالية (Sig)
1	تؤدي مخاطر الأمن السيبراني إلى اختراقات للبيانات التي تتم من خلالها الوصول إلى معلومات سرية عن أعمال البنك.	0.60	دالة عند مستوى دلالة 0.05
2	تدرك إدارة البنك أن مخاطر أمن المعلومات يمكن أن تزعزع الاستقرار المالي وتحقق خسائر مالية يمكن أن يتكبدها البنك.	0.74	دالة عند مستوى دلالة 0.05
3	يقوم البنك بضبط المخاطر السيبرانية وتخفيف الأثر المالي والتحوط منها من خلال وضع الإجراءات والتدابير للأمن السيبراني بهدف دعم الاستقرار المالي له.	0.81	دالة عند مستوى دلالة 0.05
4	يوجد فريق للاستجابة لحوادث الأمن السيبراني على مستوى البنك بما يساهم في تكثيف الجهود للاستغلال الأمثل للطاقت لتطوير منظومة الأمن السيبراني لتعزيز الاستقرار المالي للبنك.	0.55	دالة عند مستوى دلالة 0.05
5	يصدر البنك تعليمات لكيفية إدارة المخاطر السيبرانية، ووضع السياسات لإدارة أمن المعلومات والأمن السيبراني.	0.69	دالة عند مستوى دلالة 0.05
6	يعتبر إدماج المخاطر السيبرانية بصورة أفضل في تحليل الاستقرار المالي من شأنه تحسين القدرة على فهم المخاطر على	0.66	دالة عند مستوى دلالة 0.05

		مستوى النظام وتخفيف حدتها.	
7	يؤدي تقليل المخاطر النظامية المرتبطة بالبنك إلى دور إيجابي على الاستقرار المالي.	0.68	دالة عند مستوى دلالة 0.05

* الارتباط دال إحصائياً عند مستوى دلالة $\alpha = 0.05$.

يوضح جدول (3) معامل الارتباط بين كل فقرة من فقرات المجال الأول والدرجة الكلية للمجال، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوى معنوية ($\alpha = 0.05$) وبذلك يعتبر المجال صادقاً لما وضع لقياسه.

جدول (4) معامل الارتباط بين كل فقرة من فقرات المجال الثاني (إدارة مخاطر الأمن السيبراني ودعم الشمول المالي) والدرجة الكلية للمجال

الرقم	الفقرة	معامل الارتباط سبيرمان	القيمة الاحتمالية (Sig)
1	يقوم البنك بالتصدي للمخاطر السيبرانية من خلال توفير بيئة مناسبة للأمن السيبراني بهدف دعم الشمول المالي.	0.74	دالة عند مستوى دلالة 0.05
2	يقوم البنك بإعداد وتصميم معالجات للمخاطر السيبرانية تتم من خلال تحديد مصادر بداية هذه المخاطر واحتمالية حدوثها.	0.80	دالة عند مستوى دلالة 0.05
3	يقوم البنك بإعداد خطة لإدارة المخاطر السيبرانية والتي تتضمن تحديد المهام وزيادة سرعة الاستجابة للهجمات السيبرانية والتعافي منها في زمن قياسي، مما يعزز الشمول المالي.	0.86	دالة عند مستوى دلالة 0.05
4	يقوم البنك بالتغلب على المخاطر السيبرانية الناجمة عن التحول المتزايد إلى رقمنة العمليات المالية.	0.67	دالة عند مستوى دلالة 0.05
5	يقوم البنك بزيادة التركيز على تعزيز الوعي بالأمن السيبراني بين موظفيه.	0.69	دالة عند مستوى دلالة 0.05
6	يقوم البنك بتطوير أطر الرقابة والاستجابة الفعالة للمخاطر السيبرانية، بما في ذلك ضمان تنفيذ ممارسات إدارة المخاطر العامة السليمة المتعلقة بالمخاطر السيبرانية.	0.71	دالة عند مستوى دلالة 0.05
7	يقوم البنك بعقد دورات تدريبية لموظفيه تتعلق بالأمن السيبراني والشمول المالي.	0.60	دالة عند مستوى دلالة 0.05

* الارتباط دال إحصائياً عند مستوى دلالة $\alpha = 0.05$.

يوضح جدول (4) معامل الارتباط بين كل فقرة من فقرات المجال الثاني والدرجة الكلية للمجال، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوى معنوية ($\alpha = 0.05$) وبذلك يعتبر المجال صادقاً لما وضع لقياسه.

جدول (5) معامل الارتباط بين كل فقرة من فقرات المتغير المستقل (مخاطر الأمن السيبراني) والدرجة الكلية للمجال

الرقم	الفقرة	معامل الارتباط سبيرمان	القيمة الاحتمالية (Sig)
1	تعد الخدمات المالية الإلكترونية في البنك من أكثر الخدمات التي تتعرض للمخاطر المتعلقة بالأمن السيبراني.	0.64	دالة عند مستوى دلالة 0.05
2	تعتبر البرامج الضارة واحدة من أكثر التقنيات المستخدم في تحقيق الهجمات السيبرانية.	0.79	دالة عند مستوى دلالة 0.05
3	يقوم البنك بوضع خطط للتعامل مع أي خطر سيبراني يهدد معاملاته الإلكترونية في المستقبل وكيفية التعامل معه.	0.72	دالة عند مستوى دلالة 0.05
4	يقوم البنك بالاعتماد على المعايير والأطر الدولية المعروفة في إدارة المخاطر للتحوط للمخاطر السيبرانية.	0.67	دالة عند مستوى دلالة 0.05
5	يعمل البنك بشكل مستمر على تطوير وتحديث خطط استمرارية العمل بحيث تأخذ بالاعتبار الهجمات السيبرانية.	0.81	دالة عند مستوى دلالة 0.05
6	يقوم البنك بتقييم مخاطر الأمن السيبراني باستمرار لحماية بياناته من الوصول غير المصرح به أو التدمير.	0.80	دالة عند مستوى دلالة 0.05
7	تقدم إدارة المخاطر لإدارة البنك تقرير يشتمل على معلومات هامة حول المخاطر السيبرانية.	0.76	دالة عند مستوى دلالة 0.05
8	يقوم البنك بوضع إجراءات فعالة للحد من المخاطر السيبرانية لحماية عملائه.	0.75	دالة عند مستوى دلالة 0.05

* الارتباط دال إحصائياً عند مستوى دلالة $\alpha = 0.05$.

يوضح جدول (5) معامل الارتباط بين كل فقرة من فقرات المتغير التابع والدرجة الكلية للمجال، والذي يبين أن معاملات الارتباط المبينة دالة عند مستوي معنوية ($\alpha = 0.05$) وبذلك يعتبر المجال صادقاً لما وضع لقياسه.

الصدق البنائي:

يعتبر الصدق البنائي أحد مقاييس صدق الأداة الذي يقيس مدى تحقق الأهداف التي تريد الأداة الوصول إليها، ويبين مدى ارتباط كل مجال من مجالات الدراسة بالدرجة الكلية لفقرات الاستبانة. وللتحقق من الصدق البنائي قام الطالبان بحساب معاملات الارتباط بين درجة كل مجال من مجالات الاستبانة والمجالات الأخرى، وكذلك درجة كل مجال بالدرجة الكلية للاستبانة كما في جدول (6).

جدول (6) معامل الارتباط بين درجة كل مجال من مجالات الاستبانة والدرجة الكلية للاستبانة

الرقم	المجال	معامل الارتباط سبيرمان	القيمة الاحتمالية (sig)
1	الاستقرار المالي	0.71	دالة عند مستوى دلالة 0.05
2	الشمول المالي	0.76	دالة عند مستوى دلالة 0.05
3	مخاطر الأمن السيبراني	0.74	دالة عند مستوى دلالة 0.05

الدرجة الكلية	0.73	دالة عند مستوى دلالة 0.05
---------------	------	---------------------------

* الارتباط دال إحصائياً عند مستوى دلالة $\alpha = 0.05$.

يتضح من جدول (6) أن جميع معاملات الارتباط في جميع مجالات الاستبانة دالة إحصائياً وبدرجة قوية عند مستوى معنوية ($\alpha = 0.05$) وبذلك تعتبر جميع مجالات الاستبانة صادقة لما وضعت لقياسه.

أ- طريقة التجزئة النصفية (Spilt-half):

حيث تم تجزئة فقرات الاستبانة إلى جزأين (الفقرات ذات الأرقام الفردية ، والفقرات ذات الأرقام الزوجية) ثم تم حساب معامل الارتباط بين درجات الفقرات الفردية ودرجات الفقرات الزوجية وبعد ذلك تم تصحيح معامل الارتباط بمعادلة سبيرمان براون Spearman Brown:

معامل الارتباط المعدل = $\frac{2r}{1+r}$ حيث r معامل الارتباط بين درجات الفقرات الفردية ودرجات الفقرات الزوجية . وتم الحصول على النتائج الموضحة في جدول (7).

جدول (7) طريقة التجزئة النصفية لقياس ثبات الاستبانة

م	المجال	معامل الارتباط سبيرمان	معامل الارتباط سبيرمان المعدل
1	الاستقرار المالي	0.71	0.83
2	الشمول المالي	0.75	0.86
3	مخاطر الأمن السيبراني	0.76	0.87
	جميع المجالات	0.74	0.85

النتائج والتوصيات

أولاً: النتائج

توصلت الدراسة إلى النتائج التالية:

1. يوجد أثر لإدارة مخاطر الأمن السيبراني على دعم الاستقرار والشمول المالي في البنوك المدرجة في بورصة فلسطين.
2. تدرك إدارة البنوك المدرجة في بورصة فلسطين أن مخاطر الأمن السيبراني واختراقات البيانات يمكن أن تزعزع الاستقرار المالي وتحقق خسائر مالية يمكن أن تتكبدها البنوك.
3. تقوم البنوك المدرجة في بورصة فلسطين بضبط المخاطر السيبرانية وتخفيف الأثر المالي والتحوط منها من خلال وضع الإجراءات والتدابير للأمن السيبراني بهدف دعم الاستقرار المالي له.
4. يوجد فريق للاستجابة لحوادث الأمن السيبراني في البنوك المدرجة في بورصة فلسطين ليساهم في تكثيف الجهود للاستغلال الأمثل للطاقات، وتطوير منظومة الأمن السيبراني لتعزيز الاستقرار المالي للبنوك.
5. تقوم البنوك المدرجة في بورصة فلسطين بإعداد وتصميم معالجات للمخاطر السيبرانية تتم من خلال تحديد مصادر بداية هذه المخاطر واحتمالية حدوثها.
6. تقوم البنوك المدرجة في بورصة فلسطين بالتصدي للمخاطر السيبرانية من خلال توفير بيئة مناسبة للأمن السيبراني بهدف دعم الشمول المالي.
7. تقوم البنوك المدرجة في بورصة فلسطين بإعداد خطط ووضع السياسات لإدارة المخاطر السيبرانية والتي تتضمن تحديد المهام وزيادة سرعة الاستجابة للهجمات السيبرانية والتعافي منها في زمن قياسي، مما يعزز الاستقرار والشمول المالي.

8. تقوم البنوك المدرجة في بورصة فلسطين بالاعتماد على المعايير والأطر الدولية المعروفة في إدارة المخاطر للتحوط للمخاطر السيبرانية.

9. تقدم إدارة المخاطر لإدارات البنوك المدرجة في بورصة فلسطين تقرير يشتمل على معلومات هامة حول المخاطر السيبرانية، والإجراءات الفعالة للحد منها لحماية عملائها.

ثانياً: التوصيات

1. على البنوك المدرجة في بورصة فلسطين ضرورة اتخاذ إجراءات للأمن السيبراني لضمان سلامة ومثانة نظم المعلومات المالية والإدارية والحفاظ على الاستقرار والشمول المالي وبما يحقق أهدافها.

2. على البنوك المدرجة في بورصة فلسطين ضرورة أن تقوم بزيادة التوعية بأهمية وأهداف الاستقرار والشمول المالي ودورهما في تحقيق الرفاهية للعملاء والمجتمع من خلال خفض الوقت والجهد والتكلفة في تأدية الخدمات والذي يعدا مثلث جودة تقديم أي خدمة.

3. ضرورة وضع نماذج فعالة لإدارة المخاطر السيبرانية المصاحبة لتكنولوجيا المعلومات وهو ما يتطلب الرقابة المستمرة لتحديد هذه المخاطر التي قد تهدد الاستقرار المالي في القطاع المصرفي.

4. ضرورة عقد الدورات التدريبية ورش العمل في مجال الأمن السيبراني وتكنولوجيا المعلومات بمشاركة العاملين بالبنوك المدرجة في بورصة فلسطين.

المراجع:

1. Bolzani, J. (2022). Leading the Way in Payments: How Central Banks Are Using Innovation to Promote Financial Inclusion and Reshape Competition. Forthcoming, Journal of Law and Commerce of the University of Pittsburgh School of Law, 41.
2. Curti, F., Gerlach, J., Kazinnik, S., Lee, M. J., & Mihov, A. (2019). Cyber risk definition and classification for financial risk management. Federal Reserve Bank of St Louis, August, mimeo.
3. Eisenbach, T. M., Kovner, A., & Lee, M. J. (2022). Cyber risk and the US financial system: A pre-mortem analysis. Journal of Financial Economics, 145(3), 802-826.
4. Herrera Luque, F. J., Munera López, J., & Williams, P. (2021). Cyber risk as a threat to financial stability. Revista de Estabilidad Financiera/Banco de España, primavera 2021..
5. Huang, K., & Madnick, S. (2020). Cyber securing cross-border financial services: calling for a financial cybersecurity action task force. Available at SSRN 3544325.

6. Inoussa, H. (2021). The FinTech-driven Approach to Financial Inclusion: A cross-sectional study of how Financial Inclusion furthers Sustainable Development in Sub-Saharan Africa.
7. Jayakumar, S. (2020). Cyber Attacks by Terrorists and other Malevolent Actors: Prevention and Preparedness. *Handbook of Terrorism Prevention and Preparedness*, 871-930.
8. Khan, M. A., & Malaika, M. (2021). Central Bank Risk Management, Fintech, and Cybersecurity. *International Monetary Fund*.
9. Kumar, R., & Thomas, B. (2022). BRICS in Global Governance: A Gradual but Steady Expansion. *Governance and Politics*, 1(1), 100-113.
10. Piotrowski, D. (2022). Consumer perceived ethicality of banks in the era of digitalisation: The case of Poland. *Economics and Business Review*, 8(1), 90-114.
11. Pupentsova, S., & Livintsova, M. (2022). The Enterprises Risk Management in the Context of Digital Transformation. In *International Scientific Siberian Transport Forum* (pp. 1159-1167). Springer, Cham.
12. Saon Raya, S. P., & Miglanic, S., (2019), Use of Blockchain and Artificial Intelligence to promote financial inclusion in India. *TECH MONITOR* • Jan-Mar 2019.
13. Tzoneva, A., Momcheva, G., & Stoyanov, B. (2022, May). Vendor Cybersecurity Risk Assessment in an Autonomous Mobility Ecosystem. In *2022 10th International Scientific Conference on Computer Science (COMSCI)*.
14. Uddin, M. H., Mollah, S., & Ali, M. H. (2020). Does cyber tech spending matter for bank stability?. *International Review of Financial Analysis*, 72, 101587.
15. Varga, S., Brynielsson, J., & Franke, U. (2021). Cyber-threat perception and risk management in the Swedish financial sector. *Computers & security*, 105, 102239.
16. Vučinić, M. (2020). Fintech and Financial Stability Potential Influence of FinTech on Financial Stability, Risks and Benefits. *Journal of Central Banking Theory and Practice*, 9(2), 43-66.
17. Welburn, J. W., & Strong, A. M. (2022). Systemic cyber risk and aggregate impacts. *Risk Analysis*, 42(8), 1606-1622.
18. Yadav, M., & Shanmugam, S., (2022), Fintech Lending in India: the Changing Paradigm of Banking, *Journal of the Oriental Institute*, ISSN: 0030-5324, UGC Care list no. 135, 71(15), 225-232.