أثر المخاطر السيبرانية على الاستقرار المصرفي في ظل التحول الرقمي

أ. سالمة عمر محمد مسعود
قسم العلوم الإدارية والمالية، المعهد العالي للعلوم والتقنية سوق الخميس امسيحل

الملخص:

يدرس هذا البحث إشكاليةً أصبحت تشغل صانعي القرار المصرفي والهيئات الرقابية الدولية، وهي العلاقة بين التحول الرقمي في القطاع المصرفي والمخاطر السيبرانية الناشئة عنه، وانعكاساتها على مؤشرات الاستقرار المصرفي. يعتمد البحث المنهج الوصفي التحليلي من خلال استقراء الأدبيات الأكاديمية وتقارير المؤسسات المالية الدولية الكبرى كصندوق النقد الدولي ولجنة بازل وبنك التسويات الدولية.

تكشف نتائج البحث أن البنوك تجد نفسها أمام معضلة مزدوجة: التأخر في التحول الرقمي يُضعف قدرتها التنافسية، والإسراع فيه دون تعزيز الأمن السيبراني يكشف بنيتها التحتية لهجمات متصاعدة التعقيد. وتعمل المخاطر السيبرانية على تهديد الاستقرار المصرفي عبر ثلاث قنوات رئيسية: قناة السيولة من خلال تعطل أنظمة الدفع وما يُفرزه من ذعر مصرفي رقمي متسارع، وقناة السمعة والثقة التي تُؤثر في استدامة الودائع وعلاقات المراسلة الدولية، وقناة التكاليف المالية المباشرة وغير المباشرة التي تنتقص من رأس المال التنظيمي. وعلى المستوى النظامي، يُنبّه البحث إلى خطورة العدوى السيبرانية المترتبة على الاعتماد المشترك على مزودي خدمات تقنية محوريين. وعلى الرغم من الجهود التنظيمية الدولية الجادة، تظل فجوات واسعة قائمةً في الاقتصادات الناشئة والنامية. ويوصي البحث ببناء أُطر رقابية وطنية متخصصة، وتعزيز حوكمة الأمن السيبراني على مستوى مجالس الإدارة، واعتماد ثقافة الأمان منذ مراحل تصميم الخدمات الرقمية.

الكلمات المفتاحية :التحول الرقمي، المخاطر السيبرانية، الاستقرار المصرفي، المرونة التشغيلية، الذعر المصرفي الرقمي، العدوى

The Impact of Cyber Risks on Banking Stability in the Context of Digital Transformation

This paper examines a growing concern among banking policymakers and international regulatory bodies: the relationship between digital transformation in the banking sector and the emerging cyber risks it generates, and how these risks affect banking stability indicators. The study adopts a descriptive-analytical approach, drawing on academic literature and reports from major international financial institutions, including the IMF, the Basel Committee on Banking Supervision, and the Bank for International Settlements.

The findings reveal that banks face a structural dilemma: lagging in digital transformation erodes their competitive position, while accelerating it without adequate cybersecurity reinforcement exposes their infrastructure to increasingly sophisticated attacks. The study identifies three primary transmission channels through which cyber risks threaten banking stability: the liquidity channel, through payment system disruptions and the accelerated dynamics of digital bank runs; the reputation and trust channel, which affects deposit sustainability and correspondent banking relationships; and the direct and indirect financial cost channel, which erodes regulatory capital and profitability. At the systemic level, the paper highlights the significant threat of cyber contagion stemming from shared reliance on critical third-party technology providers. Despite meaningful progress in international regulatory frameworks, substantial gaps persist particularly in emerging and developing economies. The paper recommends establishing specialized national cybersecurity regulatory frameworks, strengthening board-level cyber governance, and embedding security-by-design principles throughout the digital service development lifecycle.

Keywords: Digital Transformation, Cyber Risk, Banking Stability, Operational Resilience, Digital Bank Run, Cyber Contagion, Basel Committee, International Monetary Fund.

المقدمة

منذ جائحة كوفيد–19 عام 2020، بدأت البنوك تعيد هندسة نفسها كلياً؛ تتخلى عن نماذج أعمال قديمة معمول بها منذ عقود، وتستبدلها بمنصات رقمية مفتوحة، وخدمات مصرفية عبر الهاتف المحمول، وأنظمة دفع فورية معتمدة على الذكاء الاصطناعي، وواجهات برمجة مفتوحة تتيح التكامل مع شركات التقنية المالية، هذا التحول منح البنوك مستويات مرتفعة من الكفاءة والانتشار وتحسين تجربة العميل، إلا أنه في المقابل زاد بصورة كبيرة من عدد الثغرات والمنافذ الرقمية المعرضة للهجمات السيبرانية.

أصبح الاستقرار المصرفي، الذي كان يُنظر إليه في السابق على أنه مرتبط أساسًا بعوامل اقتصادية مثل أسعار الفائدة وجودة الأصول ومستوى رأس المال، يواجه اليوم نوعًا جديدًا من التهديدات يتمثل في المخاطر السيبرانية. فهذه التهديدات لا ترتبط بالتقلبات الاقتصادية التقليدية ولا يمكن التنبؤ بها من خلال المؤشرات المالية المعتادة، بل تظهر بشكل مفاجئ عبر استهداف الأنظمة التقنية والتشغيلية للبنوك، الأمر الذي قد يحوّل مشكلة تشغيلية بسيطة إلى أزمة مالية واسعة. وقد أشارت هيئات دولية

كبرى كصندوق النقد الدولي، إلى أن مخاطر الخسائر الجسيمة الناجمة عن الحوادث السيبرانية قد تضاعفت أربع مرات منذ عام 2017، لتبلغ عتبة 2.5 مليار دولار في الحوادث المباشرة الفردية، فضلاً عن تداعيات غير مباشرة يصعب قياسها كاملاً (International Monetary Fund [IMF], 2024).

ينطلق هذا البحث من فكرة أن العلاقة بين المخاطر السيبرانية والاستقرار المصرفي أصبحت قضية ضرورية تفرضها طبيعة العمل المصرفي الحديثة. باعتبار أن البنوك اليوم تعتمد بشكل كبير على الأنظمة الرقمية والخوادم والبرامج الذكية في إدارة عملياتها، إلى درجة أصبحت فيها التكنولوجيا تمثل الأساس الذي يقوم عليه النشاط المصرفي. ومع هذا الترابط الكبير بين المؤسسات المالية، فإن أي هجوم سيبراني قد يستهدف بنكًا مهمًا يمكن أن يمتد تأثيره بسرعة إلى أنظمة الدفع والتسوية وبقية المؤسسات المرتبطة به، مما قد يسبب اضطرابات واسعة في القطاع المالي.

مشكلة البحث

تتمثل مشكلة هذا البحث في الفجوة بين السرعة المتضاعفة للتوسع الرقمي في القطاع المصرفي، والقصور الواضح في القدرة على كبح المخاطر السيبرانية الناشئة عن هذا التوسع.

ففي حين تسابق البنوك الزمن لتبني أحدث التقنيات وتقديم خدماتها عبر المنصات الرقمية، تكشف المؤشرات أن منظومات الحوكمة الأمنية وأطر إدارة المخاطر السيبرانية لم تواكب هذه القفزة بالسرعة ذاتها، مما يُفضي إلى بنى تحتية رقمية مكشوفة ومعرضة لتهديدات تزداد تطوراً وتعقيداً كل يوم (Saeed et al., 2023).

ومما يزيد الإشكالية تعقيداً أن آليات انتقال الأثر من الحادث السيبراني إلى الاستقرار المصرفي لا تزال غير محددة المعالم بصورة كافية في الأدبيات الأكاديمية العربية، رغم أن الهيئات الدولية كصندوق النقد الدولي ولجنة بازل للرقابة المصرفية باتت تُولي هذه المسألة عناية تحليلية متزايدة. وعليه، تسعى هذه الدراسة إلى تشريح هذه العلاقة وملء شيء من هذه الفجوة المعرفية.

أسئلة البحث

يسعى هذا البحث إلى الإجابة عن الأسئلة البحثية الآتية:

1- ما واقع التحول الرقمي والمخاطر السيبرانية الناشئة عنه في البيئة المصرفية الحديثة، وما أبرز أبعادهما ومكوناتهما؟
2- ما القنوات الرئيسية التي تنتقل عبرها آثار المخاطر السيبرانية إلى مؤشرات الاستقرار المصرفي على المستويين الفردي والنظامي؟
3- كيف تُعالج الأطر التنظيمية الدولية، وبالأخص مبادئ لجنة بازل وتوجيهات صندوق النقد الدولي وبنك التسويات الدولية، إشكالية بناء المرونة السيبرانية للمنظومة المصرفية؟

أهداف البحث

تسعى هذه الدراسة بشكل رئيسي إلى تحقيق الأهداف التالية:

1- بناء إطار مفاهيمي متكامل يوضح المصطلحات الأساسية المتعلقة بالتحول الرقمي والمخاطر السيبرانية والاستقرار المصرفي، والمساهمة في تقليل الغموض القائم في تعريفاتها ضمن الأدبيات الأكاديمية.
2- تحليل القنوات النظرية التي تنتقل من خلالها الصدمات السيبرانية إلى الاستقرار المصرفي، لتوضيح طبيعة هذا الارتباط وآلياته بشكل أدق.
3- استعراض الأطر التنظيمية الدولية وتقييم مدى كفايتها في مواجهة التهديدات السيبرانية المتطورة.

أهمية البحث

يكتسب هذا البحث أهميته من خلال:

أولاً: الأهمية العلمية:

يسهم هذا البحث في إثراء المكتبة الأكاديمية العربية في مجال يشهد اهتمام دولي متزايد، لكنه ما يزال يعاني من محدودية الابحاث باللغة العربية. إذ تتسم معظم الدراسات العربية المتاحة بطابع وصفي عام، دون التعمق في التحليل النظري لمسارات انتقال الأثر السيبراني وانعكاساته المالية. كما يسعى البحث إلى تقليص الفجوة بين الأدبيات الأجنبية الغنية في هذا المجال وبين القارئ العربي المتخصص، من خلال تقديم معالجة تحليلية أكثر عمقًا وارتباطًا بالسياق الأكاديمي العربي.

ثانياً: الأهمية العملية:

تكمن في توجيه صانعي القرار داخل المؤسسات المصرفية وهيئات الرقابة نحو فهم أعمق للمخاطر السيبرانية كخطر حقيقي ليس مجرد مشكلة تقنية عابرة، وفي تزويد المدراء وأعضاء مجالس الإدارة بالمعرفة اللازمة لإقامة منظومات حوكمة سيبرانية فاعلة تحمي استقرار مؤسساتهم وتحمي معه ثقة المودعين والجمهور.

منهجية البحث

يعتمد هذا البحث المنهج الوصفي التحليلي، من خلال الاستقراء النظري للأدبيات الأكاديمية من دراسات وأوراق بحثية محكّمة، والتحليل التفسيري لتقارير المؤسسات المالية الدولية الكبرى كصندوق النقد الدولي ولجنة بازل للرقابة المصرفية وبنك التسويات الدولية، بما تتضمنه من إحصاءات وبيانات وحالات تحليلية تُسعف في تحليل ظاهرة المخاطر السيبرانية وتداعياتها بصورة أعمق وأكثر دقة.

الفصل الثاني: التحول الرقمي والمخاطر السيبرانية في القطاع المصرفي

المبحث الأول: مفهوم وأبعاد التحول الرقمي

أولا: مفهوم التحول الرقمي

يعرف التحول الرقمي "بدمج العمليات الجديدة داخل المؤسسة مثل اعتماد التقنيات الجديدة والأدوات وأساليب العمل المتصلة بالإنترنت، بالإضافة إلى تنظيم داخلي جديد يجب أن تدعمه الإدارة العليا" (كريمة، وبن قيدة، 2023، ص. 5).

وعلى صعيد المؤسسات أو الحكومات يمكن تعريفه بأنه "أي إجراء تغييرات جذرية تطال نموذج العمل والإجراءات والعمليات، وقد يطال التحول عملية تغيير المنتج أو طريقة تقديم الخدمة كليا، وقد يكون استراتيجيا بالتدخل في وظائف المؤسسة كلها من المبيعات إلى التوريد وتقنية المعلومات وكل سلسلة القيمة" (عمر، 2021، ص 158).

ثانيا: الركائز التقنية الحديثة للتحول الرقمي

فيما يلي أبرز النقاط التي يعتمد عليها التحول الرقمي في القطاع المصرفي، والتي تمكّن البنوك من تطوير خدماتها وتحسين كفاءتها:

1- **الذكاء الاصطناعي والتعلم الآلي:** تعتمد البنوك على هذه التقنيات في مجالات كثيرة، من إدارة مخاطر الائتمان وكشف الاحتيال المالي إلى تخصيص الخدمات وتحسين تجربة العميل، حيث تُظهر الدراسات دور التحول الرقمي في البنوك أن الذكاء الاصطناعي والتعلّم الآلي أصبحا أساسيين في التحليلات التنبؤية، كشف الاحتيال، وتقديم خدمات مخصّصة تعتمد على معالجة كميات كبيرة من البيانات بدقة وسرعة تفوق القدرات البشرية العادية (Munira, 2025).
2- **الحوسبة السحابية:** انتقلت الكثير من البنوك من نماذج الخوادم المحلية إلى الاعتماد الواسع على البنى السحابية العامة والخاصّة والهجينة، حيث تُظهر الدراسات أن البنية السحابية تُعد من العناصر الرئيسية للتحول الرقمي المصرفي من خلال توفير مرونة عالية في الموارد، دعم التوسّع السريع، وخفض تكاليف البنية التحتية، مع بروز تحديات تتعلق بالأمن والامتثال والاعتماد على مزوّدي خدمات من أطراف ثالثة (Munira, 2025).
3- **واجهة برمجة التطبيقات المفتوحة (Open APIs):** أدّت الأطر التنظيمية الحديثة في الأنظمة المالية المتقدمة إلى دفع البنوك نحو فتح واجهات برمجة التطبيقات الخاصة بها وربطها بمزوّدي الخدمات المالية والتقنية الخارجيين، وهو ما أسهم في نشوء بيئة مصرفية مفتوحة تعزّز الابتكار والتكامل بين البنوك وشركات التكنولوجيا المالية من خلال واجهات APIs معيارية وآمنة. وهذا التطور زاد من تعقيد بيئة المدفوعات، وفرض متطلبات أعلى تتعلق بالحوكمة والأمن السيبراني لضمان حماية البيانات وسلامة المعاملات (Braine & Shukla, 2022).
4- **تقنيات البلوكتشين والعملات الرقمية للبنوك المركزية (CBDCs):** رغم أن توظيف تقنية البلوكتشين في الخدمات المصرفية التجارية ما يزال في طور التطوير والتجريب، فإن البحوث توضح أن عدداً متزايداً من البنوك المركزية يختبر عملات رقمية سيادية قائمة على تقنيات الدفاتر الموزعة والبلوك تشين، بهدف بناء بنى تحتية رقمية للمدفوعات أكثر كفاءة وشفافية وأماناً، مع إمكان دمج قواعد البيانات المركزية بالدفاتر اللامركزية لزيادة الشفافية وتعزيز الرقابة على المعاملات وتقليل التكاليف (Tunzina et al., 2023).

ثالثا: دوافع ومزايا التحول الرقمي

يمتاز التحول الرقمي من خلال نتائج دراسات سابقة أجريت على القطاع المصرفي:

1- تحسين الكفاءة التشغيلية وتقليص التكاليف اليدوية وتسريع دورات إنتاج الخدمة: أظهرت النتائج التجريبية أن التحول الرقمي يمكن أن يُحسّن أداء البنوك، ويقلل من التأثير السلبي لدخول تقنيات جديدة، ويعزز خروج القنوات غير المتصلة بالإنترنت (Xie & Wang, 2023).
2- تعزيز الشمول المالي بتوسيع نطاق الوصول الجغرافي دون الحاجة إلى شبكة فروع مكلفة: تشير النتائج إلى أن التحول الرقمي أدى إلى تحسين الراحة وكفاءة الوقت وسهولة الوصول، مما عزز تجربة العملاء البنكية بشكل كبير (Sathwika et al., 2024).
3- ارتفاع سرعة اتخاذ القرارات الائتمانية وجودتها بفضل النمذجة الكمية المتقدمة: تُمكّن التقنيات الرقمية البنوك من جمع ومعالجة وتحليل كميات ضخمة من البيانات، ما يدعم اتخاذ قرارات ائتمانية أكثر دقة وسرعة (Munira, 2025).

كما تسعى الدول بمؤسساتها المختلفة إلى تعزيز التحول الرقمي في كافة القطاعات بهدف (الرضا، والموسوي, 2025):

1- تحسين الكفاءة.
2- تقليل الهدر.
3- تعزيز إمكانية الوصول إلى الموارد والخدمات.
4- تطوير الخدمات المقدمة للمواطنين.

المبحث الثاني: طبيعة المخاطر السيبرانية الناشئة

أولا: مفهوم المخاطر السيبرانية وتصنيفاتها

تُعرَّف المخاطر السيبرانية في السياق المصرفي بأنها احتمالية تعرُّض البنك لخسائر ناجمة عن أحداث تمس أنظمته الرقمية وبياناته وبنيته التحتية التقنية.

فقد تم تعريفه بأنه "كل ما يهدد الفضاء الالكتروني ويعرض سلامته ووظيفته للخطر" (قاضي، وزيتوني، 2025، ص. 3)

كما عرفه Gordon&Loeb بأنها "الاحتمالات التي تؤدي إلى فقدان البيانات أو تعطيل العمليات أو انتهاك الخصوصية أو تلف السمعة نتيجة الثغرات أو الهجمات على البنية التحتية الرقمية" (Gordon & Loeb, 2002, p. 443).

وتتعدد أصناف التهديدات السيبرانية التي تواجهها البنوك:

1- الهندسة الاجتماعية والتصيد الاحتيالي، من خلال خداع موظف أو عميل للإفصاح عن بيانات بشكل غير مباشر.
2- بمجريات الفدية، والتي وظيفتها تعطيل عمليات الأنظمة وتسريب البيانات.
3- هجمات حجب الخدمة، وذلك عبر اخراق خوادم المصرف المستهدف بكمية كبيرة من الطلبات الغير حقيقية عبر روبوتات حتى يعجز النظام عن تقديم الخدمات للمواطنين بسهولة.

ثانيا: مصادر التهديدات السيبرانية ومواطن الضعف

يمكن تصنيف مصادر التهديد السيبراني للبنوك عادة إلى:

- الجهات المنظمة التي تتحرك بدوافع مالية وتمتلك قدرات تقنية متقدمة.
- الجهات الحكومية أو المدعومة من الحكومة وتستهدف الأنظمة المالية في إطار صراعات جيوسياسية أو لأغراض التجسس الاقتصادي.
- تهديدات داخلية من قبل الموظفين.

وفي مقدمة مواطن الضعف الهيكلية التي تُفاقم هذا الخطر: الاعتماد المتزايد على مزودي خدمات التقنية من الطرف الثالث، فالبنوك الكبرى في العالم تُفوِّض اليوم عمليات ضخمة كالاستضافة السحابية وتطوير التطبيقات وإدارة أنظمة الدفع لمزودين خارجيين، مما يجعل نقاط الضعف في هؤلاء المزودين تُصبح تلقائياً نقاط ضعف في البنك المالكة، وقد رصد صندوق النقد الدولي أن ما يزيد على نصف مزودي خدمات تكنولوجيا المعلومات للبنوك ذات الأهمية النظامية حول العالم يخدمون مؤسستين

نظاميتين أو أكثر في وقت واحد، مما يُنشئ نقاط تركز تجعل الهجمة السيبرانية الواحدة قادرة على الانتشار بصورة متزامنة عبر كامل النظام المصرفي (IMF, 2024).

الفصل الثالث: الاستقرار المصرفي ومحدداته

المبحث الأول: مفهوم وأبعاد الاستقرار المصرفي

أولا: تعريف الاستقرار المصرفي

لا يوجد في الأدبيات الاقتصادية تعريف إجرائي موحد ومحدد للاستقرار المصرفي، ذلك أن المفهوم ذو طابع متعدد الأبعاد ومتداخل المستويات، فالاستقرار المصرفي يُستخدم غالباً ضمن مفهوم أوسع هو الاستقرار المالي للنظام المصرفي أو للبنك، وتقدِّم الأبحاث عدداً من الصياغات التعريفية الواضحة.

يعرف الاستقرار المالي للنظام المصرفي على أنه "خاصية معقّدة وديناميكية لحالته، تعكس قدرته على مقاومة الأزمات والمخاطر النظامية، وأداء وظائف الوساطة (التجميع، التوزيع، إعادة التوزيع، المدفوعات والتسويات)، والتأثير الإيجابي في التحولات الاقتصادية، والعودة إلى حالة توازن" (Bayik, 2025, P. 404).

ويُعرَّف استقرار البنك نفسه على أنه "قدرته طويلة الأجل على تنفيذ العمليات التقليدية والابتكارية، والوساطة في المدفوعات، والوفاء بالالتزامات، وتحقيق نتيجة مالية إيجابية مع مراعاة المخاطر الداخلية والخارجية" (Bayik, 2025, P. 404).

ثانيا: مؤشرات الاستقرار المصرفي

يعتبر نموذج CAMELS أحد أشهر أُطر تقييم السلامة المصرفية والأكثر انتشارا في أوساط المنظمين والمحللين الماليين. وهو اختصار للمكونات الستة التي يعتمدها في تقدير صحة البنك واستقراره، وتتمثل في:

1- كفاية رأس المال (Capital Adequacy).
2- جودة الأصول (Asset Quality).
3- جودة الإدارة (Management Quality).
4- الربحية (Earnings).
5- السيولة (Liquidity).
6- الحساسية لمخاطر السوق (Sensitivity to Market Risk).

ومن أكثر المؤشرات ارتباطا بالحوادث السيبرانية هو مؤشر كفاية رأس المال، الذي تُحدده لجنة بازل في اشتراط الحفاظ على الحد الأدنى للنسبة بين رأس المال الرقابي ومجموع الأصول الموزونة بالمخاطر. فحين يُحدث الحادث السيبراني خسائر تشغيلية مباشرة، فإنه ينتقص مباشرةً من رأس المال، مما قد يدفع البنك تحت الحدود التنظيمية المطلوبة بأسرع مما يتوقع. يُضاف إلى ذلك مؤشر السيولة، الذي يُعبّر عن قدرة البنك على الوفاء بالسحوبات المفاجئة، وهو ما يُختبر بصورة مباشرة حين يتسبب الهجوم السيبراني في حدوث موجة سحب جماعي للأموال مدفوعة بحالة من الهلع وفقدان الثقة لدى المودعين.

المبحث الثاني: ثقة المودعين وسمعة المؤسسة

أولا: العلاقة بين السمعة واستدامة الودائع

تُشكّل الثقة الركيزة الصامتة التي يرتكز عليها النظام المصرفي برمّته. فالودائع المصرفية في أساسها ليست سوى ائتمان يمنحه المودع للبنك، ائتمان قائم على القناعة بأن البنك قادر على رد الأموال عند الطلب. وهذه القناعة ليست مستقلة عن الصورة الذهنية العامة للبنك وسمعته المؤسسية في السوق، بل هي متشابكة معها بصورة وثيقة.

وتكشف الأدبيات المالية، ابتداءً من أعمال دياموند وديبفيغ (Diamond & Dybvig, 1983) الكلاسيكية في نظرية الذعر المصرفي، أن تشغيل قرار سحب الودائع الجماعي (Bank Run) لا يستلزم بالضرورة أن يكون البنك في حالة إعسار فعلي؛ يكفي أن يسود الاعتقاد بين المودعين بأن البنك مُعسر أو مُهدد، وهو اعتقاد يغذي نفسه ذاتياً حتى لو كان في مبدئه مبالغاً فيه. وهنا يكمن الأثر المدمر

للحوادث السيبرانية على السمعة: فهي تُطلق التشكيك وتُغذي عدم اليقين، مما يُهيئ البيئة المناسبة لبدء سيناريوهات السحب الجماعي.

ثانيا: الذعر المصرفي الرقمي في العصر الحديث

ظاهر الذعر المصرفي ليس بظاهرة جديدة ولكن التحول الرقمي أضاف بُعداً جديداً للظاهرة التقليدية، فبينما كان الذعر المصرفي في الحقبة ما قبل الرقمنة يتطلب وقتاً لانتشار المعلومات والتشاور الاجتماعي وطوابير الانتظار أمام الفروع، أصبحت الهواتف الذكية اليوم أداةً لتحويل الودائع بنقرة واحدة في أي مكان وزمان. وقد وصف دفّي وينغر (Duffie & Younger, 2019) في ورقتهما البحثية المعنونة بـ "Cyber Runs" السيناريو المخيف الذي يمكن فيه لتقارير موثوقة عن هجوم سيبراني على بنك كبير أن تُحرك مودعي بنوك أخرى نحو السحب المتزامن الفوري، فيما يُشبه عدوى ذعر تنتشر عبر الشبكة الرقمية بسرعة الضوء.

وعلى الرغم من أن الأدلة التجريبية على ذعر مصرفي رقمي واسع النطاق لا تزال محدودة حتى اللحظة، فإن البيانات الأمريكية تُظهر أدلة ذات دلالة إحصائية على حدوث تدفقات خروج مستمرة نسبياً للودائع من البنوك الأصغر حجماً إثر التعرض للحوادث السيبرانية، دون أن ترافق ذلك بالضرورة مخاوف جدية من حيث السلامة المالية للبنك (IMF, 2024). وتُعزز هذه النتائج المخاوف من احتمال تحوّل هذه التدفقات المحدودة إلى حالة ذعر واسعة، خاصة في حال حدوث أزمة سيبرانية كبيرة.

الفصل الرابع: قنوات انتقال أثر المخاطر السيبرانية إلى الاستقرار المصرفي

يتناول هذا الفصل الآليات التي يسلكها الحادث السيبراني في طريقه من كونه إخلالاً تشغيلياً فنياً إلى أن يتحول إلى صدمة مالية ذات أبعاد قد تطال استقرار البنك المفرد أو النظام المصرفي ككل. وخلافاً للتصور البسيط الذي يُختزل فيه الأثر في الأضرار المباشرة، يكشف التحليل النظري عن منظومة متعددة القنوات ومتداخلة التأثيرات.

المبحث الأول: تحول المخاطر السيبرانية إلى مخاطر مالية ونظامية

أولا: قناة مخاطر السيولة

قد تكون قناة السيولة من أسرع القنوات تأثيراً في نقل أثر الحادث السيبراني إلى الاستقرار المصرفي. وتعمل هذه القناة بجانبين: الجانب التشغيلي المباشر، والجانب السلوكي المرتبط بالذعر.

الجانب التشغيلي، يظهر حين يُعطّل الحادث السيبراني منظومة الدفع والتحويل في البنك، سواء بتشفير البيانات أو بضرب واجهات المستخدم وإيقاف قنوات الصرف الآلي والأنظمة الداخلية. في هذه الحالة يُصبح البنك عاجزاً مؤقتاً عن التقيد بالتزاماته اليومية حتى لو كانت ميزانيته العمومية سليمة ورأسماله كافياً؛ وهي حالة من الإعسار التشغيلي (Operational Insolvency) لا المالي. وقد رصد إيزنباخ وزملاؤه (Eisenbach et al., 2022) أن هجوماً مركزاً على البنوك الكبرى قادر نظرياً على تعطيل ما يقارب 31% من حجم شبكة المدفوعات بالجملة في الولايات المتحدة الأمريكية، مما يُنبئ بأثر اقتصادي كلي بالغ الخطورة يتجاوز حدود البنك المستهدف.

أما الوجه السلوكي لقناة السيولة، فيتمثل فيما يُفرزه الحادث من خوف لدى المودعين يدفعهم إلى تسريع طلبات السحب احتياطياً. وقد نبّه دفّي وينغر (Duffie & Younger, 2019) إلى أن المودعين الكبار من المؤسسات المالية والشركات هم أسرع من غيرهم في الاستجابة لهكذا مخاوف، نظراً لقدراتهم التقنية وسعة رقعة أموالهم المودعة. وحين يُسارع مودعو الجملة إلى سحب أموالهم، يستنزف البنك احتياطيات السيولة لديه بوتيرة قد تتجاوز قدرته على التكيف حتى مع وجود مرفق الإقراض من البنك المركزي بوصفه ملاذاً أخيراً.

ثانيا: قناة مخاطر السمعة والثقة

مخاطر السمعة والثقة الأكثر استدامة وتبقى حتى بعد معالجة الحادثة بفترة طويلة، فتسريب البيانات أو تعطل الخدمات لفترة تعيق عمل العملاء، ليس بالمر الهيّن لذا الزبائن، وتتوزع آثار هذه القناة على ثلاث مسارات:

المسار الأول (أثر القيمة السوقية): تُثبت الدراسات التجريبية أن البنوك المدرجة في البورصة تُسجل عادةً انخفاضاً في أسعار أسهمها إثر الإعلان عن الاختراقات السيبرانية الكبرى. فقد أظهرت دراسات Event Study أن الشركات المستهدفة تخسر في المتوسط نحو 309.33 مليون دولار يوم الإعلان عن الحادث، وتصل الخسائر التراكمية إلى 618.65 مليون دولار خلال ثلاثة أيام (The Dynamics of Stock Market Responses Following the Cyber-Attacks News, 2025). ويعكس هذا الانخفاض توقعات المستثمرين بما سيترتب من غرامات ومصاريف إصلاح وتراجع في الحصة السوقية (Kamiya et al., 2021)، وما يُثير المخاوف أن تراجع القيمة السوقية يُقلّص القيمة الدفترية لحقوق الملكية، وبالتالي يُضعف نسب رأس المال التنظيمية (Campbell et al., 2003; Gordon et al., 2011).

المسار الثاني (هجرة العملاء): حين يفقد العملاء الثقة في قدرة البنك على حماية بياناتهم وأموالهم، فإن جزءاً منهم يلتمس ملاذاً في بنوك أخرى تبدو أكثر أمانًا. وتُشير دراسة ميدانية طويلة المدى شملت 500,000 مستخدم إلى أن العملاء الذين تعرضت بياناتهم للاختراق كانوا أكثر عرضة بستة أضعاف لإنهاء علاقتهم مع البنك خلال ستة أشهر، حتى لو تم تعويضهم مالياً (Telang & Somanchi, 2016)، كما تشير استبيانات حديثة إلى أن نحو 67% من العملاء سيفكرون في تغيير البنك بعد اختراق خطير (Integris, 2026). ويُلاحظ أن هذا السلوك أكثر وضوحاً في شريحة المودعين المؤسسيين (wholesale depositors)، الذين يمتلكون وعياً مالياً أعلى وبدائل أيسر حضوراً وقدرات تقنية أعلى للاستجابة السريعة (Duffie & Younger, 2019).

المسار الثالث (تآكل علاقة بنك المراسلة): في النظام المصرفي المترابط دولياً، تعتمد البنوك في معاملاتها العابرة للحدود على شبكة من علاقات المراسلة مع بنوك أجنبية. ورغم أن الأدبيات التجريبية المباشرة التي تربط حادثاً سيبرانياً محدداً بإلغاء علاقة مراسلة لا تزال ناشئة، إلا أن ظاهرة *De-risking* (إلغاء علاقات المراسلة) مُثبتة تجريبياً، حيث انخفضت العلاقات النشطة عالمياً بنسبة 20% بين عامي 2012 و2019 (Gordon, 2019; Financial Stability Board, 2017)، وتشير تقارير المؤسسات الدولية إلى أن متطلبات الأمن السيبراني زادت من تكاليف الامتثال وجعلت علاقات المراسلة أقل جدوى (Congressional Research Service, 2022)، ومن المنطقي الاستنتاجي أن حادثاً سيبرانياً كبيراً قد يُسرّع من هذا التآكل، إذ إن البنوك المراسِلة قد تُقدّم احتياطاً على تضييق نطاق

التسهيلات الممنوحة أو تقليص حدود التسوية البينية، مما يُعرقل عمليات البنك المستهدف الدولية ويزيد تكاليف التمويل.

ثالثا: قناة التكاليف المالية المباشرة وغير المباشرة

التكاليف المباشرة: تشمل تكاليف الاستجابة الفورية للحادثة من استئجار شركات أمن متخصصة لتحليل الاختراق وعزله، وتكاليف استعادة الأنظمة من النسخ الاحتياطية، والمدفوعات التي قد يضطر البنك إلى دفعها كفدية في حالة هجمات Ransomware، يُضاف إلى ذلك الغرامات التنظيمية التي تفرضها الجهات الرقابية عند ثبوت إهمال أمني أو انتهاك لوائح حماية البيانات، وهي غرامات بالغة في بعض الأطر التشريعية كاللائحة الأوروبية GDPR التي تُتيح فرض غرامات تصل إلى 4% من إيرادات الشركة العالمية السنوية.

التكاليف غير المباشرة: وهي أعسر في القياس وإن كانت في الغالب أضخم حجماً. فقد أشار صندوق النقد الدولي إلى أن التكاليف غير المباشرة تشمل الخسائر في الحصة السوقية جراء هجرة العملاء، وارتفاع تكاليف التمويل على المدى المتوسط، وتكاليف الاستثمار في الترقيات الأمنية التي تُفرضها الحادثة، فضلاً عن التداعيات القانونية من دعاوى تعويضية قد ترفعها فئات متضررة من العملاء (IMF, 2024). وحين تتراكم هذه التكاليف وتتجاوز الاحتياطيات المرصودة لمخاطر التشغيل، فإنها تُنتقص مباشرةً من رأس المال، وتُضعف الربحية وتُهدد نسب كفاية رأس المال.

المبحث الثاني: المخاطر السيبرانية النظامية

أولا: تأثير المخاطر السيبرانية على شبكات الدفع

تتمثل أخطر صور المخاطر السيبرانية في قدرتها على التحول من حادثة تستهدف مؤسسة بعينها إلى أزمة ذات طابع نظامي تمتد آثارها إلى مؤسسات مالية أخرى لم تكن مستهدفة بصورة مباشرة. ويُعرف هذا الامتداد بمفهوم العدوى السيبرانية (Cyber Contagion)، وهو مفهوم يستند إلى فكرة العدوى المالية التقليدية، إلا أنه يختلف عنها في أن انتقال الأثر يتم عبر قنوات تقنية ورقمية تتسم بسرعة انتشار واتساع نطاق أكبر.

وتظهر هذه العدوى داخل البيئة المالية الرقمية من خلال مسارين رئيسيين. يتمثل المسار الأول فيما يُعرف بالصدمات المشتركة (Common Shocks)، حيث تعتمد عدة مؤسسات مصرفية على مزود تقني أو بنية رقمية مشتركة، ما يجعل أي اختراق أو تعطل يصيب هذا المزود قادراً على التأثير المتزامن في عدد كبير من البنوك. وقد برز هذا بوضوح في الولايات المتحدة عام 2023، عندما تسبب هجوم ببرمجيات الفدية استهدف مزود خدمات سحابية في تعطّل عمليات نحو ستين اتحاداً ائتمانياً أمريكياً في الوقت ذاته (IMF, 2024).

أما المسار الثاني، فيرتبط بترابط شبكات الدفع والتسوية بين البنوك، إذ قد يؤدي تعطل الأنظمة التشغيلية في بنك يتمتع بأهمية نظامية إلى تأخير أو تجميد عمليات التسوية مع عدد كبير من المؤسسات المقابلة، الأمر الذي قد يولّد ضغوط سيولة تنتقل تدريجياً عبر النظام المالي.

وفي هذا السياق، أشار بنك التسويات الدولية إلى أن التشابك المتزايد بين المؤسسات المالية عبر أنظمة المقاصة والتسوية وشبكات البنوك المراسلة يوسّع نطاق انتقال آثار الهجمات السيبرانية بين المؤسسات، بما يجعل افتراض احتواء الحادث داخل حدود المؤسسة المتضررة افتراضاً محدود الواقعية في البيئة المصرفية الحديثة (Basel Committee on Banking Supervision [BCBS], 2021).

ثانيا: أثر تعطل البنوك الكبرى على الاستقرار المالي

في قلب التحليل النظامي للمخاطر السيبرانية يأتي سؤال عن: ماذا يحدث حين يستهدف الهجوم السيبراني بنكاً من تلك البنوك التي صنّفها صندوق الاستقرار المالي (FSB) ضمن البنوك ذات الأهمية النظامية العالمية (G-SIBs)؟ والجواب ينطوي على خطورة مزدوجة: فهذه البنوك تحتل مراكز رئيسية في شبكة المدفوعات الدولية، وتُدير حجم ضخم من التسويات البينية، هذا يعني أن تعطلها لأيام قليلة كفيل بإحداث اضطرابات متسلسلة تطال بنوكاً وأسواقاً ومؤسسات مالية أخرى عبر حلقات الائتمان والسيولة.

وقد تناولت دراسة إيزنباخ وزملائه (Eisenbach et al., 2022) هذا السيناريو بالتحليل الكمي الدقيق في السياق الأمريكي، ووجدت أن هجوماً سيبرانياً على أضخم خمسة بنوك أمريكية قادر على

تعطيل ما يفوق الربع من حجم معاملات شبكة المدفوعات بالجملة Fedwire، وهو ما ينعكس بأضرار اقتصادية كلية تتجاوز القطاع المصرفي لتمتد إلى سلاسل التوريد والتجارة والعمالة. ويُحذّر الباحثون من أن الفجوة بين الضرر المحتمل وحجم المصادر المخصصة رقابياً لمواجهة مثل هذا السيناريو، لا تزال فجوة واسعة تستوجب معالجة مكثفة.

الفصل الخامس: المبادرات الدولية لإدارة المخاطر السيبرانية المصرفية

أولا: توجهات لجنة بازل للرقابة المصرفية

على الرغم من أن إطار بازل يعتمد على معالجة المخاطر الائتمانية ومخاطر السوق ومخاطر التشغيل، إلا أن المخاطر السيبرانية بدأت تكتسب أهمية متزايدة في هذا السياق خصوصاً فيما يتعلق بالمخاطر التشغيلية

ففي مارس 2021 أصدرت اللجنة وثيقةً بالغة الأهمية هي "مبادئ المرونة التشغيلية" (Principles for Operational Resilience – BCBS 516)، التي تُشكّل أشمل إطار معياري دولي لمعالجة المخاطر السيبرانية في القطاع المصرفي حتى اليوم. وتنبثق هذه الوثيقة من قناعة أن بازل الثالث، رغم تطور أُطره لرأس المال بصورة غير مسبوقة، لم يُعالج بصورة كافية مسألة استمرارية العمليات تحت وطأة الصدمات غير المالية، وفي مقدمتها الحوادث السيبرانية (BCBS, 2021).

تُرسي الوثيقة سبعة مبادئ تُلزم البنوك بتطوير قدرات المرونة التشغيلية عبر:

تعزيز حوكمة المخاطر على مستوى الإدارة العليا، وضمان استمرارية الخدمات الحيوية في ظل سيناريوهات الاضطراب الشديدة، وإدارة مخاطر الأطراف الثالثة بصرامة، والأهم من ذلك كله الالتزام بالمبدأ السابع الذي يُحدد بصريح العبارة ضرورة أن تمتلك البنوك قدرات متينة لحماية أنظمة تكنولوجيا المعلومات والاتصالات، واكتشاف الحوادث السيبرانية، والاستجابة لها والتعافي منها، مع اختبار دوري منتظم لهذه القدرات (BCBS, 2021). وفي سبتمبر من العام ذاته أصدرت اللجنة نشرةً تكميلية تحثّ البنوك على تكثيف جهودها لتحسين مرونتها أمام التهديدات السيبرانية المتصاعدة، مشيرةً إلى أن جائحة كوفيد–19 فاقمت هذه المخاطر بسبب التحول الجماعي المتسارع نحو العمل عن بُعد والتحول الرقمي (BIS, 2021).

ثانيا: أطر صندوق النقد الدولي وبنك التسويات الدولية

جاء تقرير الاستقرار المالي العالمي الصادر عن صندوق النقد الدولي في أبريل 2024 حاملاً جرس إنذار واضحاً: فالمخاطر السيبرانية تُمثّل اليوم مصدر قلق رئيسياً للاستقرار المالي الكلي، ليس مجرد خطر تقني تشغيلي لتشغيل عمليات. وأثبت الصندوق من خلال تحليله الكمي أن الخسائر المباشرة المتطرفة الناجمة عن الحوادث السيبرانية قد تضاعفت أربع مرات منذ 2017 لتتجاوز 2.5 مليار دولار في الحوادث المؤسسية المفردة، مُنبهاً إلى أن هذه الأرقام هي بالضرورة تقديرات دنيا لأن الشركات كثيراً ما لا تُفصح عن الخسائر الكاملة لاعتبارات سمعية ورقابية (IMF, 2024).

وكشف الصندوق من خلال استطلاعه لعينة من البنوك المركزية والهيئات الرقابية في الاقتصادات الناشئة والنامية عن فجوات تنظيمية صارخة: 56% من هذه الجهات لا تمتلك استراتيجية وطنية للأمن السيبراني مخصصة للقطاع المالي، فيما تفتقر 42% إلى لوائح تنظيمية متخصصة لإدارة مخاطر الأمن السيبراني في المؤسسات المالية، و68% تغيب عنها وحدة رقابية متخصصة في هذا المجال (IMF, 2023). وهذه الأرقام تُشير بوضوح إلى أن المنظومة التنظيمية الدولية، على الرغم من تقدمها في الاقتصادات الكبرى، لا تزال بعيدة عن الشمول الكافي على المستوى العالمي.

وعلى صعيد بنك التسويات الدولية، ارتكزت مساهماته التنظيمية في هذا المجال بصورة رئيسية على دعم اللجان التابعة له كلجنة البنية التحتية للأسواق والمدفوعات (CPMI)، وذلك من خلال توجيهات تُركّز على صون أنظمة المدفوعات والتسوية من التهديدات السيبرانية، نظراً لكونها العصب المركزي للتدفقات المالية الدولية.

النتائج والتوصيات

بعد فهم القنوات التي تنتقل عبرها المخاطر السيبرانية، واستعراض الأطر الدولية الراهنة، يخلص هذا البحث إلى جملة من النتائج التحليلية يمكن صياغتها على النحو الآتي:

1- يساهم التحول الرقمي في تحسين الكفاءة وتعزيز التنافسية، لكنه في نفس الوقت يزيد من مستوى التعرض للمخاطر السيبرانية. وتزداد هذه الإشكالية تعقيداً لأن البنوك التي تتأخر في تبني التحول

الرقمي تفقد قدرتها التنافسية، بينما تلك التي تتسارع في التحول دون تعزيز منظوماتها الأمنية تصبح أكثر عرضة للمخاطر.

2- يُشكّل الاعتماد على مزودي الخدمات من الطرف الثالث، والترابط الشبكي الكثيف بين المؤسسات المالية، بيئةً خصبة لسيناريوهات العدوى السيبرانية النظامية، حيث يمكن لحادثة واحدة في بنك أو مزود خدمة محوري أن تتحول إلى صدمة نظامية عابرة للمؤسسات.

3- على الرغم من طرح أظر تنظيمية دولية إلى أنه هناك فجوات تنظيمية واسعة خاصةً في الاقتصادات الناشئة والنامية، تجعل المنظومة العالمية للاستقرار المصرفي غير محصّنة بصورة كافية في مواجهة التهديدات السيبرانية المتصاعدة.

4- : يُفرز التحول الرقمي نمطاً جديداً من الذعر المصرفي يُسمى الذعر المصرفي الرقمي (Digital Bank Run)، تُلغي فيه تقنيات الدفع الفوري الحواجز الزمنية والمكانية التقليدية التي كانت توفر للبنوك فسحةً من الوقت للتعامل مع أزمات السيولة، مما يرفع حدة المخاطر ويُضيّق هامش الاستجابة.

وتوصي الدراسة بالآتي:

1- إدراج اشتراطات الأمن السيبراني منذ مراحل تصميم المنتجات والخدمات الرقمية لا لاحقاً، مع الاستثمار في برامج اختبار الاختراق الدورية والتمارين المحاكاتية الواقعية (Red Team exercises) للكشف عن الثغرات قبل أن يكتشفها المهاجمون.

2- تطوير أُطر رقابية وطنية متخصصة بالمخاطر السيبرانية تستند إلى المعايير الدولية وتُكيّفها مع البيئة المحلية، مع التركيز على تطوير قدرات رقابية متخصصة للتحقق من التزام البنوك بهذه المعايير بصورة فعلية لا شكلية. ويشمل ذلك إلزام البنوك بالإفصاح عن الحوادث السيبرانية الجسيمة خلال مدد محددة، وتشجيع تبادل معلومات التهديدات بين المؤسسات المالية.

3- تعزيز منظومات التبادل الاستخباراتي للتهديدات السيبرانية بين الهيئات الرقابية الوطنية، وبناء بروتوكولات استجابة منسقة للأزمات السيبرانية ذات البُعد العابر للحدود، على غرار ما بدأت تقترحه توجيهات مجلس الاستقرار المالي (FSB).

4- إلزام البنوك بتعيين مسؤول تنفيذي رفيع للأمن السيبراني (CISO) يتمتع بصلاحيات واضحة وصلة اتصال مباشرة بمجلس الإدارة، وأن تتضمن لجان المخاطر في المجالس خبرة سيبرانية فعلية، لا مجرد وعي عام بوجود هذه المخاطر.

يفتح هذا البحث النظري أمام الباحثين اللاحقين آفاقاً خصبة للدراسات التجريبية الكمية، من بينها: قياس أثر الحوادث السيبرانية على مؤشرات الأداء المالي للبنوك في البيئة العربية بأسلوب دراسات الحدث (Event Studies)، وتحليل علاقة الأثر بين حجم الاستثمار في الأمن السيبراني ومعدلات الأداء المعدلة بالمخاطر، واختبار مدى التقارب في المخاطر السيبرانية الكلية عبر أنظمة التصنيف الرقمي للبنوك المركزية العربية.

المراجع

الرضا، ز.، والموسوي، ع. (2025). التحول الرقمي والأدوار المحتملة للإسهام في تحقيق التنمية المستدامة في العراق. *مجلة الغري للعلوم الاقتصادية والإدارية*.

عمر، عمر عبد الحفيظ أحمد. (2021). التحول الرقمي للحكومة ودوره في تحقيق أهداف التنمية المستدامة: مصر نموذجاً. *مجلة جامعة الزيتونة الأردنية للدراسات القانونية، 2*(3)، 154-179.

قاضي، أ. م. الله، وزيتوني، ص. ر. (2025). *إدارة المخاطر السيبرانية في البنوك الجزائرية في ظل التحول الرقمي: دراسة حالة لفروع البنوك العمومية بورقلة* ***(BEA – CPA – BNA)*** [مذكرة ماجستير أكاديمي غير منشورة]. جامعة قاصدي مرباح – ورقلة، كلية العلوم الاقتصادية والتجارية وعلوم التسيير.

كريمة، ج.، وبن قيدة، م. (2023). *أثر التحول الرقمي على كفاءة وأداء القطاع المصرفي: تجربة مصر نموذجاً* [ورقة بحثية غير منشورة]. جامعة يحيى فارس بالمدية، مختبر التنمية المحلية المستدامة.

Basel Committee on Banking Supervision. (2021a). *Principles for operational resilience* (BCBS 516). Bank for International Settlements.

Basel Committee on Banking Supervision. (2021b). *Revisions to the principles for the sound management of operational risk* (BCBS 515). Bank for International Settlements.

Basel Committee on Banking Supervision. (2021c). *Cyber resilience: Range of practices*. Bank for International Settlements.

Braine, L., & Shukla, S. (2022). Illustrative industry architecture to mitigate potential fragmentation across a central bank digital currency and commercial bank money. *Journal of Financial Market Infrastructures, 10*(3), 1-24.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431-448.

Congressional Research Service. (2022). *Correspondent banking and the SWIFT system* (Report No. R47391).

Diamond, D. W., & Dybvig, P. H. (1983). Bank runs, deposit insurance, and liquidity. *Journal of Political Economy, 91*(3), 401-419.

Duffie, D., & Younger, J. (2019). *Cyber runs* (Hutchins Center Working Paper No. 51). Brookings Institution.

Financial Stability Board. (2017). *Progress report on the FSB action plan to assess and address the decline in correspondent banking*.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security, 5*(4), 438-457.

Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches on stock returns: A comparison of alternative models. *Journal of Information Security, 2*(2), 49-58.

Gordon, W. J. (2019). De-risking and the demise of correspondent banking: A quantitative assessment of the impact on remittance flows. *Journal of Money Laundering Control, 22*(3), 474-488.

Integris. (2026). *Integris survey on banking security and customer trust*.

International Monetary Fund. (2023). *Mounting cyber threats mean financial firms urgently need better safeguards*. IMF Blog.

International Monetary Fund. (2024). Chapter 3: Cyber risk – A growing concern for macrofinancial stability. In *Global Financial Stability Report, April 2024*. IMF.

Kamiya, N., Kang, J. K., Kim, J. S., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics, 145*(3), 802-826.

Munira, M. S. K. (2025). Digital transformation in banking: A systematic review of trends, technologies, and challenges. In *Strategic Data Management and Innovation*. [Publisher].

Park, J. S., O'Brien, J., Cai, C. J., Morris, M. R., Liang, P., & Bernstein, M. S. (2023). Generative agents: Interactive simulacra of human behavior. In *Proceedings of the 36th Annual ACM Symposium on User Interface Software and Technology*. ACM.

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors*.

Sathwika, B., Hameed, A., Ramya, R., Babu, T., Chandra, R., & Sungheetha, A. (2024). Influence of digital transformation on the banking industry. In *Proceedings of the 2024 4th International Conference on Innovative Practices in Technology and Management (ICIPTM)* (pp. 1-6).

Telang, R., & Somanchi, A. (2016). *Security, fraudulent transactions and customer loyalty: A field study*. Federal Trade Commission.

The dynamics of stock market responses following the cyber-attacks news: Evidence from event study. (2025). *Journal of Information Systems*.

Xie, X., & Wang, S. (2023). Digital transformation of commercial banks in China: Measurement, progress and impact. *China Economic Quarterly International*.