الآثار الاقتصادية والمالية للهجمات السيبرانية في ظل التحول الرقمي: النتائج، التجارب والحلول – مع الإشارة لحالة الجزائر –

Economic and Financial Effects of Cyber Attacks in the Light of Digitization: Results, Experiences and Solutions- Algeria case study -

دراعو عزالدين

جامعة محمد بن أحمد وهران 2– وهران (الجزائر)، draou.azzeddine@univ-oran2.dz

تاريخ الارسال: 2022/04/22 **تاريخ القبول:** 2022/06/25 **تاريخ النشر:** 2022/06/30

ملخص:

تهدف هذه الدراسة إلى تبيان الآثار الاقتصادية والمالية للهجمات السيبرانية جراء اللجوء إلى التحول الرقمي، حيث تتأثر الكثير من الشركات، المؤسسات المالية وحتى الدول بعمليات القرصنة. كما تسعى الدراسة أيضا لوضع الاستراتيجيات الملائمة لحماية البيانات لدى القطاعات الحساسة، بناء على تشخيص الأسباب المؤدية للهجمات السيبرانية، وكذا الأطراف المسؤولة عنها. في المقابل، سنعتمد على المنهج الوصفي التحليلي، وكذا دراسة حالة العديد من الدول ومختلف الاحصائيات المتاحة خلال سنوات عديدة.

توصلت الدراسة إلى ضرورة الحد من الهجمات السيبرانية عن طريق وضع استراتيجيات تحمي البيانات لدى المؤسسات والدول، حيث أن هذه الهجمات أدت إلى خسائر كبيرة لدى مختلف المؤسسات وخاصة المصارف. وعليه، يبقى التعاون الدولي والاستفادة من تجارب الدول الرائدة في الأمن السيبراني هو الحل لحماية القطاعات الاقتصادية والمالية من قرصنة واختراق البيانات.

كلمات مفتاحية: التحول الرقمي، الأمن السيبراني، الهجمات السيبرانية، الآثار المالية و الاقتصادية، الجزائر

تصنيفات JEL : G2، K1، O3.

Abstract:

This study examine the economic and financial effects of cyber attacks as a result of resorting to digitization, as many companies, financial institutions and even countries are affected by piracy operations. The study also seeks to develop appropriate strategies to protect data in sensitive sectors, based on diagnosing the causes of cyber attacks. however, we will rely on the descriptive analytical method, as well as a case study of many countries and the various statistics available over many years.

as results, we found the need to reduce cyber-attacks by developing strategies that protect data for institutions and countries, as these attacks led to great losses for various institutions, especially banks. Accordingly, international cooperation and benefiting from the experiences of leading countries in cybersecurity remains the solution to protect the economic and financial sectors from hacking and data penetration.

Keywords: digitization, cyber security, cyber attacks, financial and economic impacts, Algeria

JEL Classification Cods : G2 ،K1, O3.

المؤلف المرسل: دراعو عزالدين، **الإيميل:** draou.azzeddine@univ-oran2.dz

المقدمة:

يشهد الاقتصاد العالمي عدة تحولات وتغيرات جراء دخول عالم الرقمنة، وما ينجر عنه من استبدال للمعاملات التقليدية بتعاملات رقمية. لكن وفي المقابل، تتعرض الكثير من الجهات سواء حكومات أو مؤسسات أو أفراد إلى هجمات سيبرانية تتسبب في خسائر مالية فادحة أحيانا، خاصة إذا علمنا أن معظم الدول تعتمد على الاقتصاد الرقمي بما في ذلك الدول الناشئة، في حين تبقى الدول النامية ومحدودة الدخل بعيدة نوعا ما عن التعاملات الرقمية وبالتالي قلة الخسائر الاقتصادية والمالية الناجمة عن الهجمات السيبرانية.

الإشكالية:

تتمحور إشكالية الدراسة حول: كيف يمكن التقليل والحد من الآثار الاقتصادية والمالية للهجمات السيبرانية في ظل التوجه نحو تحول رقمي للقطاع الاقتصادي والمالي؟

الأسئلة الفرعية:

- ✓ ما هي طبيعة العلاقة بين التحول الرقمي والأمن السيبراني؟
- ✓ كيف تحدث الهجمات السيبرانية؟
- ✓ ما هي الآثار المحتملة للهجمات السيبرانية اقتصاديا وماليا؟
- ✓ ما هي الحلول والاستراتيجيات الملائمة لردع الهجمات السيبرانية؟

الفرضيات:

ولمعالجة إشكالية الدراسة نقترح الفرضيات التالية:

- ✓ تعتبر الهجمات السيبرانية نتيجة طبيعية لسياسة التحول الرقمي وما ينتج عنه من ثغرات رقمية وقانونية؛
- ✓ الالتزام بمعايير الأمن السيبراني يسمح بتقليل الآثار الاقتصادية والمالية للهجمات السيبرانية.

أهمية الدراسة

- تعتبر الدراسة مميزة بحكم تطرقها للجوانب الاقتصادية والمالية للهجمات السيبرانية؛
- تعتمد الدراسة على تحليل المؤشرات المالية للمؤسسات المتضررة من الهجمات السيبرانية؛
- تسمح الدراسة باستشراف الحلول المستقبلية للتخفيف والتصدي للهجمات السيبرانية.

أهداف الدراسة:

- تسعى الدراسة إلى إعطاء مفهوم محدد وبسيط للأمن السيبراني وكذا الهجمات السيبرانية؛
- التركيز على الجوانب المالية والاقتصادية للهجمات السيبرانية بما في ذلك البنوك؛
- التطرق لتجارب الدول في التصدي للقرصنة السيبرانية وتقديم الحلول اللازمة.

منهج الدراسة:

سنعتمد خلال هذه الدراسة على الأسلوب الوصفي التحليلي، بما يسمح بجمع البيانات وتشخيص الإشكالية وفق منهجية علمية سليمة تسمح بالخروج بنتائج هامة حول معالجة الهجمات السيبرانية، بالإضافة لتقنية دراسة الحالة التي تسمح لنا بدراسة تجارب الدول في التعامل مع آثار التحول الرقمي من هجمات سيبرانية و خسائر مالية.

هيكل الدراسة:

يتم تقسيم الدراسة إلى جزئين نظري وتطبيقي. حيث تناول الجزء النظري مفهومي التحول الرقمي والأمن السيبراني خصوصا، بما في ذلك التطرق لأهم أركان الأمن والهجمات السيبرانية. أما الجزء التطبيقي، فقد تناول نبذة عن الهجمات السيبرانية، بالإضافة إلى التطرق لأهم الآثار الاقتصادية والمالية للهجمات السيبرانية، خاصة على المصارف والمؤسسات المالية. أيضا، تم التطرق لتجارب العديد من الدول بما يسمح باستخلاص العبر والحلول لمواجهة الهجمات السيبرانية.

1. الإطار النظري للدراسة:

سيعتمد هذا الإطار على تقديم كل من مفهومي التحول الرقمي، الأمن السيبراني وكذا الهجمات السيبرانية، حيث يتم التطرق إلى كافة الإستراتيجيات والسياسات المتعلقة بالمعلومات وأجهزة الكمبيوتر، البنية التحتية، وبرامج المعلوماتية، بالإضافة للانتقال الرقمي ضمن مجالات الاقتصاد و المالية.

1.1. التحول الرقمي:

1.1.1. مفهوم التحول الرقمي:

اختلف الباحثون في تعريف التحول الرقمي حسب الغاية من جهة، والجهة المخولة بالتحول الرقمي من جهة أخرى. وعليه، فإننا سنحاول تناول المفهوم الأقرب لموضوع الدراسة. فالتحول الرقمي ما هو إلا: " مشروع حكومي يشمل كافة خدمات المؤسسات والقطاعات المختلفة بالدولة، ويتمثل في تحويل الخدمات الحيوية والأساسية المرتبطة بخدمة الأفراد، والمؤسسات، والاستثمارات المختلفة، من شكلها التقليدي إلى الشكل الإلكتروني الذكي، بالاعتماد على التقنيات الحديثة والمتطورة " (معيزي، 2021، صفحة 648)، فالتحول الرقمي يمكن اعتباره بمثابة التغير المتعلق بالتكنولوجيا الرقمية وما يمكن إحداثه من تحول في طريقة العمل، وهو ما من شأنه ضمان خدمات بشكل أسرع وأفضل.

2.1.1. أساسيات حول التحول الرقمي: المتطلبات، التقنيات و المجالات

لضمان تحول رقمي لابد من تحديد الرؤية بوضوح حول مشروع التحول، بالإضافة لإرساء ثقافة التغيير لدى الجميع، بما يسمح بتغيير نموذج التكلفة، وبالتالي بدء الإعمال في السحابة (معيزي، 2021، الصفحات 648-649).

إن عملية التحول الرقمي تمر عبر عدة متطلبات أبرزها دعم الإدارة العليا وتزكيتها للعملية، بالإضافة للدعم البشري عبر كوادر مدربة ومؤهلة. أيضا، فإن الجانب اللوجستي يعتبر مهما مثل توفير الأجهزة الرقمية والبرمجيات الضرورية. في المقابل، هناك تقنيات متعددة للتحول الرقمي من شأنها ضمان الاستمرارية والاستدامة لعملية التحول ولعل أبرزها: تقنية البلوكشين، البينات

الضخمة وتقنية الأمن السيبراني. أخيرا، فإن مجالات تطبيق الرقمنة قد تشمل العديد من القطاعات والمجالات على غرار: الاقتصاد، الصناعة، الصحة والتعليم.

الجدول (01): أساسيات لضمان التحول الرقمي

متطلبات التحول الرقمي	تقنيات التحول الرقمي	مجالات التحول الرقمي
– دعم الإدارة العليا – كفاءات بشرية مؤهلة – متطلبات تقنية (الأجهزة والبرامج)	– الذكاء الاصطناعي – إنترنت الأشياء – الواقع الافتراضي والواقع المعزز – البلوكشين – الطباعة ثلاثية الأبعاد – البيانات الضخمة – الحوسبة السحابية – الأمن السيبراني	– الاقتصاد – الصناعة – التجارة والاستثمار – السياحة – الصحة – التعليم

المصدر: (نسيمة، 2021، صفحة 344)

3.1.1. التحول الرقمي ضمن قطاع الاقتصاد والخدمات المالية:

من بين المجالات والقطاعات التي يمكن أن يشملها التحول الرقمي هو الاقتصاد، فالاقتصاد الرقمي هو: " اقتصاد مبني أساسا على التطور التكنولوجي والمعلوماتي الذي يزيد من فرص نمو وتطور المنتجات والخدمات خصوصا القابلة للتداول التجاري رقميا عبر الشبكات المعلوماتية " (السيد، 2020، صفحة 6). فعلا، فهناك قطاعات اقتصادية كثيرة استفادت من خدمات التحول الرقمي على غرار التجارة والخدمات المالية، وهذا عبر استثمارها في تكنولوجيات المعلومات والاتصالات، لينتج عن ذلك ما يعرف لدينا بالتجارة الإلكترونية والتي استطاعت بذلك تخفيض تكاليف الاستيراد والتصدير، وكذا الصيرفة الإلكترونية والبنوك الإلكترونية وهو ما عزز من فرص الشمول المالي والوصول إلى فئة كبيرة من المتعاملين.

أيضا، يمكن قياس أثر التحول الرقمي في قطاعي التجارة والخدمات المالية كما يلي: (العربية، 2020، الصفحات 70- 71)

- ✓ تطوير وابتكار الحلول الجديدة لمصلحة المتعاملين بما يخدم مصالحهم ويخفض القيود الإدارية؛
- ✓ إتاحة الخدمات المالية عبر التكنولوجيا المالية لذوي الدخل المحدود خاصة في الدول النامية؛
- ✓ زيادة حجم التدفقات المالية عبر مختلف التبادلات التجارية؛
- ✓ تشجيع المنافسة والابتكار والإنتاجية لدى مختلف المتعاملين؛
- ✓ إجراء المعاملات المالية عبر الهواتف المحمولة، الأجهزة اللوحية ومختلف التقنيات الحديثة.

4.1.1. التحول الرقمي والأمن السيبراني:

يعتبر الأمن السيبراني من التقنيات المرافقة والمساهمة في عملية التحول الرقمي حيث يسمح بضمان مستقبل قوي من الحماية الرقمية وأمن المعلومات وحماية الخصوصية الرقمية في التحديات المجتمعية، وكذا التركيز على الأنظمة المبتكرة والجيل القادم والأمان والخصوصية السيبرانية العامة (العربية، 2020، صفحة 181). ولهذا الغرض، يتم نشر إرشادات خاصة حول العمل الآمن

عن بعد وتأمين الأنظمة المعلوماتية، بالإضافة لإنشاء تطبيقات للأمن السيبراني كتوجه ضروري لتطوير الرقمنة واستخدامها الواسع في حالة الأزمات كجائحة كورونا (بشاري، 2020، صفحة 604).

2.1. ماهية الأمن السيبراني:

تطورت المفاهيم التقليدية للأمن ولم تعد تقتصر على الأمن الميداني فقط، بل امتدت إلى مجالات حماية الممتلكات والبيانات المتواجدة على الشبكة العنكبوتية وكذا الشبكات الداخلية. وفي هذا السياق، نشير إلى أن أمن المعلومات يعتبر غير كاف في ظل التحول والثورة الرقمية الحاصلة، وعليه يجب توسيع نطاق الحماية والتأمين من الشبكات الداخلية إلى الشبكات الخارجية والدولية. أين يظهر لنا مفهوم أوسع وأشمل من أمن المعلومات، ألا وهو الأمن السيبراني.

1.2.1. أساسيات حول الأمن السيبراني:

لم يعد يقتصر دور الأمن السيبراني على حماية البيانات فقط، بل امتد مفهومه وماهيته إلى عدة أبعاد وأهداف لابد من دراستها والتعمق فيها.

أ. مفهوم الأمن السيبراني:

السيبرانية تعني فضاء الإنترنت، وهي مرتبطة بكلمة Cyber (وريدة، 2021، صفحة 811). كما أن المجال السيبراني يشمل مختلف قواعد البيانات، الاتصالات وكذا الشبكات (حكيم، 2018، صفحة 107). وفي هذا السايق يستخدم الكثير من الباحثين مؤخرا مصطلح الفضاء السيبراني نكاية عن التطور الحاصل في قواعد البيانات والشبكات التي أصبحت تربط الهيئات وحتى الدول ببعضها البعض الكترونيا.

فالفضاء السيبراني هو: " مصطلح حديث، ظهر نتيجة لثورة تكنولوجيا المعلومات، ويشمل جميع الحواسيب والمعلومات التي بداخلها والأنظمة والبرامج والشبكات المفتوحة لاستعمال الجمهور العام أو تلك الشبكات التي صممت لاستعمال فئة محددة من المستعملين ومنفصلة عن شبكة الإنترنت العامة، فالفضاء السيبراني هو العالم المادي والمفاهيمي الذي توجد فيه جميع هذه الأنظمة " (فرحات، 2019، صفحة 90).

فصعوبة اكتشاف الخروقات الأمنية والمتسبب فيها قد عزز التوجه نحو عولمة مفهوم الأمن السيبراني بما يسمح باحتواء مختلف الهجمات ضمن فضاء شبه موحد، وهو ما من شأنه ردع التجاوزات عبر مختلف التقنيات العالية والمتطورة وكذا دعم مختلف الأجهزة الأمنية والقضائية في مهامها.

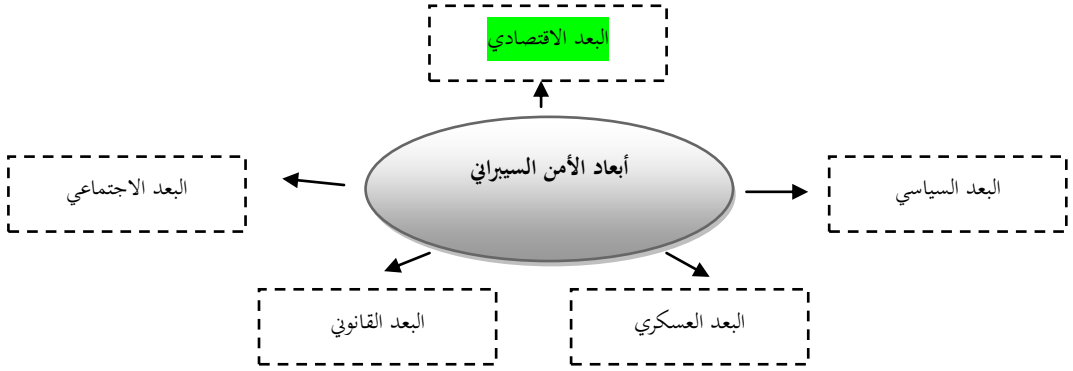
ب. الأهداف والمهام الأساسية للأمن السيبراني:

1. ضمان حماية وسرية قواعد البيانات الشخصية؛
2. حماية المواطنين والمستهلكين من المخاطر المحتملة في مجالات استخدام الإنترنت؛
3. تأسيس صناعة ريادية وطنية للأمن السيبراني؛ (وريدة، 2021، صفحة 813)
4. حماية وتحصين أنظمة التشغيل والولوج للشبكات الداخلية والخارجية؛

ج. أبعاد الأمن السيبراني:

يرتبط الأمن السيبراني بعدة مجالات حيوية سواء داخل الدولة أو خارجها، مما يزيد من أهمية العناية بصناعة أمنية سيبرانية تسمح بمرافقة التطور الحاصل في مختلف قطاعات الاقتصاد، المالية، الدفاع، القانون، والمجتمع.

الشكل (01) : أبعاد الأمن السيبراني



المصدر: (عسيري، الصفحات 7-8)

فيما يخص البعد الاقتصادي وبفضل أنظمة حماية الشبكات الإلكترونية والعنكبوتية، أصبحت الأسواق المالية جد متصلة ببعضها عن ذي قبل، أيضا استطاعت البنوك ومختلف المؤسسات المالية قادرة على تبادل رؤوس الأموال وإلكترونيا في ظرف وجيز. بالإضافة إلى تطور مختلف الصناعات القائمة على التعاملات الرقمية. أما سياسيا، فالأمن السيبراني قد ساهم في حماية الوثائق الهامة والحساسة للدولة من أي تجسس أو تسريب. اجتماعيا، " يحافظ الأمن السيبراني على أخلاقيات المجتمع من مختلف التهديدات كالمواد الإباحية، الإرهاب ونشر الفكر المتطرف، والإتجار بالمخدرات " (عسيري، صفحة 7).

على الصعيد العسكري، تسمح الحماية السيبرانية بربط الوحدات العسكرية ببعضها البعض عبر الشبكات العسكرية في الفضاء الالكتروني. في المقابل، تعتبر هناك رابطة تبادلية بين البعد القانوني والأمن السيبراني، فالقانون يحمي التعاملات الإلكترونية، والأمن السيبراني يساهم في حماية البيانات المعالجة وضمان سريتها، بالإضافة إلى ضمان استمرارية المعالجة القانونية للقضايا المختلفة (عسيري، صفحة 8).

2.2.1 آليات الهجمات السيبرانية:

تعتمد الهجمات السيبرانية على عدة آليات ومفاهيم لابد من توضيحها، وهو ما من شأنه المساعدة في إعداد الإستراتيجيات الملائمة لمواجهتها.

أ. مفهوم الهجمات السيبرانية:

تنوعت مفاهيم الهجمات في الفضاء السيبراني، إلا أنها تتفق كلها على ضرورة ردعها والتصدي لها عبر عصرنة الأنظمة الأمنية وكذا نشر الوعي حول طبيعة هذه الهجمات. " فهجمات الفضاء السيبراني أحد أنواع النزاع أو الصراع المسلح الأكثر ديناميكية، فهي تختلف عن أشكال النزاعات التقليدية، ويمكنها الحدوث بشكل غير مرئي وغير مشهود، مثل أن تقوم المخابرات الخاصة لأي دولة بشن هجمات باستخدام الأسلحة السيبرانية من أجل تخريب البنية التحتية المعلوماتية الخاصة بدولة أخرى " (حكيم، 2018، صفحة 108).

ب. أسباب انتشار الهجمات السيبرانية:

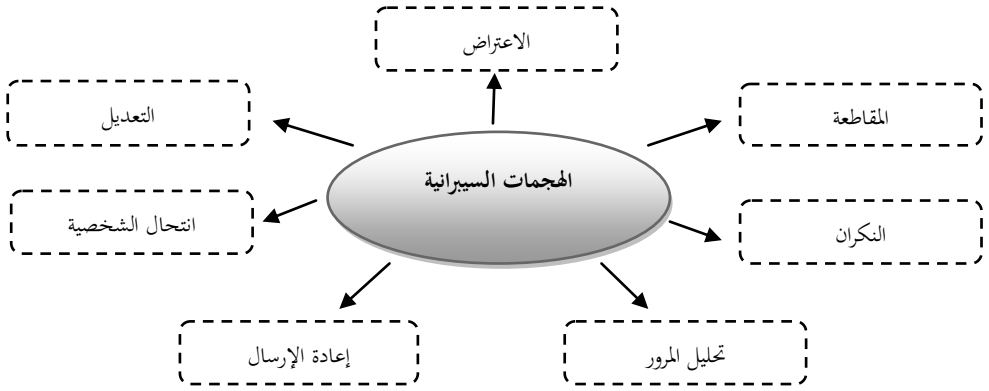
ترتبط الهجمات السيبرانية عموما بمدى قدرة الأنظمة الأمنية على حماية البيانات ومختلف التكنولوجيات المستخدمة في ذات الإطار، وعليه نجد: (فرحات، 2019، الصفحات 96-97)

- عدم صلابة بنية الشبكات المعلوماتية مما يسهل عملية اختراقها؛
- مرافقة العمليات العسكرية الميدانية؛
- الاعتماد المتزايد للدول على الفضاء السيبراني؛
- سهولة الوصول إلى المعدات المساعدة على الهجمات السيبرانية؛
- بقاء هوية المهاجم مجهولة يساعد على توسع نطاق الهجمات.

ت. أبرز الهجمات السيبرانية:

قد تتسبب هجمات سيبرانية مثل المقاطعة في وضع النظام خارج الاستخدام. أما الاعتراض فيمكن المهاجمين من الوصول إلى بيانات الغير بطريقة غير قانونية. في حين أن التعديل يؤدي إلى التلاعب بالبيانات الشخصية، بالإضافة لانتحال الشخصية. كذلك نجد نمط النكران، أين يتم الإدعاء بعدم القيام بإرسال أي شيء. في المقابل، نجد تقنية تحليل المرور والتي تسمح بمراقبة الاتصال الشبكي بهدف الحصول على معلومات. أخيرا، نجد هجمات على شكل إعادة الإرسال والذي يسمح للمهاجم بإعادة توجيه المعلومات نحو مسار يخدم مصالحه (الشيخ، 2015، الصفحات 4-5).

الشكل (02): الهجمات السيبرانية الأكثر شيوعا



المصدر: (الشيخ، 2015، صفحة 4)

2. الجزء التطبيقي للدراسة:

يتم التطرق للآثار المترتبة عن الهجمات السيبرانية جراء الانتقال إلى الرقمنة، بما في ذلك الآثار الاقتصادية والمالية، والتي تتكبدها الشركات، المؤسسات المالية وحتى الدول، مع التطرق لأهم التجارب الدولية لمواجهة تلك الهجمات، وآليات التصدي والردع السيبراني التي يمكن الاستفادة منها في بناء تحالف دولي ضد الخسائر الاقتصادية والمالية لناجمة عن الهجمات السيبرانية، مع الإشارة لحالة الجزائر، ومدى امتلاكها لمنظومة ردع سيبراني تسمح لها بالتوجه نحو الرقمنة بأقل الأضرار والخسائر.

1.2. الآثار الاقتصادية والمالية للهجمات السيبرانية:

تتسبب الهجمات السيبرانية بخسائر مالية كبيرة تصل لملايير الدولارات سنويا. فخلال الفترة 2014- 2018، تعرضت عدة شركات اقتصادية لهجمات سيبرانية استهدفت بياناتها عبر أسلوب الاختراق، فقد تعرضت شركة Ebay الأمريكية مثلا لسرقة 140 مليون حساب مصرفي سنة 2014. في حين تعرضت شركة الطيران البريطانية سنة 2018 إلى هجوم سيبراني كبير أدى إلى تدهور قيمة أسهم الشركة المسيرة في البورصة.

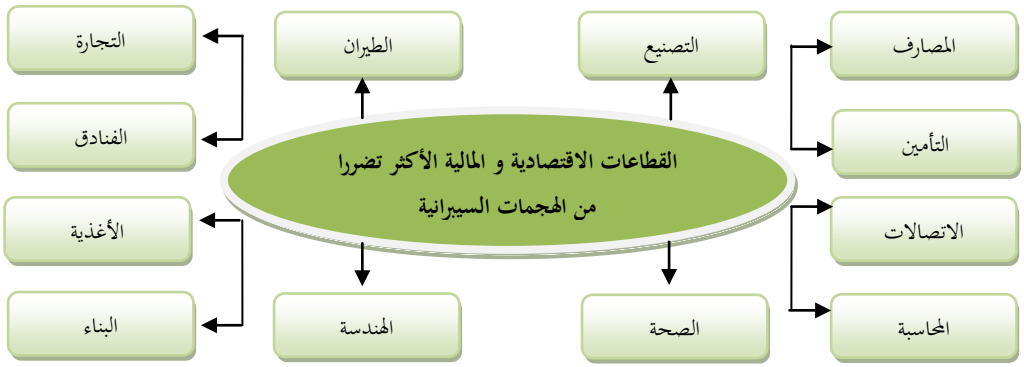
الجدول (02): الهجمات السيبرانية على الشركات خلال الفترة 2014– 2018

الرقم	الشركة	تاريخ الهجوم	آثار الهجمات السيبرانية
01	eBay الأمريكية	ماي 2014	سرقة بيانات 140 مليون حساب مصرفي
02	Sony Pictures	نوفمبر 2014	سرقة البيانات بما في ذلك الأفلام الجديدة وجعلها متاحة للجمهور على الانترنت
03	Orange	2015	تمت سرقة ملايين البيانات الشخصية وبلغت تكلفة هذه الحوادث أكثر من 24 مليون يورو
04	TV5 موند	أفريل 2015	أصبحت الأنظمة غير قادرة على العمل لفترة أطول وتم قطع البث
05	Airaner Ryanair	2016	سرقة 5 مليون دولار أمريكي بعد نقل إلكتروني مزور عبر بنك صيني
06	Airline البريطانية	عام 2018	وصلت عملية الاختراق إلى 380 ألف عملية شراء تذاكر، وانخفضت قيمة الأسهم بنحو 3 % في سوق لندن

المصدر: (للتأمين، 2021)

في المقابل، تعتبر سنة 2018 سنة الاختراقات الأمنية بامتياز، نظرا لحدة وكثافة الهجمات السيبرانية المنفذة، بالإضافة إلى حجم الخسائر الاقتصادية والمالية التي تسبب بها.

الشكل (03): القطاعات الاقتصادية والمالية الأكثر تضررا من الهجمات السيبرانية



المصدر: (للتأمين، 2021، صفحة 4)

تعتبر القطاعات الاقتصادية والمالية الأكثر عرضة للهجمات السيبرانية. وكما هو موضح في الشكل أعلاه، نجد أن المصارف من بين المؤسسات المالية المستهدفة، إضافة إلى قطاع التأمين والمحاسبة. دون أن ننسى قطاعات اقتصادية وتجارية مثل: التصنيع، الطيران، الفندقة. وبناء عليه، وجب التصدي لهذه الهجمات حتى لا تتسبب بالمزيد من الخسائر لأحد أهم قطاعات الحياة ألا وهو الاقتصاد.

2.2. الخسائر المالية والحلول العملية للهجمات السيبرانية:

أشار صندوق النقد الدولي من خلال عدة دراسات قام بها أن المخاطر السيبرانية تعتبر أحد أهم المخاطر التي تواجه الاستقرار المالي العالمي سنة 2018. حيث، " يعتبر القطاع المالي من أكبر القطاعات المستهدفة بالهجمات الإلكترونية الخبيثة نسبة لدوره في الوساطة المالية واعتماده على نظم المعلومات في أداء مهامه " (بقا، 2019، صفحة 29)

1.2.2. التكلفة الاقتصادية والمالية للهجمات السيبرانية:

نظرا لتطور المعاملات المالية الرقمية، أصبحت الهجمات السيبرانية أكثر حدة وتأثيرا، حيث تضاعفت بمعدل 3 مرات خلال العقد الماضي، وأصبحت تتسبب في حدوث اضطرابات كبيرة في الأنظمة المالية والمصرفية عبر فقدان الثقة لدى العملاء مما يؤدي إلى المطالبة بسحب ودائعهم، إضافة إلى مشكل السيولة. (جنكيتسون، 2020)

الجدول (03): سرقة البنوك المركزية والخاصة سنتي 2015 و 2016

الرقم	السنة	الهيئة	الهجمات والآثار
01	2016	بنك بنغلاديش	سرقة 81 مليون دولار من حسابه في بنك نيويورك
02	2015	بنك Del Austro الإكوادوري	سرقة 12 مليون دولار
03	2015	بنك الشرق الأقصى الدولي التايواني	سرقة أكثر من 60 مليون دولار

المصدر: (بقا، 2019، صفحة 20)

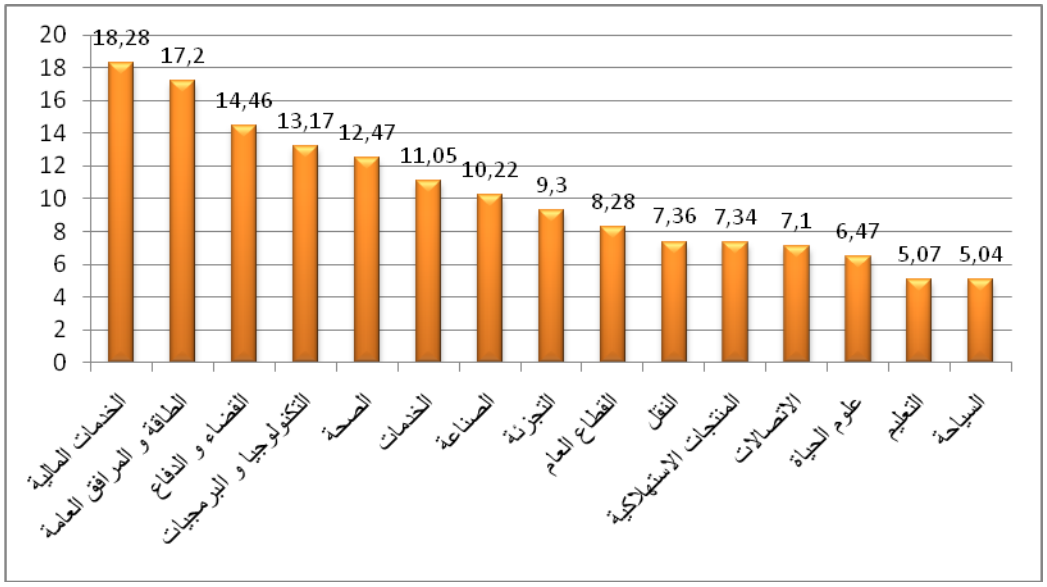
وفي الجدول أعلاه، يظهر جليا حجم الخسائر المالية جراء سرقة المصارف حيث تعدت 80 مليون دولار خلال الهجمة السيبرانية الواحدة. وعليه، يمكن اعتبار المؤسسات المالية والمصرفية بمختلف أنواعها الوجهة الأولى للهجمات السيبرانية، وهو ما يحتم عليها إدراج ذلك في سياساتها في مجال إدارة المخاطر، وذلك عبر القيام بصيانة سيبرانية لكل شبكاتها الرقمية وبرمجياتها الإلكترونية، وهو ما من شأنه استقطاب المزيد من المستثمرين والمودعين.

الشكل (04): التكلفة المالية للهجمات السيبرانية ضد قطاعي المالية والتجارة في إفريقيا، سنة 2017

المصدر: (الإفريقي، 2019، صفحة 54)

ففي إفريقيا مثلا، تشكل التكلفة المالية للخسائر المالية و الاقتصادية لقطاع المصارف و المؤسسات المالية ما يقارب 23 % من إجمالي الأصول المتداولة، و هو مؤشر مرتفع جدا و يهدد استمرارية و تنافسية القطاع، بالإضافة لتدهور قطاع التجارة الإلكترونية الذي عرف خسائر مالية قدرت بحوالي 16 % سنة 2017. في الأخير، تبقى السياسة الوقائية هي الحل الأنجع لتخفيف بثار الهجمات السيبرانية عبر الاستثمار في مجالات الحماية الرقمية و تعزيز أنظمة التشفير و حماية البيانات و الأرصدة لمختلف المتعاملين الاقتصاديين سواء المحليين أو المستثمرين الأجانب.

الشكل (05): متوسط التكلفة السنوية للجريمة السيبرانية حسب القطاع الاقتصادي لعينة من الشركات العالمية بملايين الدولارات، 2017



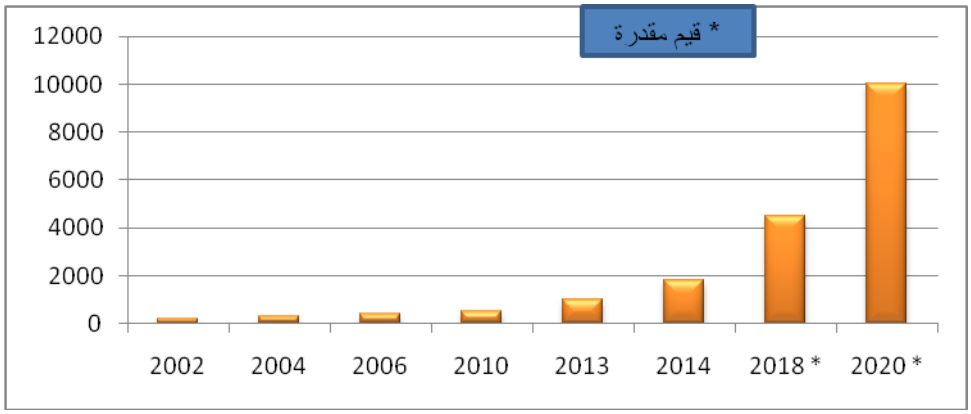
المصدر: (بقا، 2019، صفحة 31)

وكما يشير إليه الشكل أعلاه، فإن القطاعات الاقتصادية والمالية لم تسلم من الخسائر الناجمة عن الهجمات السيبرانية، حيث أصبحت أدوات القرصنة الآن أقل تكلفة، أكثر سهولة وأشد قوة (جنكيتسون، 2020)، وهو ما يجعل هذه الأدوات متاحة للمهاجمين بمختلف تصنيفاتهم، كما يمكنهم من إلحاق أضرار مباشرة ومعتبرة بمختلف الكيانات. وعليه، فقد أصبح التحالف الدولي لمواجهة الهجمات السيبرانية أمرا حتميا.

2.2.2. سوق التأمين السيبراني كآلية للتخفيف من آثار الهجمات السيبرانية على القطاع الاقتصادي و المالي:

يعتبر قطاع التأمين من أهم الوسائل التي تساهم في الحد والتصدي للهجمات السيبرانية. فقد بلغ حجم سوق التأمين السيبراني 4.52 مليار دولار سنة 2017، ومن المتوقع أن يصل إلى 17.55 مليار دولار سنة 2023، مسجلا معدل نموي سنوي 25.4 % (للتأمين، 2021، صفحة 02).

الشكل (06): التأمين السيبراني: إجمالي الأقساط المكتتبة العالمية (مليون دولار)



المصدر: (للتأمين، 2021، صفحة 3)

يتميز أيضا سوق التأمين السيبراني بارتفاع أقساطه (أنظر الشكل أعلاه) بسبب وجود عدد محدد من الشركات التي تقدم هذا النوع من الخدمات. بالإضافة لفرض شروط واستثناءات صعبة على المؤسسات و الهيئات الراغبة في التأمين السيبراني.

ومن مميزات خدمة التأمين السيبراني أنها تمكن الهيئات المؤمنة من تحديد الثغرات الأمنية السيبرانية والتعامل معها. خاصة إذا علمنا أن حوالي 37 % من الشركات التي تم إجراء مسح عليها بالتقرير تعرضت لهجمات سيبرانية تسببت بحدوث خروقات للبيانات، بالإضافة لمتوسط الأثر الاقتصادي للحدث الذي وصل إلى 2.1 مليون دولار. (**للتأمين، 2021، صفحة 03**)

3.2. أفضل الممارسات والتجارب الدولية للحد من الآثار الاقتصادية و المالية للهجمات السيبرانية:

أصبح الاقتصاد العالمي يتكبد ما يفوق 230 مليار دولار سنويا جراء الهجمات السيبرانية، وبمعدل 1000 هجوم كل دقيقة (الجواد، 2020، صفحة 374)، فالهجمات السيبرانية تحاكي إلى حد كبير الهجمات التقليدية من ناحية النتائج، والتي قد تكون كارثية وذات آثار مدمرة. في حين تختلف آليات التنفيذ والاستراتيجيات المتبعة في تنفيذ الهجوم السيبراني من قبل الأطراف الفاعلة، سواء كانت جماعات إرهابية أو حكومات معادية أو مجرد قراصنة. (الجواد، 2020، صفحة 476)

1.3.2. التجربة الافريقية:

تم تأسيس" اتفاقية الأمن الإلكتروني وحماية البيانات الشخصية " لدول وحكومات الاتحاد الإفريقي، حيث تسعى هذه الاتفاقية المعروفة أيضا باسم اتفاقية مالابو إلى اتباع نهج مشترك على المستوى القاري بشأن الأمن السيبراني وكذا وضع الحد الأدنى من المعايير والإجراءات لتحديد بيئة رقمية موثوقة لتطوير الاتصالات الإلكترونية وضمان احترام الخصوصية على الأنترنت (الإفريقي، 2019، صفحة 53).

2.3.2. التجربة الصينية:

في نوفمبر 2016، تبنى البرلمان الصيني القانون الجديد الخاص بالأمن السيبراني الوطني، وهو يتكون من 7 فصول، والذي أصبح نافذا بنهاية 2017. كما يعتبر هذا القانون متوازنا إلى حد كبير، أين قام بتحديد مهام القطاعات الحكومية اتجاه تأمين الشبكات والبيانات، بالإضافة إلى ضبط ومراقبة نشاطات مزودي الإنترنت. كما قام أيضا بإلزام مختلف الشركات والمؤسسات المالية والمصرفية بوضع وتجديد برامج حماية ضد الهجمات السيبرانية (هاثاواي، 2017، صفحة 4). كما تطلق الصين على هذه الإستراتيجية اسم " الجدار الناري العظيم "، وهي بذلك تفرض رقابة سيبرانية صارمة على كل تعاملات الانترنت وتحد من قدرة المواقع العالمية في الولوج إلى كياناتها الاقتصادية، الحكومية والاجتماعية عبر سياسة الحجب (الوطن، 2021، الصفحات 3-4)

3.3.2. التجربة الأمريكية:

في سنة 2014، قامت السلطات الأمريكية بالإعلان عن " برنامج العمل لتحسين الأمن السيبراني للبنى التحتية الحساسة "، والذي يعتمد على الجانب التطوعي للمؤسسات والكيانات الكبرى من أجل الانخراط والاستثمار في هذا البرنامج وحماية ممتلكاتها من أي اختراق أو هجوم سيبراني، وحسب الإحصائيات، فإن حوالي 30 % من الهيئات الأمريكية سواء الحكومية أو الخاصة قد انخرطت فعلا في هذا الإطار (هاثاواي، 2017، صفحة 4). كما تركز الو.م.أ أيضا على تحديد الشركات الكبرى التي تساهم بأكثر من 2 % من إجمالي الناتج المحلي حتى تعزز نظام إدارة المخاطر لديها (هاثاواي، 2017، صفحة 3).

في ماي 2021، تم استصدار أمر رئاسي تنفيذي بغرض تحديد آليات الحماية السيبرانية بما يتناسب مع حدة الهجمات المسجلة. كما يهدف القانون إلى تحديث الخدمات السحابية للوكالات الفيدرالية، وتطوير برامج تدريب متخصصة بمراجعة تقنيات السلامة السيبرانية والكشف المبكر عن الثغرات الأمنية (الوطن، 2021، الصفحات 3-4)

4.3.2. التجربة الأوربية:

في جانفي 2020، قامت السلطات الأمنية في ألمانيا بتحديث أنظمة حماية الشبكات وصيانتها، وقامت أيضا بتدشين مركز آخر للدفاع السيبراني. في حين تمكنت بريطانيا من التصدي ل 850 هجوم سيبراني سنة 2020، وهذا بفضل أسطول دفاع سيبراني بقيادة وزارة الدفاع ومكتب الاتصالات الإلكتروني. في المقابل، تعمل المفوضية الأوربية على تحديث قواعدها للأمن السيبراني عبر العناية بالقطاعات الحساسة كالصحة والدفاع، كل هذا ضمن ما يعرف ببرنامج " توجيه الشبكات وأمن المعلومات " (الوطن، 2021، الصفحات 3-4)

4.2. قراءة في التجربة الجزائرية لتعزيز الأمن السيبراني:

يتميز الاقتصاد الجزائري باعتماده على إيرادات المحروقات بنسبة تتجاوز 95 %. ورغم هذا لا يزال النظام المالي يعتمد على اقتصاديات المديونية والتبعية للمصارف في تمويل مختلف المشاريع (مليكة، 2021، صفحة 193). إن تطوير و عصرنة القطاع المصرفي ومروره عبر الرقمنة لابد أن يتزامن مع إستراتيجية وطنية للأمن السيبراني لضمان حماية الودائع وقرصنة البيانات.

1.4.2. التحول الرقمي في الجزائر:

أ. الخدمات المالية:

انتقل القطاع المصرفي في الجزائر في عملية التحول الرقمي عبر ما يعرف بالصيرفة الإلكترونية، وعلى شكل البطاقات الممغنطة ما بين البنوك، بالإضافة إلى مرافقة عمليات التجارة الإلكترونية لمختلف المتعاملين الاقتصاديين.

ب. النشاط التجاري:

عرفت الجزائر لأول مرة عملية رقمنة النشاط التجاري عبر تقنية السجل الإلكتروني، وهو ما يسمح بمرافقة مختلف الأنشطة التجارية وتخفيف التعاملات الإدارية. أيضا، فقد تم تدعيم مؤسسة بريد الجزائر، في أواخر سنة 2016 بنظام البطاقة الإلكترونية الذهبية، وهذا بغرض تنشيط عمليات الدفع والسحب الإلكترونيين، سواء تعلق الأمور بالدفع للغير أو تسديد الفواتير.

الجدول (04) : المؤشرات الاقتصادية والعالمية لتطور قطاع تكنولوجيا المعلومات والاتصالات في الجزائر (القيم بمليار دج)

نوع المؤشر	المؤشر	2010	2018
	رقم أعمال القطاع	459 (سنة 2013)	458
مؤشر اقتصادي	عدد المؤسسات الاقتصادية بالقطاع	200903	266301
	قيمة الصادرات	0,076	1,129
	قيمة الواردات	86,661	242,424
مؤشر عالمي	تطور القطاع- IDI	2,86	4,76
	تطور الإدارة الإلكترونية- IDEG	0,374	0,422

المصدر: (بشاري، 2020، صفحة 588)

عرفت مؤشرات وقيم قطاع الاتصالات تطورا ملحوظا من سنة 2010 إلى سنة 2018 وهذا بفضل حرص السلطات على دعم القطاع ورفع الاستثمار العمومي عبر زيادة حصة الأغلفة المالية الموجهة لذات القطاع. رغم هذا، لا تزال الجزائر بعيدة في التصنيف العالمي وفق مؤشري IDI، IDEG لسنة 2017، أين حققت المراتب 102 و 130على الترتيب.

2.4.2. الجانب القانوني للأمن السيبراني في الجزائر:

يتم معالجة القضايا المتعلقة بالأمن السيبراني عبر عدة قوانين من بينها: القانون 04-15 المتضمن تعديل قانون العقوبات، أين خصص قسمه السابع مكرر لأنظمة المعالجة الآلية للمعطيات (سمير، 2017، صفحة 264). أيضا، تم إصدار القانون 09- 04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، سنة 2009 (سمير، 2017، صفحة 265)، أين تم تعريف الجريمة الالكترونية وإدراجها ضمن الأعمال المعاقب عليها قانونا (المادة 02). في المقابل، تم إصدار القانون 03-16 المؤرخ في 2016/06/19 المتضمن البصمات الجنائية في الإجراءات الجزائية لتحديد هوية الأشخاص، وهو ما يشكل إضافة نوعية في إطار مواجهة الهجمات السيبرانية. فالجزائر تسعى من خلال تشريعاتها إلى مطابقة ومحاكاة ما جاءت به التشريعات الدولية والاتفاقيات المبرمة في المجر سنة 2001 المتضمنة معالجة الجرائم السيبرانية (بوازدية، 2019، صفحة 127)

3.4.2. الجانب العملياتي للأمن السيبراني في الجزائر:

استطاعت الجزائر تشكيل قطاع عملياتي وتقني للأمن السيبراني يضم عدة هيئات ووكالات متخصصة موزعة بين الأمن الوطني والدرك الوطني. وهي تتوفر على معدات جد متطورة لحماية الأشخاص والممتلكات وحماية الاقتصاد الوطني أيضا: (سمير، 2017، الصفحات 270-274)

1. مركز الوقاية من جرائم الإعلام الآلي والجرائم المعلوماتية للدرك الوطني؛
2. المعهد الوطني للأدلة الجنائية وعلم الإجرام للدرك الوطني؛
3. المصلحة المركزية لمكافحة الجريمة المعلوماتية التابعة لمديرية الأمن الوطني؛
4. الهيئة الوطنية للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها.

هذا وقد تعرضت الجزائر كغيرها من الدول والاقتصادات إلى عدة هجمات سيبرانية استهدفت مواقع حكومية بالدرجة الأولى، بالإضافة لاستهداف مؤسسات اقتصادية. لكن تبقى هوية وطبيعة المهاجمين غير معلن عنها لحد الآن، كما لم يتم الإعلان عن المؤسسات المتضررة وحجم الخسائر المتكبدة، إلا أن السلطات تعتبر أن: " مهمة حماية وتأمين والدفاع عن فضائنا السيبراني هي مسؤولية جماعية تضمن من خلال استراتيجية وطنية شاملة للأمن السيبراني يتعين أن ينخرط فيها الجميع " (آمال، 2021، صفحة 20)

5.2. الدروس المستفادة، الحلول والاستراتيجيات المقترحة لمواجهة الهجمات السيبرانية:

أ. **الحلول التقنية:** تعتمد أساسا على اعتماد كلمة سر صعبة الاختراق وتغييرها بصفة دورية، كما يتعين استخدام تقنية التوقيع الرقمي لدى المصارف وشركات البطاقات الائتمانية (عواشرية، 2020، صفحة 136- 137)

ب. **التدخل التشريعي:** ينبغي اصدار قوانين مرنة لحماية البنية الرقمية لمختلف الهيكل الاقتصادية والمالية، بالإضافة لضرورة تناسقها مع القوانين الدولية للأمن السيبراني.

ت. **الشراكة بين القطاع العام والخاص:** ضرورة التنسيق اللوجستي والتقني بين مختلف الهيئات العمومية والخاصة فيما يخص تبادل المعلومات حول التهديدات والهجمات السيرانية المحتملة.

ث. **التعاون الدولي:** ضرورة التعاون بين الكيانات الاقتصادية والمالية من جهة وبين الحكومات من جهة أخرى، لضمان استرجاع الحسابات المقرصنة، وإنشاء قاعدة بيانات لحماية الاستثمارات والبنى التحتية.

ج. **محو أمية التقنية المالية ونشر الوعي الرقمي:**إعداد برامج لمحو الأمية المالية بما يحقق الفائدة والمنفعة للأفراد تحت مظلة الشمول المالي. كما يجب توفير الدعم الفني لمستخدمي التطبيقات الرقمية خاصة المبتدئين، وهذا من أجل كسب ثقة المواطن وضمان ولائه (العربية، 2020، صفحة 73).

ح. **تخصيص هياكل للردع السيبراني:** وهو ما نصت عليه المادة 14 من اتفاقية بودابست للإجرام المعلوماتي، حيث يسمح ذلك بالمواجهة السريعة والدقيقة لأي هجوم سيبراني.

7. **إعداد الخرائط السيبرانية:** وذلك عن طريق إعداد خرائط لأهم الروابط التشغيلية والتكنولوجية المتبادلة والبنية التحتية ذات الأهمية الحرجة.

8. **تطوير استراتيجيات الاستجابة:** يجب أن يكون النظام المالي قادرا على استئناف عملياته بسرعة حتى في مواجهة هجمة سيبرانية ناجحة، لا سيما في البلدان منخفضة الدخل (جنكيتسون، 2020، صفحة 02).

9. **استراتيجية الردع السيبراني:** يتوجب خفض تكلفة الهجمات لسيبرانية والحد من خطرها عبر إجراءات ردعية فعالة لمصادرة عائدات الجريمة ومقاضاة المجرمين بالاستعانة بالجهود الدولية (جنكيتسون، 2020، صفحة 02).

10. **تطوير القدرات الوقائية:** ينبغي مساعدة الاقتصادات النامية والبلدان منخفضة الدخل على تعزيز الاستقرار المالي ودعم الشمول المالي، وذلك عبر ضمان الاستفادة من التكنولوجيا بشكل يحفظ الأمن والسلامة اللتان تعتبران قضية محورية في التنمية (جنكيتسون، 2020، صفحة 03).

3. النتائج والتوصيات:

1.3. النتائج: توصلت الدراسة إلى مجموعة من النتائج المهمة، أبرزها:

- ✓ أصبح التحول الرقمي بكل أبعاده ضرورة ملحة خاصة في الجانب الاقتصادي و الخدمات المالية؛
- ✓ تحتاج عملية التحول الرقمي إلى عدة تقنيات أبرزها الأمن و الحماية السيبرانية؛
- ✓ يعتبر الأمن السيبراني ذا بعد اقتصادي ومالي يستحق الدراسة والبحث؛
- ✓ استطاعت الهجمات السيبرانية مؤخرا تكبيد خسائر كبير للشركات والدول؛
- ✓ أصبح الأمن السيبراني يدخل ضمن استراتيجة إدارة المخاطر لدى المؤسسات المالية؛

- ✓ يتم التصدي للهجمات السيبرانية عبر أنظمة دفاع رقمية وكذا التأمين ضده؛
- ✓ تعتبر تجربة الجزائر فتية في مواجهة الهجمات السيبرانية نظرا لعدم تطور اقتصادها الرقمي.

2.3. التوصيات: وبناء عليه، فقد تمكنا من اقتراح بعض التوصيات الهامة:

- ✓ إنشاء قطب التميز الوطني في الأمن السيبراني في إطار إستراتيجية وطنية شاملة بالموازاة مع سياسة التحول الرقمي؛
- ✓ التعاون الدولي والإقليمي في مجال الأمن السيبراني؛
- ✓ تطوير المعدات والتقنيات المستخدمة في الحماية السيبرانية؛
- ✓ اعتماد تقنية التوقيع الرقمي لحماية أموال المصارف والمؤسسات؛
- ✓ زيادة عدد التشريعات والقوانين المتعلقة بالأمن السيبراني بما يضمن عدم وجود ثغرات أمنية؛
- ✓ نشر الوعي لدى مختلف الفاعلين بالمعاملات الرقمية وكيفية تأمين البيانات؛
- ✓ تدريب وتطوير قدرات الفاعلين في مجال الأمن السيبراني حماية للاقتصاد والمصارف.

المصادر والمراجع:

1. الاتحاد المصري للتأمين. (2021). الهجمات الإلكترونية (السيبرانية) والتأمين. تاريخ الاسترداد 19 أوت, 2021، من نشرة الاتحاد المصري للتأمين: PageDetailID=1324&Https://www.ifegypt.org/NewsDetails.aspx?Page_ID=1244

2. أميرة عبد العظيم مُحَمَّد عبد الجواد. (2020). المخاطر السيبرانية وسبل مواجهتها في القانون الدولي العام. مجلة الشريعة والقانون ، صفحة 374.

3. بارة سمير. (2017). الأمن السيبراني في الجزائر: السياسات والمؤسسات. المجلة الجزائرية للأمن الإنساني ، صفحة 264.

4. جمال بوازدية. (2019). الإستراتيجية الجزائرية في مواجهة الجرائم السيبرانية: التحديات والآفاق المستقبلية. مجلة العلوم القانونية والسياسية ، صفحة 127.

5. جنيفر إليوت، نايجل جنكيتسون. (2020). المخاطر السيبرانية: التهديد الجديد للاستقرار المالي. تاريخ الاسترداد 2 أوت , 2021، من صندوق النقد الدولي: https://www.imf.org/ar/News/Articles/2020/12/07/blog-cyber-risk-is-the-new-threat-to-financial-stability

6. حميدة لحمر، فريدة حموم. (جوان, 2021). التعاون الأمني في جنوب شرق آسيا في مواجهة تهديدات الأمن السيبراني. مجلة طبنة للدراسات العلمية الأكاديمية ، صفحة ص: 534.

7. خالد ياسين الشيخ. (2015). أمن نظم المعلومات والرقابة. سوريا: جامعة دمشق.

8. خيلية وريدة. (ديسمبر, 2021). إشكالية المواطنة في ظل قيم التكنولوجيا الحديثة وبين حرية المواطن والأمن السيبراني. حوليات جامعة الجزائر 1 ، صفحة 810.

9. عقون شراف، غضبا مليكة. (سبتمبر, 2021). واقع مناخ الاستثمار الأجنبي المباشر في الجزائر– دراسة تحليلية وقياسية للفترة 1999– 2019. مجلة اقتصاد المال والأعمال ، صفحة 193.

10. علاء الدين فرحات. (سبتمبر, 2019). الفضاء السيبراني: تشكيل ساحة المعركة في القرن الحادي والعشرين. مجلة العلوم القانونية والسياسية ، صفحة 90.

11. علم الدين بقا. (أفريل, 2019). مخاطر الهجمات الإلكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي. مجلة دراسات تنموية، المعهد العربي للتخطيط ، صفحة 29.

12. غريب حكيم. (ديسمبر, 2018). الإرهاب السيبراني والأمن الدولي: التهديدات العالمية الجديدة وأساليب المواجهة. المجلة الجزائرية للدراسات السياسية ، صفحة 107.

13. فضيل الشريف آمال. (2021). الأمن السيبراني والدفاع السيبراني: رهانات وتحديات. مجلة الجيش ، صفحة 20.

14. فيصل مُحَّد عسيري. الأمن السيبراني وحماية أمن المعلومات، . رسالة علمية غير منشورة.

15. مجلة درع الوطن. (2021). الهجمات السيبرانية: تهديد متعاظم للأمن واللاستقرار والاقتصاد العالمي. تاريخ الاسترداد 19 08, 2021، من www.nationshield.ae/index.php/home/details/research/

16. ميليسا هاثاواي. (2017). إدارة الخطر السيبراني الوطني، فهم الخطر السيبراني، رسالة علمية غير منشورة. ص: 04. تاريخ الاسترداد 21 سبتمبر, 2021، من potomacinstitute: https://potomacinstitute.org/images/CRI/Managing-National-Cyber-Risks_FINAL-Arabic.pdf