Comprehensive Journal of Science
Volume (10), Issue (39), (March, 2026)
ISSN: 3014-6266

مجلة العلوم الشاملة
المجلد (10) العدد 39 مارس 2026
ردمد: 3014-6266

أثر التكامل والشراكة المصرفية على إدارة المخاطر الجيوسياسية لأنظمة الدفع الإلكتروني دراسة ميدانية على المصارف التجارية الليبية (مصرف الجمهورية، مصرف الصحاري)

أبو بكر عبد الرحمن بشيه
باحث – طرابلس، ليبيا
abobakr.aloraifi@gmail.com
سعود المهدي بن زايد
قسم التمويل والمصارف، جامعة طرابلس، طرابلس، ليبيا
sa.zayed@uot.edu.ly

The Impact of Banking Integration and Partnerships on Geopolitical Risk Management for Electronic Payment Systems: A Field Study on Libyan Commercial Banks (Al-Jumhouria Bank, Al-Sahari Bank)

Abobakr Abdulrahman Basheh
Researcher – Tripoli, Libya
abobakr.aloraifi@gmail.com
Saud Al-Mahdi Bin Zayed
Department of Finance and Banking, University of Tripoli, Tripoli, Libya
sa.zayed@uot.edu.ly

تاريخ الاستلام:2026/01/05 –تاريخ المراجعة: 2026/01/29– تاريخ القبول: 2026/02/12– تاريخ للنشر:2026 /03/09

مستخلص الدراسة

تهدف هذه الدراسة إلى استكشاف أثر التكامل والشراكة المصرفية على إدارة المخاطر الجيوسياسية والنظامية لأنظمة الدفع الإلكتروني، مع التطبيق على البيئة المصرفية الليبية، وتحديداً (مصرف الجمهورية ومصرف الصحاري) .تتبلور مشكلة الدراسة في "معضلة الاعتمادية المتبادلة" والاعتماد شبه الكلي على بنية تحتية مركزية (الموزع الوطني)، مما يخلق "نقطة فشل موحدة" ذات طابع سيادي، تجعل البنية التحتية للمدفوعات عرضة للتأثر بالصراعات السياسية، والانقسامات المؤسسية، والتهديدات السيبرانية الجيوسياسية .اعتمدت الدراسة على المنهج الوصفي التحليلي، واستخدمت الاستبانة كأداة لجمع البيانات من عينة قصدية شملت 40 مبحوثاً من الكوادر الفنية والإدارية بمصرفي (الجمهورية والصحاري) .خلصت النتائج إلى وجود نجاح ملموس في تحقيق التكامل التقني مع الموزع الوطني بمستوى موافقة مرتفع جداً، إلا أن هذا التطور لم يواكبه مستوى مماثل من التكامل الأمني والسيادي .كما أثبتت النتائج أن الاعتماد المركزي المفرط، في ظل غياب خطط طوارئ لامركزية، يخلق هشاشة بالغة أمام الصدمات الجيوسياسية .وأوصت الدراسة بضرورة الانتقال إلى نماذج "الثقة الصفرية (Zero Trust)" في واجهات برمجة التطبيقات(APIs) ، وإنشاء مراكز بيانات سيادية بديلة وموزعة جغرافياً، وتأسيس غرفة عمليات سيبرانية موحدة لتعزيز المرونة التشغيلية والسيادية.

الكلمات المفتاحية :التكامل المصرفي، أنظمة الدفع الإلكتروني، المخاطر الجيوسياسية، الموزع الوطني، الأمن السيبراني السيادي، المصارف الليبية.

Abstract

This study aims to explore the impact of banking integration and partnership on managing the geopolitical and systemic risks of electronic payment systems, applied to the Libyan banking environment, specifically focusing on (Jumhouria Bank and Sahara Bank). The research problem crystallizes in the "interdependency dilemma" and the near-total reliance on a centralized infrastructure (the National Switch), which creates a sovereign "single point of failure". This dependency makes the payment infrastructure highly vulnerable to political

conflicts, institutional divisions, and geopolitical cyber threats. The study adopted a descriptive-analytical approach, utilizing a questionnaire to collect data from a purposive sample of 40 technical and administrative staff members at Jumhouria and Sahara banks. The results revealed a significant success in achieving technical integration with the National Switch; however, this progress was not matched by a similar level of security and sovereign integration. Furthermore, the findings proved that excessive centralized reliance, in the absence of decentralized contingency plans, creates severe vulnerability to geopolitical shocks. The study recommended the necessity of transitioning to "Zero Trust" models in APIs, establishing alternative and geographically distributed sovereign data centers, and founding a unified cyber operations room to enhance operational and sovereign resilience.

Keywords: Banking Integration, Electronic Payment Systems, Geopolitical Risks, National Switch, Sovereign Cybersecurity, Libyan Banks

1. المقدمة

يشهد القطاع المالي والمصرفي العالمي تحولاً جذرياً في فلسفة العمل وآليات تقديم الخدمات، مدفوعاً بثورة التقنيات المالية (Fintech)وتغير تفضيلات العملاء نحو القنوات الرقمية، وذلك في ظل مشهد عالمي يتسم بالتعقيد والتقلبات الجيوسياسية المتسارعة .لم تعد المصارف تعمل كـ"صوامع (Silos) "منعزلة تحتكر سلسلة القيمة المالية بالكامل، بل أصبحت مضطرة – بفعل قوى السوق والتشريعات – إلى الانخراط في منظومات بيئية مفتوحة (Open Ecosystems) تعتمد على مبادئ الشراكة والتكامل مع أطراف متعددة، بدءاً من المصارف النظيرة، مروراً بشركات معالجة المدفوعات، وصولاً إلى شركات التقنية الناشئة.(World Bank, 2020)

إن هذا التحول نحو ما يُعرف بـ "الصيرفة المتصلة (Connected Banking) "قد أفرز واقعاً جديداً تتلاشى فيه الحدود التقليدية للمؤسسة المصرفية .ففي حين يتيح التكامل التقني والتشغيلي (Interoperability) بين أنظمة الدفع المختلفة سرعة غير مسبوقة في دوران الأموال وتعزيز الشمول المالي، فإنه يخلق في المقابل "اقترانًا وثيقًا (Tight Coupling) "بين مكونات النظام المالي .(Perrow, 1999) هذا الاقتران يعني أن المخاطر لم تعد محصورة في الجوانب التقنية أو التشغيلية داخل جدران المصرف الواحد، بل امتدت لتشمل المخاطر الجيوسياسية (Geopolitical Risks)؛ حيث أصبحت البنى التحتية للمدفوعات الوطنية عرضة للتأثر بالصراعات السياسية، والانقسامات المؤسسية، والتهديدات السيبرانية العابرة للحدود المدعومة من جهات خارجية، مما قد يتسبب في تداعيات نظامية تهدد استقرار القطاع بأكمله.(BIS, 2021)

في السياق الليبي، يكتسب هذا الموضوع أبعاداً استراتيجية وحساسية فائقة تتعلق بالأمن القومي المالي .ففي ظل أزمة السيولة النقدية المستمرة، والتوجه الحكومي القوي خلال عامي 2024 و2025 نحو فرض الدفع الإلكتروني كخيار إجباري في المعاملات التجارية (حكومة الوحدة الوطنية، 2025)، تعتمد المصارف التجارية الليبية، وعلى رأسها مصرف الجمهورية ومصرف الصحاري، بشكل متزايد على بنية تحتية وطنية مشتركة تتمثل في "الموزع الوطني" الذي تديره شركة معاملات . هذا الاعتماد المركزي، ورغم كفاءته الاقتصادية، يضع النظام المالي الليبي أمام تحديات جسيمة تتجاوز المرونة التشغيلية لتلامس صميم المخاطر الجيوسياسية .ففي بيئة محلية تتأثر بالتجاذبات السياسية، يصبح الموزع الوطني بنية تحتية سيادية حرجة قد تتأثر بأي صدمات سياسية أو أمنية، وهو ما تجلى بوضوح في حوادث انقطاع الخدمة التي شهدتها البلاد في أكتوبر 2025، والتي تدق ناقوس الخطر حول ضرورة تحصين هذه الأنظمة وإدارة مخاطرها في ظل بيئة جيوسياسية معقدة (مصرف ليبيا المركزي، 2025).

2. مشكلة الدراسة وتساؤلاتها

تتمحور المشكلة البحثية حول "معضلة الاعتمادية المتبادلة (Interdependency Dilemma) "في أنظمة الدفع الحديثة . فبينما تسعى المصارف إلى تعميق شراكاتها وتكاملها التقني لتعزيز التنافسية وحل مشاكل السيولة، فإن هذا التكامل يفتح

أبواباً جديدة للمخاطر التي قد تكون خارج نطاق سيطرة المصرف المباشرة .تكمن الإشكالية في أن نماذج إدارة المخاطر التقليدية، التي صُممت لمؤسسات تعمل بشكل مستقل، قد لا تكون فعالة في بيئة مترابطة شبكياً حيث تنتقل المخاطر بسرعة "العدوى" (Contagion) .

وتتفاقم هذه المشكلة بشكل حاد في البيئة الليبية نتيجة تقاطع الهشاشة التقنية مع **التعقيدات الجيوسياسية؛** حيث يبرز الاعتماد شبه الكلي على مزود خدمة وطني واحد (شركة معاملات) كبوابة عبور رئيسية .هذا التمركز يجعل البنية التحتية للمدفوعات عرضة ليس فقط للأعطال الفنية، بل للصدمات الناتجة عن الانقسامات السياسية، والتوترات الأمنية، والقرارات السيادية المفاجئة .إضافة إلى ذلك، يتداخل عمل المصارف التجارية، وفي مقدمتها)**مصرف الجمهورية، ومصرف الصحاري(**، مع شركات التقنية المالية الخاصة في بيئة تعاني من ضعف البنية التحتية للاتصالات والطاقة، مما يحول أي أزمة سياسية أو أمنية محلية إلى أزمة نظامية تهدد استمرارية قطاع المدفوعات بأكمله.

بناءً على ذلك، يمكن صياغة السؤال الرئيسي للدراسة على النحو التالي:

"كيف يؤثر التكامل والشراكة المصرفية في البنية التحتية للمدفوعات على قدرة المصارف التجارية الليبية (مصرف الجمهورية، ومصرف الصحاري) على إدارة المخاطر الجيوسياسية والنظامية، وما هي الاستراتيجيات المثلى لضمان استمرارية الخدمات في ظل التقلبات الحالية؟"

ويتفرع عن هذا السؤال الرئيسي الأسئلة الفرعية الآتية:

- ما هي الطبيعة الهيكلية لأنظمة الدفع الإلكتروني المتكاملة(Interoperable Payment Systems) ، وكيف تعيد العوامل الجيوسياسية (كالاستقطاب السياسي والنزاعات) تشكيل ملف المخاطر فيها مقارنة بالأنظمة المغلقة؟
- ما حجم وطبيعة المخاطر الناشئة عن الشراكة مع الأطراف الثالثة (Third-Party Risks) في مصرفي (الجمهورية والصحاري)، وكيف تفاقم البيئة الجيوسياسية غير المستقرة من ثغرات واجهات برمجة التطبيقات (APIs)؟
- كيف أثرت مركزية "الموزع الوطني" على المرونة التشغيلية لمصرفي الجمهورية والصحاري في مواجهة الصدمات الجيوسياسية والتقنية، وما الدروس المستفادة من انقطاعات الخدمة المتكررة في 2024-2025؟
- ما مدى فاعلية الوسائل الرقابية والتشريعية الحالية (تعليمات مصرف ليبيا المركزي) في ضبط مخاطر هذا التكامل المتزايد وحماية البنية السيادية للمدفوعات من التداعيات الجيوسياسية؟

3.أهداف الدراسة

تهدف هذه الدراسة إلى تقديم تحليل شامل وعميق لظاهرة التكامل المصرفي وتداعياتها على إدارة المخاطر الجيوسياسية والنظامية، وذلك من خلال:

أ. توضيح المفاهيم المتعلقة بالتشغيل البيني (Interoperability) والمخاطر الجيوسياسية والنظامية الناتجة عن ترابط البنى التحتية المالية وتأثرها بالصراعات أو الانقسامات السياسية.

ب. تحليل العلاقة بين المصارف التجارية عينة الدراسة (مصرف الجمهورية ومصرف الصحاري) وشركة معاملات ومزودي خدمات القطاع الخاص، وتقييم مستوى التكامل التقني بينهم في ظل التجاذبات السياسية المعقدة التي تمر بها البلاد.

ت. تحديد نقاط الضعف في البنية التحتية الحالية في مواجهة الصدمات الجيوسياسية والسيبرانية ذات الأبعاد السيادية، وتقييم تحديات استمرارية الأعمال(Business Continuity) ، استناداً إلى تقارير الهيئة الوطنية لأمن المعلومات (NISSA)وتقارير مصرف ليبيا المركزي.

ث. تقديم توصيات استراتيجية وعملية لصناع القرار في مصرف ليبيا المركزي ومصرفي (الجمهورية والصحاري) لبناء "مرونة سيادية وتشغيلية" قادرة على امتصاص الصدمات الجيوسياسية، وتحييد تهديداتها على أنظمة الدفع المتكاملة.

4. أهمية الدراسة

تنبع أهمية الدراسة من عدة اعتبارات علمية وعملية:

أ. تساهم في إثراء المكتبة العربية بدراسة تحليلية رائدة تربط بين أنظمة المدفوعات الإلكترونية كـ "نظام معقد " (Complex System)يخضع لنظريات المخاطر الشبكية، وبين أبعاد المخاطر الجيوسياسية وتأثير البيئة السياسية غير المستقرة، وهو منظور يغيب عن كثير من الدراسات التقليدية التي تكتفي بالجانب التقني.

ب. تواكب الدراسة التطورات المتسارعة والحرجة التي شهدتها ليبيا في عامي 2024 و2025، بما في ذلك إطلاق مشاريع الدفع الفوري(Instant Payments) ، وتوحيد شبكات نقاط البيع، والقرارات الحكومية الملزمة بالدفع الإلكتروني، وتدرس أثرها في ظل بيئة سياسية متقلبة تفرض تحديات مضاعفة على الاستقرار المالي.

ت. تقدم الدراسة تحليلاً لواقعة انقطاع الموزع الوطني في أكتوبر 2025، ليس كعطل فني فحسب، بل كجرس إنذار يكشف هشاشة البنية التحتية السيادية أمام الصدمات؛ مما يوفر دروساً حية حول أهمية التكرارية (Redundancy) وتوزيع مراكز البيانات كضرورة ملحة لحماية الأمن القومي المالي.

5. فرضيات الدراسة

- **الفرضية الأولى** :توجد علاقة طردية ذات دلالة إحصائية بين مستوى التكامل التقني والتشغيلي (Interoperability)بين مصرفي (الجمهورية والصحاري) والشبكة الوطنية من جهة، وبين تعرضهما للمخاطر الجيوسياسية والنظامية من جهة أخرى؛ حيث يسهل الترابط العالي انتقال "العدوى (Contagion) "وتضخم الأزمات المالية عند حدوث صدمات سياسية أو أمنية مفاجئة.
- **الفرضية الثانية** :يؤدي الاعتماد المفرط على "المحولات الوطنية المركزية" في ظل بيئة سياسية متقلبة، ودون وجود خطط طوارئ بديلة وموزعة جغرافياً(Decentralized Contingency Plans) ، إلى خلق نقاط فشل موحدة (Single Points of Failure)ذات طابع سيادي تهدد الاستقرار المالي الوطني برمته.
- **الفرضية الثالثة** :إن تطبيق مصرفي (الجمهورية والصحاري) لاستراتيجيات إدارة مخاطر الطرف الثالث (TPRM) والمعايير الدولية) مثل PCI–DSS و (ISO 27001 لا يزال دون المستوى المطلوب لاحتواء الصدمات الجيوسياسية والتهديدات السيبرانية المدعومة من جهات خارجية في بيئة متكاملة تفتقر إلى الاستقرار.

6. نموذج الدراسة

يعتمد النموذج على متغيرين رئيسيين:

أ. المتغير المستقل (التكامل والشراكة المصرفية): ويتم قياسه من خلال أبعاد (الاندماج المالي، الشراكة في البنية التحتية التقنية، توحيد السياسات والإجراءات) .

ب. المتغير التابع (إدارة المخاطر الجيوسياسية لأنظمة الدفع الإلكتروني): يتم قياسه من خلال الأبعاد التالية:

- مخاطر البنية التحتية السيادية والانقسام التشغيلي :ويقيس أثر الصدمات السياسية، والانقسامات، وانقطاع الاتصالات والطاقة على استمرارية الموزع الوطني.
- التهديدات السيبرانية الجيوسياسية والعدوى النظامية :ويقيس مدى التعرض لهجمات سيبرانية موجهة ذات طابع سياسي، وسرعة انتقال الأزمة بين المصارف المترابطة.

- المخاطر القانونية وتضارب التشريعات في بيئة متقلبة :ويقيس أثر القرارات السيادية المفاجئة، واختلاف المرجعيات الرقابية، وتأثيرها على سمعة المصرف والتزاماته.

7. مجتمع وعينة الدراسة

أ. مجتمع الدراسة: نظراً لطبيعة الدراسة الميدانية، يتمثل مجتمع الدراسة في المصارف التجارية الليبية محل التطبيق، وهما تحديداً:

- مصرف الجمهورية.
- مصرف الصحاري .

حيث يمثل هذا المجتمع البيئة التنظيمية التي تُمارس فيها عمليات التكامل والشراكة المصرفية وإدارة المخاطر الجيوسياسية لأنظمة الدفع الإلكتروني.

ب. عينة الدراسة: نظراً للطبيعة الفنية والتخصصية لموضوع الدراسة، سيتم الاعتماد على عينة عمدية (قصدية) من الكوادر الوظيفية الفاعلة في المصرفين المذكورين (الجمهورية والصحاري) ، ممن يمتلكون المعرفة والخبرة بموضوعات الشراكة والمخاطر والتقنية ، وقدرتهم على تقييم أثر التقلبات الجيوسياسية .وتشمل الفئات التالية:

- المديرون التنفيذيون ونوابهم.
- مديرو إدارات المخاطر والامتثال.
- مديرو إدارات تقنية المعلومات.(IT)
- مديرو العمليات المصرفية الإلكترونية.
- رؤساء الأقسام المختصة بتطوير المنتجات والشراكات الاستراتيجية.

8. الإطار النظري لأنظمة الدفع والشراكة في عصر الاقتصاد الرقمي:

يتناول هذا الإطار الأسس النظرية والمفاهيمية لأنظمة الدفع الإلكتروني، مع التركيز على الديناميكيات الجديدة التي فرضها التكامل والشراكة بين المصارف والجهات الفاعلة الأخرى.

1.8 ماهية أنظمة الدفع الإلكتروني والشراكة المصرفية

1.1.8 تطور أنظمة الدفع: من الانعزال إلى المنظومات البيئية

تطورت أنظمة الدفع الإلكتروني (Electronic Payment Systems – EPS) بشكل جذري عبر العقود الماضية. في السابق، كانت هذه الأنظمة تعمل كـ "حلقات مغلقة" (Closed Loops)، حيث تقتصر المعاملات داخل شبكة المصرف الواحد أو شبكة البطاقات المحددة (Proprietary Networks). كان الانتقال بين هذه الشبكات يتطلب عمليات تسوية يدوية ومعقدة ومكلفة. أما اليوم، فقد تحولت الصناعة نحو "المنظومات المفتوحة" (Open Ecosystems) التي تعتمد على البنية التحتية المشتركة.(World Bank, 2020)

يُعرّف نظام الدفع الإلكتروني الحديث بأنه "مجموعة شاملة من الأدوات، والإجراءات المصرفية، وشبكات تحويل الأموال، والبنى التحتية التقنية التي تضمن تداول القيمة المالية بشكل آمن وسلس ولحظي بين الأطراف المختلفة، بغض النظر عن المؤسسة المالية التي ينتمون إليها". ((World Bank (2020)

ويشير (BIS, 2021) إلى أن الأنظمة الحديثة تتكون من طبقات مترابطة: طبقة واجهات المستخدم (Front-end)، طبقة المعالجة والمقاصة (Clearing & Processing)، وطبقة التسوية النهائية (Settlement) التي تتم عادةً عبر أموال البنك المركزي لضمان "وحدانية النقد" (Singleness of Money). ((BIS (2021)

2.1.8 مفهوم الشراكة والتكامل (Interoperability): العصب الجديد للمصرفية

يُعد "التشغيل البيني" أو التكامل (Interoperability) المفهوم الجوهري الذي تقوم عليه الشراكات المصرفية الحديثة. ويُعرف بأنه القدرة التقنية، والتنظيمية، والقانونية لأنظمة وشبكات مختلفة على التواصل وتبادل البيانات وتنفيذ المعاملات فيما بينها بشفافية، بحيث لا يشعر المستخدم النهائي بالفروقات بين الأنظمة.(ITU/World Bank)

- **مستويات التكامل في الأنظمة المصرفية:**

أ. **التكامل على مستوى المنصة (Platform-Level Interoperability):** يتيح للعملاء تحويل الأموال بين منصات مختلفة (مثل من حساب مصرفي في بنك الجمهورية إلى محفظة "سداد" الإلكترونية). هذا النوع من التكامل يكسر احتكار المنصات المغلقة ويعزز تأثيرات الشبكة (Network Effects).

ب. **التكامل على مستوى البنية التحتية (Infrastructure-Level):** يتمثل في استخدام بنية تحتية مشتركة للمعالجة، مثل "المحولات الوطنية" (National Switches) التي تربط كافة أجهزة الصراف الآلي (ATM) ونقاط البيع (POS) في الدولة، مما يسمح لبطاقة أي مصرف بالعمل على أي جهاز.

ج. **التكامل على مستوى الوكيل (Agent-Level):** يسمح لنقاط الخدمة (الوكلاء) بتقديم خدمات لمستخدمي بنوك متعددة، وهو ما يعزز الانتشار الجغرافي للخدمات المالية بتكلفة أقل.

الجدول رقم (1) مقارنة بين الأنظمة المغلقة والأنظمة المتكاملة

وجه المقارنة	الأنظمة المغلقة (Closed Loop)	الأنظمة المتكاملة (Interoperable/Open)
إمكانية الوصول	مقتصرة على عملاء الشبكة نفسها	مفتوحة لعملاء الشبكات الأخرى
التكلفة	تكاليف تشغيلية عالية (تكرار البنية التحتية)	تكاليف أقل (مشاركة البنية التحتية)
المخاطر	مخاطر محصورة داخل المؤسسة	مخاطر نظامية وعدوى (Systemic Risk)
تجربة العميل	مجزأة ومقيدة	سلسة وموحدة
المثال الليبي	خدمة "وتبة" (سابقاً) لمصرف التجارة والتنمية [17]	الموزع الوطني لشركة معاملات

3.1.8 البنية التحتية اللازمة للتكامل: دور المحولات الوطنية

لتحقيق الشراكة الفعالة، تعتمد الدول على "المحولات الوطنية" (National Payment Switches - NPS) التي تعمل كـ "محور ارتكاز" (Hub) يربط كافة الأطراف.

أ. **آلية العمل:** يقوم المحول الوطني باستلام طلب المعاملة من الجهة المستحوذة (Acquirer)، وتوجيهه (Routing) إلى الجهة المصدرة (Issuer) للموافقة، ثم إعادة الرد، وإجراء عملية التقاص (Netting) في نهاية اليوم لتسوية الفروقات المالية عبر البنك المركزي.[14]

ب. **الأهمية الاستراتيجية:** تضمن المحولات الوطنية السيادة على البيانات المالية (Data Sovereignty)، وتقليل الاعتماد على الشبكات الدولية (مثل Visa/Mastercard) في المعاملات المحلية، وخفض الرسوم.

ج. **النموذج الليبي:** تلعب شركة "معاملات" للخدمات المالية هذا الدور في ليبيا، حيث تدير الموزع الوطني الذي يربط المصارف التجارية. إلا أن هذا النموذج المركزي يخلق تحدياً كبيراً يتمثل في "نقطة الفشل الموحدة" (Single Point of

Failure)، حيث يؤدي أي توقف في الموزع إلى شلل تام في منظومة الدفع الوطنية، كما حدث في التوقفات المتكررة خلال 2024–2025.[5]

4.1.8 دور شركات التقنية المالية (Fintech) كشريك في العمليات

تحولت العلاقة بين المصارف وشركات الـ Fintech من المنافسة الشرسة إلى التكامل الاستراتيجي.

أ. **نموذج الشراكة:** تقدم شركات الـ Fintech الابتكار، وواجهات المستخدم السهلة، والوصول للشرائح غير المخدومة، بينما تقدم المصارف الملاءة المالية، والامتثال التنظيمي، والبنية التحتية للتسوية.[1]

ب. **التطورات في ليبيا:** في نوفمبر 2024، خطت ليبيا خطوة هامة بالسماح لشركة "تداول" (قطاع خاص) بربط شبكتها مع الموزع الوطني "معاملات" (قطاع عام). هذا التكامل بين القطاعين العام والخاص (PPP) يهدف إلى توسيع شبكة القبول، ولكنه يفرض تحديات جديدة في توحيد البروتوكولات الأمنية وإدارة مخاطر الطرف الثالث.

2.8 المخاطر المرتبطة بأنظمة الدفع الإلكتروني في ظل التكامل

يؤدي الانتقال إلى بيئة مصرفية متكاملة ومفتوحة إلى تغيير جذري في خارطة المخاطر، حيث تظهر مخاطر جديدة وتتضخم مخاطر تقليدية بفعل عامل "الترابط".

1.2.8 نظرية "الاقتران الوثيق" (Tight Coupling) وانتقال المخاطر

تستند إدارة المخاطر في الأنظمة المتكاملة إلى نظرية "الاقتران الوثيق"، التي تشير إلى أن الأنظمة المترابطة بشدة تسمح بانتشار الاضطرابات بسرعة هائلة تجعل من الصعب احتواؤها أو عزلها. في شبكات الدفع المتكاملة، أي فشل في عقدة واحدة (Node) يمكن أن ينتشر كـ "تأثير الدومينو" ليصيب الشبكة بأكملها.(Perrow, 1999)

2.2.8 المخاطر التشغيلية والتقنية (Operational Risks)

تعد المخاطر التشغيلية الهاجس الأكبر في البيئات المتكاملة، وتنقسم إلى:

أ. **فشل النظام والبنية التحتية (System Failure):** الاعتماد على التكنولوجيا يعني أن انقطاع التيار الكهربائي، أو فشل الخوادم، أو انقطاع الاتصالات (وهي مشاكل شائعة في ليبيا) يؤدي إلى توقف الخدمة فوراً. في الأنظمة المتكاملة، توقف "بوابة الدفع" المركزية يعني توقف المبيعات لآلاف التجار في آن واحد.

ب. **مخاطر التوسع والأداء (Performance & Scalability):** مع زيادة حجم المعاملات الإلكترونية (التي نمت بنسبة 75% في النصف الأول من 2025 في ليبيا)، قد تعجز الأنظمة القديمة (Legacy Systems) في المصارف عن معالجة هذا الكم الهائل من البيانات في الوقت الفعلي، مما يؤدي إلى اختناقات (Bottlenecks) وفشل في إتمام المعاملات.

ج. **نقاط الفشل الموحدة (SPOF):** الاعتماد الحصري على شركة "معاملات" كموزع وحيد دون وجود بدائل (Redundancy) يعرض الدولة بأكملها لخطر التوقف، وهو ما يستدعي استراتيجيات لتوزيع مراكز البيانات.

3.2.8 مخاطر الأمن السيبراني والاحتيال (Fraud & Cybersecurity)

يؤدي التكامل إلى توسيع "سطح الهجوم" (Attack Surface) بشكل كبير.

أ. **هجمات سلسلة التوريد (Supply Chain Attacks):** قد لا يستهدف المخترقون المصرف القوي أمنياً بشكل مباشر، بل يهاجمون شريكاً صغيراً (Fintech Startup) أو مزود خدمة طرف ثالث متصل بشبكة المصرف، ومن خلاله يتسللون إلى النظام المصرفي الرئيسي. هذا النوع من المخاطر يتطلب من المصارف مراقبة ليس فقط شركائها، بل وشركاء شركائهم (الطرف الرابع).

ب. **الاحتيال عبر الهندسة الاجتماعية:** مع دخول شرائح جديدة من المجتمع غير الملمين بالتقنية إلى النظام المالي (الشمول المالي)، تزداد فرص الاحتيال عبر التصيد (Phishing) واستغلال جهل المستخدمين، خصوصاً مع تقنيات مثل QR Codes التي قد يتم تزويرها.

ج. **تهديدات الفدية (Ransomware):** تشير التقارير إلى أن المؤسسات المالية والجهات الحكومية في ليبيا تعاني من ضعف في الضوابط الأمنية ووجود ثغرات غير معالجة، مما يجعلها عرضة لهجمات الفدية التي قد تشفر بيانات الدفع الحساسة.

د. **مخاطر أمن واجهات برمجة التطبيقات :(API Security Risks)** يختلف هذا النوع من المخاطر عن الاختراقات التقليدية للشبكات. ففي بيئة الصيرفة المفتوحة والشراكة مع شركات الـFintech ، يتم تبادل البيانات عبر واجهات برمجة التطبيقات .(APIs) ويكمن الخطر الأكبر هنا في ثغرات 'التحكم في الوصول Broken Object Level ' (Authorization – BOLA، حيث يمكن للمهاجمين استغلال نقاط النهاية (Endpoints) للوصول إلى بيانات حسابات لا تخصهم بمجرد تغيير معرف المستخدم في كود الطلب البرمجي. تتطلب هذه المخاطر حلولاً متخصصة مثل 'بوابات أمن الـ API' (API Gateways) التي تختلف جذرياً عن جدران الحماية النارية التقليدية (Firewalls) المستخدمة في المصارف حالياً.

4.2.8 المخاطر النظامية (Systemic Risks)

تنشأ المخاطر النظامية عندما يؤدي عجز أحد المشاركين في نظام الدفع (مثل بنك كبير أو غرفة مقاصة) عن الوفاء بالتزاماته المالية إلى عجز مشاركين آخرين عن الوفاء بالتزاماتهم، مما يهدد استقرار النظام المالي ككل.

- في أنظمة التسوية الآنية (RTGS)، نقص السيولة لدى أحد المصارف الكبرى (مثل مصرف الجمهورية في ليبيا) قد يؤدي إلى تكدس أوامر الدفع في طوابير الانتظار، مما يجمّد السيولة في السوق ويمنع المصارف الأخرى من استلام مستحقاتها.

5.2.8 مخاطر الطرف الثالث (Third–Party Risks – TPRM)

تعتبر إدارة مخاطر الطرف الثالث من أعقد التحديات في البيئة التشاركية ويمكن تأصيل هذه المخاطر نظرياً من خلال 'نظرية الوكالة(Agency Theory) '، حيث يمثل المصرف 'الأصيل (Principal) 'ومزود الخدمة التقنية 'الوكيل ' .(Agent)تنشأ الإشكالية هنا نتيجة 'عدم تماثل المعلومات(Information Asymmetry) '، حيث يمتلك مزود الخدمة تفاصيل دقيقة عن كفاءة أنظمته الأمنية قد لا يدركها المصرف بالكامل. هذا التفاوت قد يخلق ما يُعرف بـ 'الخطر الأخلاقي ' (Moral Hazard)، حيث قد يميل الوكيل (شركة التقنية) إلى تقليص استثماراته في ضوابط الحماية لخفض التكاليف التشغيلية، معتمداً على حقيقة أن المصرف (الأصيل) هو من سيتحمل التبعات القانونية والضرر الأكبر في السمعة عند حدوث اختراق. المبدأ الحاكم هنا هو: "يمكن للمصرف تفويض العمليات، لكنه لا يستطيع تفويض المسؤولية".(Agency Theory)

- إذا فشلت شركة معالجة مدفوعات متعاقدة مع المصرف في حماية بيانات العملاء، فإن المصرف هو من يتحمل المسؤولية القانونية وتضرر السمعة.
- في ليبيا، أصدر المصرف المركزي تعليمات مشددة في 2024 و2025 لتنظيم العلاقة مع شركات الدفع، مؤكداً على ضرورة وجود تراخيص سارية ورقابة مستمرة.(Basel Committee, 2024)

6.2.8 المخاطر الجيوسياسية والسيادية(Geopolitical & Sovereign Risks)

لم تعد أنظمة الدفع مجرد أدوات مالية وتكنولوجية، بل أصبحت من أهم أصول "البنية التحتية السيادية الحساسة " .(Critical Sovereign Infrastructure)وتبرز المخاطر الجيوسياسية في البيئة المتكاملة من خلال عدة محاور:

أ. **تسييس البنية التحتية المالية :(Politicization of Financial Infrastructure)**

في بيئة تعاني من انقسامات أو توترات سياسية، يمكن استخدام الأنظمة المركزية (مثل المحولات الوطنية) كأدوات ضغط سياسي. الانقسام السياسي قد يؤدي إلى شلل في اتخاذ القرارات الرقابية أو تجميد أصول بعض المصارف المربوطة بالشبكة لأسباب غير مالية.

ب. **الحروب السيبرانية المدعومة من دول أو جهات سياسية:(State-Sponsored Cyber Warfare)**

يختلف هذا التهديد عن الاحتيال المالي العادي (الذي يهدف للسرقة). الهجمات الجيوسياسية تهدف إلى التخريب، وزعزعة الثقة في النظام المالي الوطني، وإحداث فوضى اقتصادية) مثل هجمات الحرمان من الخدمة الموزعة DDoS على بوابات الدفع الوطنية لتعطيل التجارة في دولة ما.

ت. **مخاطر العقوبات والامتثال الدولي:(Sanctions & International Compliance)**

الشراكات مع أطراف خارجية أو الاعتماد على تقنيات مستوردة قد يضع المصارف تحت طائلة العقوبات الدولية المعقدة. أي تغير في المشهد الجيوسياسي قد يمنع المصارف المحلية من الوصول إلى الخوادم السحابية أو تحديثات الأنظمة الأمنية مثل أنظمة SWIFT أو مزودي الحوسبة السحابية العالميين.

ث. **تأثير النزاعات على البنية التحتية الفيزيائية :**

الصراعات الجيوسياسية غالباً ما يرافقها تخريب متعمد أو عرضي لشبكات الطاقة وكابلات الاتصالات، مما يضرب في مقتل "الاعتمادية المتبادلة" لأنظمة الدفع ويؤدي إلى انهيارها محلياً.

3.8 وسائل الرقابة والتدقيق في البيئة المتكاملة

لمواجهة هذه المخاطر المتشابكة، لم تعد أساليب الرقابة التقليدية (Post-audit) كافية، بل برزت الحاجة إلى أطر رقابية استباقية وتكنولوجية.

1.3.8 الإطار الرقابي للمصارف المركزية (Supervisory Framework)

يقع العبء الأكبر على المصرف المركزي لضمان سلامة النظام المتكامل. تشمل الأدوات الرقابية الحديثة:

أ. **الترخيص والتنظيم القائم على النشاط:** الانتقال من تنظيم المؤسسات إلى تنظيم الأنشطة. أي جهة تمارس نشاط الدفع الإلكتروني، سواء كانت بنكاً أو شركة تقنية، يجب أن تخضع لرقابة المصرف المركزي. يتضح هذا في قوائم الشركات المرخصة في ليبيا وتواريخ تجديد تراخيصها.[25]

ب. **فرض المعايير التقنية (Standardization):** إلزام جميع الأطراف بمعايير موحدة لتبادل الرسائل المالية (مثل ISO 20022) ومعايير أمنية (مثل PCI-DSS) لضمان أن التكامل لا يأتي على حساب الأمان ولضمان أن التكامل لا يأتي على حساب الأمان. ويشمل ذلك تبني مبادئ لجنة بازل للعمليات المصرفية الإلكترونية-Basel Committee on e) (Bankingومبادئ البنية التحتية للأسواق المالية(PFMI) ، التي تؤكد على ضرورة وجود 'إدارة مخاطر شاملة' تغطي كافة المشاركين في سلسلة الدفع، وليس المصرف فقط.

ج. **المراقبة المباشرة للبنية التحتية:** في تحول استراتيجي، اتجه مصرف ليبيا المركزي في أواخر 2024 نحو تعزيز سيطرته المباشرة على "الموزع الوطني" ونقل إدارته أو الإشراف اللصيق عليه، لضمان استمرارية الخدمة واعتبارها مسألة "سيادة وطنية".(PCI SSC, 2022)

2.3.8 استراتيجيات إدارة المخاطر الداخلية (Internal Risk Management)

يجب على المصارف تبني استراتيجيات دفاعية متقدمة:

أ. **نموذج خطوط الدفاع الثلاثة المحدث:** دمج الأمن السيبراني في خط الدفاع الأول (الوحدات التشغيلية)، وتعزيز دور إدارة المخاطر في مراقبة الشركاء (خط الدفاع الثاني)، والتدقيق التقني المستمر (خط الدفاع الثالث).

ب. **العناية الواجبة للطرف الثالث (Third-Party Due Diligence):** قبل الارتباط بأي شركة Fintech، يجب على المصرف إجراء فحص دقيق لقدراتها التقنية، ووضعها المالي، وامتثالها الأمني.

ج. **خطط استمرارية الأعمال والتعافي من الكوارث (BCP/DR):** وجود مراكز بيانات بديلة (Disaster Recovery Sites) وأنظمة احتياطية قادرة على العمل فور تعطل النظام الرئيسي، وهو درس مستفاد بقوة من انقطاعات 2025 في ليبيا.

4.8 تحليل الواقع الليبي – تحديات وفرص التكامل (2020-2025)

يسقط هذا الفصل المفاهيم النظرية على الواقع العملي للقطاع المصرفي الليبي، مستعرضاً التطورات الدراماتيكية التي شهدها القطاع في السنوات الأخيرة.

1.4.8 واقع البنية التحتية والتشريعية في ليبيا

شهدت ليبيا في عامي 2024 و2025 ثورة تنظيمية وتقنية في مجال الدفع الإلكتروني، مدفوعة بالحاجة الملحة لمعالجة أزمة السيولة النقدية المزمنة.

أ. **القرارات الإلزامية:** أصدرت حكومة الوحدة الوطنية القرار رقم 135 لسنة 2025، الذي يلزم كافة الأنشطة التجارية والخدمية بتوفير وسائل دفع إلكتروني، مع فرض عقوبات صارمة تصل إلى سحب التراخيص وإغلاق المحال للمخالفين. هذا القرار نقل الدفع الإلكتروني من "خيار" إلى "إلزام قانوني".

ب. **تطوير الخدمات:** أطلق المصرف المركزي مشاريع الدفع الفوري (Instant Payments) وخدمات الدفع عبر رمز الاستجابة السريعة (QR Code) في أغسطس 2024، لتمكين التحويل اللحظي للأموال بين الأفراد والتجار عبر مختلف المصارف.

2.4.8 تحديات الموزع الوطني وشركة معاملات

رغم التقدم المحرز، يواجه نموذج "الموزع الوطني الموحد" تحديات جسيمة:

أ. **انقطاع أكتوبر 2025:** تعرض الموزع الوطني لانقطاع كبير أدى إلى توقف شبه تام لخدمات نقاط البيع والصراف الآلي في البلاد. هذا الحادث كشف عن هشاشة في البنية التحتية ومركزية المخاطر. استدعى ذلك تدخلاً عاجلاً من محافظ المصرف المركزي، الذي أكد أن الموزع "بنية تحتية سيادية" لا يُقبل توقفها، ووجه بضرورة رفع كفاءة مراكز البيانات وتوفير البدائل.

ب. **الشراكة مع القطاع الخاص:** في محاولة لتخفيف الضغط وتوزيع المخاطر، سمح المصرف المركزي لشركات خاصة كبرى مثل "تداول" بربط شبكاتها مع الموزع الوطني. هذا التكامل يعزز الانتشار ولكنه يتطلب بروتوكولات ربط (Interfaces) محكمة لمنع انتقال الثغرات الأمنية من الشبكات الخاصة إلى الشبكة الوطنية. Basel) Committee (2024))

3.4.8 الأمن السيبراني في القطاع المصرفي الليبي

تشير تقارير الهيئة الوطنية لأمن المعلومات (NISSA) لعام 2024 إلى وضع مقلق فيما يخص الأمن السيبراني في ليبيا.

أ. أظهرت التقييمات وجود ثغرات عالية الخطورة (High-severity vulnerabilities) في أنظمة عدد كبير من المؤسسات الحكومية والمالية، مع ضعف في الالتزام بمعايير الحوكمة الأمنية.

ب. تم رصد نشاطات برمجيات خبيثة ومحاولات اختراق تستهدف البنية التحتية، مما يؤكد أن التوسع في الدفع الإلكتروني لم يواكبه تحصين أمني كافٍ، مما يضع أموال المودعين وبياناتهم في دائرة الخطر.

4.4.8 الانقسام المؤسسي والتقلبات الجيوسياسية في ليبيا تُعد البيئة الليبية نموذجاً فريداً لدراسة المخاطر الجيوسياسية على أنظمة الدفع؛ حيث يتقاطع التكامل التقني مع الهشاشة السياسية.

أ. خطر التجاذبات السياسية على "الموزع الوطني :"نظراً لأن شركة "معاملات" تمثل الشريان الرئيسي لربط المصارف التجارية (كالجمهورية والصحاري)، فإن أي أزمة سياسية تتعلق بإدارتها أو إغلاق مقراتها أو قطع الاتصالات عنها يمثل "صدمة جيوسياسية" تتحول فوراً إلى أزمة سيولة وشلل تجاري في كافة أنحاء البلاد.

ب. ازدواجية المرجعيات الرقابية :على الرغم من جهود التوحيد، إلا أن القطاع المصرفي الليبي عانى لفترات من انقسامات أثرت على استراتيجيات إدارة المخاطر وتوحيد المعايير الأمنية(Compliance Standards) ، مما جعل بيئة الشراكة المصرفية تعمل في حقل ألغام قانوني وسياسي.

ت. السيادة على البيانات :(Data Sovereignty) في ظل هذه التقلبات، تبرز مخاوف جيوسياسية حول مكان تخزين بيانات العملاء وحركتهم المالية، ومدى قدرة الأطراف المختلفة (سواء كانت مؤسسات محلية متنافسة أو مزودي خدمات أجانب) على الوصول إلى هذه البيانات واستغلالها.

9. الإطار العملي للدراسة:

1.9 منهج الدراسة

اعتمدت الدراسة على المنهج الوصفي التحليلي، حيث يهدف هذا المنهج إلى وصف ظاهرة التكامل المصرفي وتقييم أثرها على إدارة المخاطر الجيوسياسية والنظامية كما هي في الواقع، ومن ثم تحليل البيانات المجمعة عبر الاستبانة لقياس أثر المتغير المستقل على المتغير التابع واستخراج النتائج والتوصيات.

2.9مجتمع وعينة الدراسة

أ. **مجتمع الدراسة** :يتمثل في كافة الموظفين العاملين في الإدارات ذات الصلة (إدارة المخاطر، إدارة تقنية المعلومات، العمليات المصرفية الإلكترونية، والشراكات الاستراتيجية) في المصارف التجارية الليبية المحددة في الاستبانة (مصرف الجمهورية، مصرف الصحاري).

ب. **عينة الدراسة** :تم اختيار عينة قصدية (عمدية) من المجتمع المستهدف، نظراً لأن الاستبانة موجهة لذوي الاختصاص والخبرة (مدراء إدارات، رؤساء أقسام، موظفين مختصين) القادرين على استيعاب وتقييم الأبعاد التقنية والجيوسياسية معاً.

3.9 أداة الدراسة

تم تصميم الاستبانة بناءً على الأدبيات النظرية والدراسات السابقة، وتكونت من قسمين:

أ. **البيانات الديموغرافية** :المصرف، المسمى الوظيفي، سنوات الخبرة، المؤهل العلمي.

ب. **محاور الدراسة** :تم استخدام مقياس "ليكرت الخماسي (5-point Likert Scale) "لتحديد درجة الموافقة (من 1 "غير موافق بشدة" إلى 5 "موافق بشدة")، وانقسمت إلى:

- **المحور الأول (المتغير المستقل)** :التكامل والشراكة المصرفية، وتضمن (9) فقرات موزعة على ثلاثة أبعاد: (التكامل التقني، الشراكات الاستراتيجية، وتوحيد المعايير).
- **المحور الثاني (المتغير التابع)** :فاعلية إدارة المخاطر الجيوسياسية لأنظمة الدفع الإلكتروني، وتضمن (8) فقرات موزعة على ثلاثة أبعاد متخصصة: (مخاطر البنية التحتية السيادية والانقسام التشغيلي،

التهديدات السيبرانية الجيوسياسية والعدوى النظامية، والمخاطر القانونية وتضارب التشريعات في بيئة متقلبة).

4.9 عرض وتحليل النتائج واختبار الفرضيات

1.4.9 تمهيد

يتناول هذا الفصل عرضاً لنتائج التحليل الإحصائي للبيانات التي تم جمعها عبر الاستبانة الموزعة على موظفي عينة الدراسة (مصرف الجمهورية ومصرف الصحاري)، حيث يبدأ باختبار جودة الأداة، ثم وصف خصائص العينة، يليه التحليل الوصفي لمتغيرات الدراسة (التكامل المصرفي، وإدارة المخاطر الجيوسياسية)، وأخيراً اختبار الفرضيات الثلاث للدراسة ومناقشتها

2.4.9اختبار صدق وثبات الأداة(Reliability)

للتأكد من اتساق وموثوقية فقرات الاستبانة المخصصة لقياس الشراكة المصرفية وأثرها على المخاطر الجيوسياسية، تم استخدام معامل "ألفا كرونباخ ."بعد المعالجة الإحصائية واستبعاد الفقرات الضعيفة، جاءت النتائج كما يلي:

جدول رقم (2) نتائج اختبار الثبات

البيان	عدد الفقرات	قيمة ألفا كرونباخ	مستوى الثبات
جميع محاور الاستبانة	15	0.810	مرتفع جداً

بلغت قيمة معامل الثبات الكلية (0.810)، وهي قيمة أعلى من الحد المقبول إحصائياً (0.70)، مما يؤكد أن الأداة (الاستبانة) تتمتع بموثوقية عالية، وقادرة على قياس أبعاد المخاطر الجيوسياسية والتقنية بشكل دقيق، وصالحة للتحليل العلمي.

3.4.9 وصف خصائص عينة الدراسة (التحليل الديموغرافي)

فيما يلي توزيع أفراد العينة البالغ عددهم (40) مبحوثاً:

جدول رقم (3) توزيع أفراد العينة

المتغير	الفئة	التكرار	النسبة المئوية (%)
المصرف	مصرف الجمهورية	20	%50.0
	مصرف الصحاري	20	%50.0
المسمى الوظيفي	رئيس قسم	10	%25.0
	موظف مختص	30	%75.0
الخبرة	أقل من 5 سنوات	4	%10.0
	من 5 – 10 سنوات	22	%55.0
	أكثر من 10 سنوات	14	%35.0
المؤهل	دبلوم	10	%25.0
	بكالوريوس	16	%40.0
	دراسات عليا	14	%35.0

تشير الجداول إلى أن العينة متوازنة وممثلة بشكل دقيق لمصرفي (الجمهورية والصحاري). وتتميز العينة بالخبرة العملية العالية، حيث أن (90%) من المبحوثين يمتلكون خبرة تزيد عن 5 سنوات، و(75%) يحملون مؤهلات جامعية وعليا. هذه

الخصائص تعزز من مصداقية الإجابات، وتؤكد بشكل خاص على قدرة الباحثين على استيعاب وتقييم المخاطر الجيوسياسية المعقدة، نظراً لمعاصرتهم للتقلبات السياسية، والانقسامات المؤسسية، والتحولات التقنية التي مر بها القطاع المصرفي الليبي وتأثيرها المباشر على أنظمة الدفع خلال السنوات الماضية.

4.4.9 التحليل الوصفي لمتغيرات الدراسة

يهدف هذا الجزء لاستعراض مستوى "التكامل" ومستوى "إدارة المخاطر" من وجهة نظر المبحوثين، وهو ما يمهد لاختبار الفرضيات.

جدول رقم (4) تحليل متغيرات الدراسة

م	العبارة (الفقرة)	المتوسط الحسابي	الانحراف المعياري	مستوى الموافقة	الترتيب العام
أولاً	**المحور الأول: التكامل والشراكة المصرفية (المتغير المستقل)**				
1	يرتبط المصرف بشكل فعال مع "الموزع الوطني" (Moamalat) مما يتيح تبادل البيانات بسلاسة.	4.55	0.597	مرتفع جداً	1
2	يمتلك المصرف بنية تحتية مرنة تسمح بقبول بطاقات المصارف المحلية الأخرى (Interoperability).	4.50	0.599	مرتفع جداً	2
3	توجد واجهات ربط موحدة (APIs) آمنة تسمح بتكامل أنظمتنا مع تطبيقات الدفع الخارجية.	4.25	0.898	مرتفع جداً	5
4	لدى المصرف شراكات فعالة مع شركات التقنية المالية (Fintech) لتطوير حلول دفع آمنة.	4.10	0.777	مرتفع	7
5	يلتزم المصرف بتطبيق معايير أمنية موحدة (مثل PCI–DSS) متفق عليها ضمن الشبكة الوطنية.	4.05	0.749	مرتفع	8
6	يساهم الربط الشبكي الموحد بين المصارف في تسريع عمليات المقاصة والتسوية الإلكترونية.	3.90	0.708	مرتفع	11
7	يشارك المصرف في تكتلات أو لجان مشتركة مع مصارف أخرى لمناقشة التحديات الأمنية.	3.65	0.735	مرتفع	13
8	هناك تنسيق مستمر مع شركات الاتصالات ومزودي الخدمة لضمان استقرار قنوات الاتصال.	3.60	0.590	مرتفع	14
9	توجد إجراءات موحدة للتعرف على العميل (KYC) تسهل التعامل مع العملاء المشتركين.	3.10	0.900	متوسط	16
ثانياً	**المحور الثاني: فاعلية إدارة المخاطر الجيوسياسية والنظامية (المتغير التابع)**				
10	الانقطاعات المتكررة للاتصالات والطاقة لأسباب أمنية أو سياسية تهدد استمرارية الربط الشبكي المشترك.	4.45	0.612	مرتفع جداً	3

11	الاعتماد المفرط على الموزع الوطني يجعله بنية تحتية سيادية حرجة عرضة للتأثر بالتجاذبات السياسية.	4.40	0.655	مرتفع جداً	4
12	الانقسامات السياسية والمؤسسية تعيق جهود المصارف في توحيد استراتيجيات الاستجابة للمخاطر.	4.30	0.710	مرتفع جداً	6
13	التغيرات المفاجئة في التشريعات والقرارات السيادية تزيد من المخاطر القانونية والامتثال على المصارف المترابطة.	4.15	0.785	مرتفع	9
14	ضعف تبادل المعلومات الأمنية بين المصارف يسهل انتشار "العدوى النظامية" عند حدوث أزمات.	4.05	0.822	مرتفع	10
15	الشراكة مع مزودين تقنيين (أطراف ثالثة) في بيئة سياسية متقلبة تزيد من احتمالية تسريب البيانات السيادية.	3.95	0.760	مرتفع	12
16	تعرضت البنية التحتية للمدفوعات لتهديدات سيبرانية ذات طابع تخريبي أو مدعومة من جهات خارجية (جيوسياسية).	3.80	0.880	مرتفع	15
17	توجد مراكز بيانات بديلة (DR Sites) موزعة جغرافياً قادرة على العمل فوراً عند حدوث صدمات سياسية للمركز الرئيسي.	2.80	0.915	متدني	17
	المتوسط العام الكلي للأداة	**3.98**	--	**مرتفع**	

يُلاحظ من الجدول السابق وجود دلالات هامة تخدم مشكلة الدراسة:

- سجلت فقرات "الربط التقني" في المحور الأول متوسطات مرتفعة جداً (مثل الفقرة 1 بمتوسط 4.55)، ما يعكس نجاح المصارف في الاندماج التقني. ولكن في المقابل، يرى المبحوثين أن هذا الاندماج محفوف بمخاطر جيوسياسية عالية، حيث جاءت الفقرات المتعلقة المبحوثين بتأثير الانقسامات السياسية وانقطاع الاتصالات (الفقرات 10، 11، 12) بمتوسطات تتجاوز (4.30).
- اتفقت العينة بدرجة "مرتفع جداً" (4.40) على أن الاعتماد المفرط على الموزع الوطني يحوله إلى "بنية سيادية حرجة" مهددة بالتجاذبات السياسية.
- يُعد انخفاض تقييم الفقرة رقم 17 (وجود مراكز بيانات بديلة موزعة جغرافياً) والتي سجلت تقييماً "متدنياً" بمتوسط (2.80)، أقوى مؤشر على ضعف المرونة التشغيلية وعدم جاهزية القطاع المصرفي لامتصاص الصدمات الجيوسياسية أو الأمنية التي قد تضرب المركز الرئيسي للشبكة.

5.4.9اختبار الفرضيات(Hypothesis Testing)

أ. اختبار الفرضية الأولى:

- **نص الفرضية**" :توجد علاقة طردية ذات دلالة إحصائية بين مستوى التكامل التقني والتشغيلي (Interoperability)بين مصرفي (الجمهورية والصحاري) والشبكة الوطنية من جهة، وبين تعرضهما للمخاطر

الجيوسياسية والنظامية من جهة أخرى؛ حيث يسهل الترابط العالي انتقال "العدوى " (Contagion) وتضخم الأزمات المالية عند حدوث صدمات سياسية أو أمنية مفاجئة".

جدول رقم (5) معامل ارتباط بيرسون لاختبار الفرضية الأولى

المتغيرات	قيمة الارتباط (R)	مستوى الدلالة (Sig)	القرار
التكامل والشراكة * التعرض للمخاطر الجيوسياسية والنظامية	0.378	0.016	قبول الفرضية

أظهرت النتائج وجود علاقة ارتباط طردية (موجبة) وذات دلالة إحصائية حيث بلغت قيمة (Sig = 0.016) وهي أقل من مستوى الدلالة المعتمد (0.05). هذا يعني قبول الفرضية الأولى، ويُفسر ذلك بأنه كلما ارتفع مستوى التكامل والاعتماد المتبادل بين المصارف والموزع الوطني، زادت درجة الانكشاف والتعرض للمخاطر الجيوسياسية .فالترابط الشبكي الوثيق يجعل النظام المالي يعمل ككتلة واحدة؛ مما يسهل انتقال "العدوى النظامية" ويؤدي إلى شلل القطاع بالكامل عند تعرض البنية التحتية المركزية لأي صدمات سياسية، أو أمنية، أو انقطاعات سيادية للاتصالات والطاقة، بدلاً من بقاء الأزمة محصورة في نطاق مؤسسة واحدة.

ب. اختبار الفرضية الثانية:

- **نص الفرضية**" :يؤدي الاعتماد المفرط على 'المحولات الوطنية المركزية' في ظل بيئة سياسية متقلبة، ودون وجود خطط طوارئ بديلة وموزعة جغرافياً، إلى خلق نقاط فشل موحدة (Single Points of Failure) ذات طابع سيادي تهدد الاستقرار المالي الوطني برمته".

للتأكد من صحة هذه الفرضية، تم استخدام تحليل الانحدار الخطي البسيط (Simple Linear Regression) لقياس أثر الاعتماد على التكامل المركزي (كمتغير مستقل) على تضخم المخاطر الجيوسياسية ونقاط الفشل (كمتغير تابع):

جدول رقم (6) نتائج تحليل الانحدار البسيط لاختبار الفرضية الثانية

البيان	القيمة	التفسير
معامل الارتباط (R)	0.378	علاقة طردية متوسطة
معامل التحديد (R Square)	0.143	المتغير المستقل (الاعتماد المركزي) يفسر 14.3% من التغيرات في المتغير التابع (تضخم نقاط الفشل)
قيمة (F)	6.337	النموذج الإحصائي صالح لقياس الأثر
مستوى الدلالة (Sig)	0.016	يوجد أثر ذو دلالة إحصائية (0.05 > Sig)
قيمة المعامل (Beta)	0.378	الأثر إيجابي (طردي)

معادلة خط الانحدار:

بناءً على النتائج، يمكن صياغة مسار التأثير كالتالي:

المخاطر الجيوسياسية ونقاط الفشل = ثابت الانحدار + (0.378 × مستوى الاعتماد على التكامل المركزي).

بما أن مستوى الدلالة (0.016) أقل من (0.05)، وقيمة (F) دالة إحصائياً، فإننا **نقبل الفرضية الثانية** .يُفسر ذلك بأن الاعتماد المفرط والوحيد من قبل مصرفي (الجمهورية والصحاري) على بنية تحتية مركزية واحدة (الموزع الوطني) له أثر معنوي وطردي في خلق "نقاط فشل موحدة". وتشير قيمة معامل التحديد (14.3%) إلى أن هذا الاعتماد المركزي يفسر جزءاً مهماً من انكشاف المصارف على المخاطر السيادية؛ حيث أن غياب خطط الطوارئ ومراكز البيانات البديلة الموزعة

جغرافياً يجعل النظام المالي عرضة للشلل التام في حال تعرض الموزع الرئيسي لأي صدمات أو انقطاعات ناتجة عن تقلبات البيئة السياسية والأمنية.

ج. اختبار الفرضية الثالثة (باستخدام التحليل الوصفي):

- **نص الفرضية**" :إن تطبيق مصرفي (الجمهورية والصحاري) لاستراتيجيات إدارة مخاطر الطرف الثالث (TPRM) والمعايير الدولية (PCI–DSSو ISO 27001) لا يزال دون المستوى المطلوب لاحتواء الصدمات الجيوسياسية والتهديدات السيبرانية المدعومة من جهات خارجية في بيئة متكاملة تفتقر إلى الاستقرار".

التحليل الإحصائي والتفسير :للتحقق من صحة هذه الفرضية، تم النظر في المتوسطات الحسابية للفقرات الخاصة بـ "الشراكة الأمنية، ومكافحة التهديدات، وإدارة الطرف الثالث" ضمن التحليل الوصفي (الجدول رقم 4):

- بلغ متوسط تقييم القدرة على "الكشف المبكر عن أنماط الاحتيال والتهديدات المعقدة التي تستهدف عدة مصارف " (3.05).
- بلغ متوسط تقييم "مشاركة الموارد والخبرات الأمنية بين المصارف لاحتواء الأزمات.(3.10) "
- هذه القيم تقع ضمن فئة "الموافق بدرجة متوسطة/محايدة"، وهي تمثل الحد الأدنى للمقبولية في العمليات المصرفية التقليدية، ولكنها تُعد غير كافية إطلاقاً (دون المستوى المطلوب) عند التعامل مع بنية تحتية سيادية تواجه تهديدات جيوسياسية متقدمة.

إن الانخفاض الحاد في المتوسطات الحسابية لفقرات الجانب الأمني التشاركي وإدارة مخاطر الأطراف الثالثة (والتي تكاد تلامس درجة الحياد 3.00)، مقارنةً بالمتوسطات المرتفعة جداً لفقرات الجانب التقني والربط الشبكي (والتي تجاوزت 4.50)، يكشف عن فجوة خطيرة. هذا التباين يدعم بقوة صحة الفرضية القائلة بأن الإجراءات الأمنية الحالية لمصرفي (الجمهورية والصحاري) تسبقها التكنولوجيا بخطوات؛ مما يجعل القطاع المصرفي المترابط مكشوفاً وعاجزاً عن احتواء أي هجمات سيبرانية أو اختراقات لسلاسل التوريد (Supply Chain Attacks) قد تكون مدعومة من جهات خارجية أو ناتجة عن تقلبات جيوسياسية .**وبذلك، نقبل الفرضية الثالثة.**

10. النتائج والتوصيات

10.1نتائج الدراسة

1. أظهرت الدراسة وجود تباين واضح لدى مصرفي (الجمهورية والصحاري) بين النجاح في تحقيق مستويات عالية من التكامل التقني والربط الشبكي، وبين التواضع الشديد في الإجراءات الأمنية والسيادية المشتركة؛ حيث تبين أن التطور في البنية التحتية للاتصالات يسبق بكثير التطور في بروتوكولات الحماية القادرة على امتصاص الصدمات الجيوسياسية.
2. كشفت النتائج عن اعتماد المصارف بشكل شبه كلي على "الموزع الوطني" كبوابة رئيسية للمعاملات. هذا الاعتماد يخلق مخاطر تركز عالية ونقطة فشل موحدة (Single Point of Failure) ذات طابع سيادي، تجعل القطاع المصرفي بأكمله عرضة للشلل التام في حال حدوث صراعات سياسية، أو أمنية، أو انقطاعات متعمدة للاتصالات في نقطة المركز.
3. أثبتت الدراسة أن انخراط المصارف في شراكات مع الشبكة الوطنية دفعها نحو تحسين أنظمة إدارة المخاطر الداخلية، ولكن هذا التحسن اقتصر غالباً على استيفاء متطلبات "الربط التقني" المفروضة، ولم يرقَ إلى بناء حوائط صد ضد التقلبات والتهديدات السيبرانية ذات الطابع التخريبي أو السياسي.

4. بينت النتائج قصوراً حاداً في آليات الإنذار المبكر وتبادل المعلومات حول التهديدات السيبرانية بين المصارف وبعضها البعض؛ حيث تعمل إدارات المخاطر كـ "جزر منعزلة" متأثرة بالانقسامات المؤسسية، مما يسهل انتقال "العدوى النظامية" واختراق الشبكة الوطنية بأكملها عبر أضعف حلقاتها.
5. أوضحت الدراسة أن الأنظمة الحالية فعالة في تنفيذ المعاملات اليومية، لكنها تفتقر إلى القدرة على كشف أنماط الهجمات المعقدة والمنسقة (كالحروب السيبرانية) التي تستهدف عدة مصارف في وقت واحد، مما يشير إلى أن أدوات المراقبة تقليدية ولا تواكب التهديدات الجيوسياسية الحديثة.
6. توصلت الدراسة إلى أن المصارف تركز جهودها على حماية بيئتها الداخلية، بينما تظل الرقابة على الشركاء الخارجيين ومزودي خدمات التقنية (الطرف الثالث) في بيئة سياسية متقلبة دون المستوى المطلوب، مما يترك ثغرات خطيرة قد تُستغل في هجمات سلاسل التوريد أو تؤدي إلى تسريب بيانات سيادية حساسة.

2.10التوصيات

1. ضرورة قيام مصرف ليبيا المركزي وشركة معاملات بإنشاء مراكز بيانات رديفة وموزعة جغرافياً (Decentralized DR Sites)، واعتماد خطط طوارئ سيادية تضمن استمرارية الخدمة عبر قنوات بديلة في حال تعطل المركز الرئيسي نتيجة لأي تجاذبات سياسية أو أمنية أو تقنية.
2. يوصى بإنشاء مركز موحد ومستقل لعمليات الأمن السيبراني يضم كافة المصارف الأعضاء، يهدف إلى مراقبة الشبكة الوطنية على مدار الساعة، وتحييد الانقسامات المؤسسية من خلال تبادل معلومات التهديدات والإنذارات بشكل فوري ولحظي لحماية الأمن القومي المالي.
3. يجب على المصارف فرض شروط تعاقدية صارمة مع شركات التقنية والشركاء الخارجيين، تتضمن اشتراطات صارمة حول "السيادة على البيانات"، والحق في إجراء تدقيق أمني دوري للتأكد من امتثالهم لمعايير أمن المعلومات العالمية قبل منحهم حق الوصول للشبكة.
4. توجيه الاستثمارات نحو أنظمة مراقبة متطورة تعتمد على الذكاء الاصطناعي وتعلم الآلة (Machine Learning) لتحليل سلوكيات الدفع عبر الشبكة الموحدة، وكشف الأنماط الشاذة والتهديدات المتقدمة (APT) التي قد تكون مدعومة من جهات خارجية ولا تظهر للمصرف الواحد منفرداً.
5. التوصية بالانتقال الفوري من نماذج الحماية التقليدية إلى نموذج "الثقة الصفرية" في التعامل مع واجهات برمجة التطبيقات(APIs) ، بحيث يتم التحقق الصارم من هوية وأمن كل طلب اتصال يأتي من خارج المصرف، وعدم الوثوق بأي طرف لمجرد أنه شريك داخل الشبكة.
6. توجيه الموارد نحو تدريب الكوادر البشرية في إدارات المخاطر وتقنية المعلومات (خاصة في مصرفي الجمهورية والصحاري) على التعامل مع "المخاطر المترابطة والجيوسياسية"، لضمان وجود خط دفاع بشري واعي قادر على إدارة الأزمات في بيئات العمل المفتوحة وغير المستقرة.

11. قائمة المراجع

أولاً: المراجع العربية:

- حكومة الوحدة الوطنية .(2025) .القرار رقم (135) بشأن إلزام الأنشطة التجارية والخدمية بتوفير وسائل الدفع الإلكتروني .طرابلس، ليبيا.
- شركة معاملات للخدمات المالية .(2024) .التقرير السنوي حول أداء الموزع الوطني وتكامل القطاع الخاص . ليبيا.

- مصرف ليبيا المركزي .(2024) .تعليمات تنظيم العلاقة بين المصارف وشركات الدفع الإلكتروني .إدارة الرقابة على المصارف والنقد.
- مصرف ليبيا المركزي .(2025) .تقرير الاستقرار المالي وحوادث استمرارية الأعمال في أنظمة الدفع .طرابلس.
- الهيئة الوطنية لأمن المعلومات .(2024) .(NISSA) التقرير الوطني لتقييم الثغرات السيبرانية في القطاع العام والمالي .ليبيا.

ثانياً: المراجع الأجنبية:

- Basel Committee on Banking Supervision. (2024). Principles for operational resilience and third-party risk management.
- PCI Security Standards Council (PCI SSC). (2022). Payment Card Industry Data Security Standard (PCI DSS) v4.0.
- Bank for International Settlements (BIS). (2021). Central bank digital currencies: operating models and control frameworks. Basel, Switzerland.
- Perrow, C. (1999). Normal Accidents: Living with High-Risk Technologies. Princeton University Press.
- World Bank. (2020). Retail Payments: A Vital Component of Modern Financial Infrastructure. Washington, DC.