مجلة البحوث القانونية والاقتصادية
JOURNAL OF LEGAL AND ECONOMIC RESEARCH
المجلد: 9 العدد:2 الشهر:6 السنة: 2026
ص.ص 617 - 636

الأمن السيبراني في المملكة العربية السعودية :الواقع، التحديات ورؤية 2030

Cybersecurity in the Kingdom of Saudi Arabia: Current Status Challenges, and Vision 2030

ريمة يونس[1]
جامعة الجزائر3- الجزائر
rymi18@hotmail.fr
مخبر إستراتيجيات التحول الاقتصادي.

أمال فياش
جامعة الجزائر3- الجزائر
fiacheamel@gmail.com

تاريخ الاستلام: 2026-04-22	تاريخ القبول للنشر: 2026-05-02

ملخص

تهدف الدراسة إلى إبراز واقع الأمن السيبراني في المملكة العربية السعودية، من خلال تسليط الضوء على المفاهيم والنظريات المرتبطة به، بما يساهم في تحليل الوضع الراهن واستشراف الآفاق المستقبلية، تبدأ الدراسة بعرض أهم التعاريف والمفاهيم الأساسية للأمن السيبراني وآليات إدارته، ثم تنتقل إلى تحليل واقع الأمن السيبراني في المملكة، من خلال تتبع تطور ترتيبها في مؤشر الأمن السيبراني العالمي الصادر عن المعهد الدولي للتنمية الإدارية خلال الفترة 2020-2024 .كما تتناول الدراسة أبرز التحديات والمخاطر السيبرانية التي تواجه الدولة، إلى جانب استعراض المبادرات الوطنية والبرامج التنموية التي أطلقتها الجهات الرسمية بهدف تعزيز القدرات السيبرانية، وكذلك معالجة مدى ارتباط الأمن السيبراني برؤية المملكة 2030، ودوره في تحقيق أهدافها الإستراتيجية.

توصلت الدراسة إلى أن المملكة قد حققت إنجازات ملموسة في بناء منظومة متكاملة للأمن السيبراني، الأمر الذي مكنها من احتلال مراكز متقدمة على الصعيد العالمي ومع ذلك، فإن تسارع التطورات التكنولوجية يفرض ضرورة الاستمرار في تطوير السياسات وتعزيز القدرات لمواجهة التحديات السيبرانية المتجددة.

الكلمات المفتاحية: الأمن السيبراني، تحديات الأمن السيبراني، مؤشر الأمن السيبراني العالمي، رؤية السعودية 2030.

تصنيف JEL: H56 ;H11 ;O33 ;L86

[1] ريمة يونس

Abstract

This study aims to highlight the current state of cybersecurity in the Kingdom of Saudi Arabia by focusing on the concepts and theories associated with it, contributing to the analysis of the present situation and the projection of future prospects. The study begins by presenting the most important definitions and basic concepts of cybersecurity and its management mechanisms, then moves on to analyze the cybersecurity landscape in the Kingdom by tracking its ranking in the Global Cybersecurity Index issued by the International Institute of Management Development during the period 2020–2024. The study also addresses the main cybersecurity challenges and risks facing the country, alongside reviewing national initiatives and development programs launched by official authorities to strengthen cybersecurity capabilities. Additionally, it examines the relationship between cybersecurity and Saudi Arabia's Vision 2030 and its role in achieving the strategic objectives. The study concludes that the Kingdom has made tangible achievements in building an integrated cybersecurity system, enabling it to occupy advanced positions globally. However, the rapid pace of technological developments necessitates the continuous enhancement of policies and capabilities to address emerging cybersecurity challenges.

Keywords: Cybersecurity, Cybersecurity Challenges, Global Cybersecurity Index, Saudi Vision 2030.

JEL Classification: L86 ;O33 ;H11 ;H56.

مقدمة :

شهد العالم خلال العقود الأخيرة تحولات عميقة بفعل الثورة الرقمية والتطور المتسارع في تكنولوجيا المعلومات والاتصال، مما أدى إلى بروز الفضاء السيبراني كمجال حيوي يؤثر في مختلف الأنشطة الاقتصادية والاجتماعية، وفي هذا السياق، أصبح الأمن السيبراني أحد الركائز الأساسية لضمان حماية البيانات والبنى التحتية الرقمية، والحفاظ على استمرارية الأعمال والمؤسسات.

وتأتي المملكة العربية السعودية ضمن الدول التي أولت اهتمامًا كبيرًا بتعزيز منظومة الأمن السيبراني، خاصة في ظل توجهها نحو التحول الرقمي وتنويع الاقتصاد بعيدًا عن النفط، وقد انعكس هذا الاهتمام في تحسن ترتيب المملكة في المؤشرات الدولية، وتبنيها لمجموعة من السياسات والمبادرات الوطنية المتقدمة.

ومع ذلك، فإن التوسع في استخدام التكنولوجيا يرافقه تزايد في التهديدات السيبرانية، مما يفرض تحديات كبيرة تتطلب استجابات إستراتيجية متكاملة توازن بين الأمن والتنمية.

في ظل التحول الرقمي المتسارع الذي تشهده المملكة العربية السعودية، تبرز إشكالية رئيسية تتمثل في:

إلى أي مدى نجحت المملكة العربية السعودية في تعزيز منظومة الأمن السيبراني في ظل التحول الرقمي، وما أبرز التحديات والجهود المبذولة لتحقيق ذلك في إطار رؤية 2030؟

ويتفرع عن هذه الإشكالية مجموعة من التساؤلات الفرعية:

- ما المقصود بالأمن السيبراني وما هي أهم مفاهيمه وأبعاده النظرية؟
- كيف تطور واقع الأمن السيبراني في السعودية وفق المؤشرات الدولية؟
- ما أبرز التحديات والمخاطر السيبرانية التي تواجه المملكة؟
- ما هي المبادرات والبرامج الوطنية المعتمدة لتعزيز الأمن السيبراني في المملكة؟
- كيف يساهم الأمن السيبراني في تحقيق أهداف رؤية 2030؟

المنهج المتبع:

تعتمد هذه الدراسة على المنهج الوصفي التحليلي، من خلال استعراض الأدبيات النظرية المتعلقة بالأمن السيبراني، وتحليل واقع المملكة العربية السعودية في هذا المجال، مع توظيف البيانات والتقارير الدولية ذات الصلة، خاصة مؤشر الأمن السيبراني العالمي، بهدف تفسير الظواهر واستخلاص النتائج.

تقسيمات البحث:

تم تقسيم البحث إلى عناصر أساسية وهي:

- الإطار النظري والمفاهيمي للأمن السيبراني.
- واقع الأمن السيبراني في المملكة العربية السعودية وتطور ترتيبها في المؤشرات الدولية.
- التحديات والمخاطر السيبرانية في المملكة العربية السعودية.
- المبادرات والبرامج الوطنية لتعزيز الأمن السيبراني .
- دور الأمن السيبراني في تحقيق رؤية المملكة العربية السعودية 2030.

1- الإطار النظري والمفاهمي للأمن السيبراني:

سنتطرق أولا مفهوم الأمن السيبراني، ثم أهدافه وفي الأخير التعرف على الأبعاد التي يعالجها الأمن السيبراني.

1.1- مفهوم الأمن السيبراني:

تفاوتت التشريعات الدولية والوطنية، إلى جانب الأحكام القضائية، في محاولاتها لوضع تعريف موحد للأمن السيبراني، لذا سنستعرض أهم التعريفات فيما يلي:

عرّف الاتحاد الدولي للاتصالات (ITU) الأمن السيبراني في تقريره لعامي 2010-2011 حول اتجاهات إصلاح الاتصالات، بأن الأمن السيبراني هو:"مجموعة من المهام، تشمل جمع الموارد والسياسات والإجراءات الأمنية والإرشادات ونهج إدارة المخاطر والتدريب وأفضل الممارسات والتقنيات التي تهدف إلى حماية البيئة السيبرانية وأصول المؤسسات والمستخدمين"(Adel & MILOUD, 2025, p. 70).

كما عرف الأمن السيبراني بأنه منظومة من الإجراءات والتقنيات الرامية إلى حماية الأجهزة الرقمية وقنوات الاتصال المرتبطة بها، بما يضمن استقرارها وموثوقيتها وخلوها من المخاطر والتهديدات، ويتطلب ذلك اعتماد مستوى مناسب من الحماية يكون كافيًا لمنع الوصول غير المصرح به أو أي تدخل قد يترتب عليه أضرار ذات طابع شخصي أو مهني أو تنظيمي أو مالي أو حتى سياسي، ولا يقتصر نطاق الأمن السيبراني على حماية الحواسيب فحسب، بل يمتد ليشمل مختلف مكونات البيئة التكنولوجية، إذ يرتبط في جوهره بحماية الأفراد الذين يعتمدون، بصورة مباشرة أو غير مباشرة، على الأنظمة والوسائط الإلكترونية في حياتهم اليومية.(بوصبع، 2024، صفحة 137).

الأمن السيبراني هو منظومة من التقنيات والممارسات المصممة لحماية الأجهزة والبيانات والبرمجيات من التهديدات والهجمات الإلكترونية. وبشكل عام، يركز هذا المجال على تأمين الأنظمة المعلوماتية الحساسة، ومكافحة الجرائم الإلكترونية، وتعزيز قدرات الدفاع السيبراني(بوقرص، 2022، صفحة 66).

2.1- أهداف وأبعاد الأمن السيبراني

1.2.1-أهداف الأمن السيبيراني

تتمثل أهداف الأمن السيبراني فيما يلي(المهندي، 2025، صفحة 210):

- مراقبة المخاطر المرتبطة بالكوارث الطبيعية والبشرية؛
- مراقبة البيئة السيبرانية؛
- مراقبة المخاطر التشغيلية التي قد تؤدي إلى تدمير الأنترنت، وذلك من خلال وضع إستراتيجيات لإدارة مخاطر الأمن السيبراني؛
- الحد من التجسس والتخريب الإلكتروني على مستوى أجهزة الدولة والأفراد؛
- إتخاذ جميع الإجراءات الضرورية لحماية المواطنين والمقيمين على حد سواء من المخاطر المحتملة في مجال إستخدام الإلكترونيات؛
- يساهم في سد الفجوات والثغرات في الشبكات وأنظمة المعلومات؛
- توفير الحماية اللازمة والضرورية من أي إختراق في النظم الإلكترونية.

2.2.1- أبعاد الأمن السيبيراني

يوجد للأمن السيبراني أبعاد متعددة، يمكن تصنيفها على النحو التالي:

أ- البعد القانوني

إن التطورات التكنولوجية المتسارعة، تفرض مواكبة التشريعات القانونية لها، من خلال وضع أطر وتشريعات للأعمال القانونية وغير قانونية في الفضاء السيبيراني، فالملاحظ أن الجريمة السيبرانية تفتقد في معظم البلدان إلى الأطر القانونية الصارمة للتعامل معها، إضافة إلى ضرورة تفعيل التعاون الدولي المشترك لمكافحتها(المرداس، 2023، صفحة 215).

ب- البعد الاقتصادي

يشمل هذا البُعد حماية الموارد الاقتصادية وتجنب خسارتها، حيث تسعى المؤسسات جاهدةً لحماية أصولها الاقتصادية من الأضرار الناجمة عن ضعف الأمن وخطر الهجمات أو الاختراقات التي قد تُقلل من القيمة الاقتصادية لأي مؤسسة أو دولة.(Tadjeddine & Benazza, 2025, p. 285)

ج- البعد الاجتماعي

يُشير التقرير الصادر عن منظمة "المجتمع هو نحن" إلى أن حوالي 2.5 مليار شخص، أو 35% من سكان العالم، يستخدمون الإنترنت، والذي له دوراً هاماً في تمكين المواطنين من التعبير عن آرائهم وتطلعاتهم في مختلف المجالات، ومع ذلك فإنه يُشكل أيضاً تهديدات مثل الإرهاب، وانتشار الأيديولوجيات المتطرفة، وتجنيد الشباب وتشجيع الاتجار غير المشروع (Tadjeddine & Benazza, 2025, p. 285).

لهذا يجب توفير تعليم وتدريب في مجال تكنولوجيا المعلومات والاتصالات، وليس فقط تدابير الردع والأمن، كما يجب غرس ثقافة الأمن في ثقافة تكنولوجيا المعلومات، ومن الضروري تطوير مجموعة من الأخلاقيات الأمنية التي يتم قبولها واحترامها من قبل جميع العاملين في الفضاء السيبراني(سليمان و بوقرين، 2022، صفحة 47).

د- البعد العسكري

نشأ الإنترنت في بيئة عسكرية قبل أن يمتد إلى الأوساط الأكاديمية والبحثية التي ساهمت في تعزيز القدرات العسكرية والإنجازات العلمية، وتتجلى مخاطر الهجمات الإلكترونية في التجسس والسرقة والاختراقات، مما قد يؤدي إلى نتائج ملموسة مثل اندلاع النزاعات المسلحة(tadjeddine & benazza, 2025, p. 285).

هـ- البعد السياسي

يتضمن هذا البعد مسؤولية الدولة وسيادتها في تحقيق الأمن السيبراني، مما يتطلب جهودا شاملة، ولا ينبغي أن تقتصر هذه الجهود على دعم البحث والتطوير فحسب، بل يجب أن تشمل أيضاتعزيز ثقافة الأمن، وتنفيذ استراتيجيات الوقاية والإبلاغ، وتشجيع تبادل المعلومات، ورفع مستوى الوعي بأفضل الممارسات وإدارة المخاطر(tadjeddine & benazza, 2025, p. 285).

2- واقع الأمن السيبراني في السعودية

شهدت المملكة العربية السعودية مؤخرا تطورات عدة بشأن تنظيم الأمن السيبراني، إذ جرى إصدار مرسومًا ملكيًا رقم 6801 لعام 1439/2/11 (31 أكتوبر 2017)، للموافقة على لائحة الهيئة الوطنية للأمن السيبراني، المحددة لأدوار ومسؤوليات الهيئة، والتي تعزز قانون استخدام تكنولوجيا المعلومات والاتصالات في الوكالات الحكومية. الجدير بالذكر أن الشركات في المملكة العربية السعودية، عانت وقت بداية جائحة كورونا ولجوئها إلى العمل عن بُعد، من الملايين من الهجمات الإلكترونية والتي بلغ عددها 22.5 مليون هجوم إلكتروني، كلف الدولة خسائر قُدرت بـ 6.5 مليون دولار.

ولموقع المملكة العربية السعودية الاستراتيجي في المنطقة، تعرضت البنية التحتية لتكنولوجيا المعلومات والاتصالات في كل من القطاعين العام والخاص لتهديدات مستمرة بسبب الحوادث الإلكترونية، تلك الحوادث التي أثرت بالسلب على الاقتصاد من حيث المستوى المالي والتشغيلي والتكتيكي(Bakkah، 2025).

وفي ظل هذا الواقع، برز الأمن السيبراني كأحد المرتكزات الأساسية الداعمة لمسار التحول الرقمي المتسارع في المملكة، وكعامل حاسم في تعزيز الاستقرار الاقتصادي وترسيخ الثقة في البيئة الرقمية. وقد تجسد هذا التوجه في التقدم اللافت الذي أحرزته المملكة في مؤشر الأمن السيبراني العالمي الصادر عن المعهد الدولي للتنمية الإدارية(IMD) ، نتيجة تبني سياسات واستراتيجيات وطنية شاملة، قادتها الهيئة الوطنية للأمن السيبراني، وركزت على تطوير البنية التحتية الرقمية، وبناء القدرات الوطنية، ورفع مستوى الوعي الأمني. ويُبرز الجدول التالي تطور ترتيب المملكة في هذا المؤشر خلال الفترة (2020–2024)، بما يعكس حجم التقدم المحقق، ومدى اتساقه مع مستهدفات رؤية السعودية 2030 في بناء اقتصاد رقمي آمن ومستدام.

جدول رقم(01) :تطور ترتيب السعودية في مؤشر الامن السيبراني (2020-2024)

السنة	الترتيب العالمي	الملاحظة
2020	المرتبة 11 عالميا	مرحلة التأسيس وتعزيز الإطار المؤسسي
2021	المرتبة7 عالميا	بداية التموقع ضمن الدول المتقدمة
2022	المرتبة 4 عالميا	تحسن ملحوظ بفضل تعزيز الأطر التنظيمية
2023	المرتبة 2 عالميا	قفزة نوعية ودخول المراتب الأولى
2024	المرتبة 2 عالميا	الحفاظ على الأداء الريادي

المصدر:(World Competitiveness Yearbook, 2020-2021-2022-2023-2024).

يظهر تطور ترتيب المملكة العربية السعودية في مؤشر الأمن السيبراني خلال الفترة (2020–2024) تحسنًا تدريجيًا ملحوظًا، حيث انتقلت من المرتبة 11 عالميًا سنة 2020 إلى المرتبة الثانية عالميًا في عامي 2023 و2024، وفقًا لتقارير المعهد الدولي للتنمية الإدارية .ويعكس هذا التحسن انتقال المملكة من مرحلة بناء الأسس التنظيمية والمؤسسية إلى مرحلة التمكين والريادة في المجال السيبراني.

كما يرتبط هذا المسار التصاعدي فعالية السياسات الوطنية في هذا المجال والتزام المملكة بتعزيز أمنها السيبراني وفق رؤية السعودية2030، التي جعلت من التحول الرقمي ركيزة أساسية لتحقيق اقتصاد متنوع ومستدام، فقد أسهمت على الابتكار، وبناءا لقدرات، والتعاون الدولي، مما مكنها من التحول إلى نموذج رائد على المستوى العالمي في هذا المجال.

3- التحديات والمخاطر السيبرانية في السعودية

تواجه المملكة العربية السعودية شأنها شأن مختلف دول العالم، جملة من التحديات المتشابكة في مجال الأمن السيبراني، وتتنوع بين الجوانب التقنية المرتبطة بالتهديدات الرقمية، وأخرى ذات أبعاد اجتماعية وسياسية، ومن أبرز هذه المخاطر والتحديات:

1.3- الهجمات الالكترونية المنظمة

تعد من أخطر التهديدات السيبرانية التي تواجه الشركات في السعودية، حيث تستهدف برمجيات الفدية (Ransomware)إذ يقوم المهاجمون بتشفير البيانات

الحساسة وطلب فدية مقابل فك التشفير، كما تستهدف الهجمات الموجهة للبنى التحتية الحيوية الحساسة مثل الطاقة (النفط والغاز)، البنوك، الصحة(chobixo Tech، 2026)

2.3- نقص الكوادر والخبرات المتخصصة

:رغم الجهود المبذولة في مجالات التعليم والتدريب، لا يزال الطلب المتنامي على المهارات السيبرانية يمثل تحديًا كبيرًا في توفير الكفاءات المؤهلة، خاصة في ظل المنافسة العالمية المتزايدة على استقطاب الخبرات في هذا المجال الحيوي والمتسارع التطور(المرداس، 2023، صفحة 216)

3.3- التهديدات السياسية والممولة دوليا

تواجه بعض الجهات الحكومية والبنى التحتية الحيوية في المملكة محاولات اختراق متقدمة تنفذها مجموعات سيبرانية مرتبطة بجهات خارجية، وتهدف هذه الهجمات إلى التجسس أو إحداث اضطرابات في تقديم الخدمات، كما برزت في الآونة الأخيرة تحذيرات من نشاط مجموعات "الهاكتيفيست" ذات الدوافع السياسية، لا سيما المرتبطة بالقضايا الإقليمية، والتي قد تعلن عن تنفيذ هجمات واسعة النطاق تستهدف مؤسسات داخل المملكة.(أكاديمية الأمن السيبراني، 2025)

4.3- ضعف الوعي الأمني لدى المستخدمين

يُعدّ ضعف الوعي الأمني لدى المستخدمين من أبرز نقاط الهشاشة في منظومة الأمن السيبراني، حيث ينعكس ذلك في محدودية الالتزام بالممارسات الأمنية السليمة، مثل استخدام كلمات مرور قوية وتحديث الأنظمة بشكل دوري. كما أن نقص الإدراك بالمخاطر السيبرانية لدى بعض الأفراد يجعلهم أكثر عرضة لأساليب الهندسة الاجتماعية والتصيد الاحتيالي، الأمر الذي يساهم بشكل مباشر في تسهيل نجاح الهجمات الإلكترونية واختراق الأنظمة المعلوماتية (Aljedaani, Ahmad, Zahedi, & Babar, 2020).

5.3- تحديات التحول الرقمي والتقنيات الحديثة

مع إستخدام تقنيات مثل الحوسبة السحابية، الذكاء الاصطناعي، تظهر مخاطر جديدة مثل "الذكاء الاصطناعي الظلي"(إستخدام غير منضبط للتقنيات) وصعوبة حوكمة البيانات.(IBM، 2026)

6.3- تطور التهديدات السيبرانية وتعقدها

أصبحت الهجمات الالكترونية أكثر تطورا، حيث لم تعد تقتصر على الفيروسات التقليدية، بل تشمل الهجمات المدعومة بالذكاء الاصطناعي، هجمات الحرمان من الخدمة (DDoS)، التهديدات الداخلية، وهذا يجعل إكتشافها والتصدي لها أكثر صعوبة.(حميدي، 2025).

4-المبادرات والبرامج الوطنيةفي السعودية

تبذل المملكة العربية السعودية اهتمامًا متزايدًا بتعزيز منظومة الأمن السيبراني، حيث حققت مكانة متقدمة على الصعيد الدولي في هذا المجال، وتتولى الهيئة الوطنية للأمن السيبراني قيادة هذه الجهود عبر تنفيذ حزمة متكاملة من المبادرات والبرامج الوطنية، التي تهدف إلى تنمية القدرات البشرية والتقنية، ودعما لابتكار، ونشر الوعي الأمني، وفيما يلي أبرز هذه المبادرات والبرامج الوطنية في مجال الأمن السيبراني بالمملكة (الهيئة الوطنية للأمن السيبراني، 2025):

1.4-مبادرات بناء القدرات والتدريب (الأكاديمية الوطنية للأمن السيبراني)

1.1.4-برنامج سايبرك (CyberK):

يهدف هذا البرنامج إلى إعداد وتدريب نحو 1500 مختص سعودي، من خلال تأهليهم في مجالات متعددة ضمن قطاع الأمن السيبراني، بما يسهم في تعزيز الكفاءات الوطنية في هذا المجال الحيوي.

2.1.4-مبادرة البحث الصيفي الدولي في الأمن السيبراني

أطلقت هذه المبادرة في يناير 2026 بهدف تنمية وتعزيز القدرات البحثية لدى الطلاب والباحثين السعوديين، من خلال دعم مهاراتهم في مجالات الأمن السيبراني التي تمثل أولوية وطنية.

3.1.4-التدريب السيبراني للجهات الحكومية

تعني هذه البرامج المتخصصة بتعزيز قدرات وكفاءة فرق الأمن السيبراني في الجهات الحكومية، بما يمكنها من حماية أصولها التقنية وضمان أمن بنيتها الرقمية بكفاءة عالية.

2.4- مبادرات الابتكار والاستثمار (تحفيز السوق)

تُعدّ من الركائز الأساسية لتحفيز السوق وتعزيز النمو الاقتصادي. فهي تسهم في دعم رواد الأعمال والشركات الناشئة من خلال توفير التمويل، وتبسيط الإجراءات، وخلق بيئة مشجعة على الإبداع والتطوير. كما تساعد هذه المبادرات على جذب الاستثمارات المحلية والأجنبية، وتطوير قطاعات جديدة قائمة على المعرفة والتكنولوجيا، مما ينعكس إيجابًا على فرص العمل وزيادة التنافسية في السوق. وبذلك، يشكل الابتكار والاستثمار معًا محركًا فعالًا لتحقيق التنمية المستدامة، ومن بين هذه المبادرات التي سعت المملكة العربية السعودية على تحقيقها هي(الهيئة الوطنية للأمن السيبراني، 2025):

1.2.4-مسرعة الأمن السيبراني(Cyber Accelerator)

أطلقت الهيئة نسخاً متعددة مثل النسخة الثالثة في نوفمبر 2025لدعم الشركات الناشئة والمبتكرين في المجال السيبران، وتحفيز الاستثمار في قطاع الأمن السيبراني مع تعزيز منظومة ريادة الأعمال في المملكة.

2.2.4-منح الابتكار في تحديات صناعة الأمن السيبراني

مبادرة تستهدف إستكشاف الحلول المبتكرة لمواكبة المستجدات والتوجهات العالمية ومواجهة التحديات الحالية والمستقبلية في مجال الأمن السيبراني، من خلال تعزيز التعاون بين الجهات الأكاديمية والبحثية وجهات القطاعين العام والخاص، بما يسهم في نمو صناعة الأمن السيبراني على المستوى الوطني، وذلك ضمن مبادرات "البرنامج الوطني للبحث والتطوير والابتكار في الأمن السيبراني".

3.2.4-برنامج ريادة الأعمال في الأمن السيبراني

برنامج لتطوير بيئة ريادة الأعمال ودعم المشاريع المبتكرة في الأمن السيبراني، وتنوع المبادرات التي تتسم بها لتغطية رحلة رواد الاعمال في المجال منذ تحويل الأفكار الإبداعية إلى مشاريع مستدامة.

4.2.4-البرنامج الوطني للبحث والتطوير والابتكار في الأمن السيبراني

برنامج متخصص يضم مجموعة من المبادرات النوعية التي تهدف إلى تعزيز الشراكات المستدامة على المستويين المحلي والدولي، بما يسهم في تمكين منظومة البحث والتطوير والابتكار في قطاع الأمن السيبراني، كما يعمل على توسيع آفاق تطوير الأبحاث والابتكارات وصقل الكفاءات الواعدة في المجالات ذات الأولوية الوطنية، بما يتوافق مع التوجهات السيبرانية والتطورات التقنية الراهنة والمستقبلية، ويسعى البرنامج كذلك إلى دعم الإنتاج العلمي وتعزيز تبادل المعرفة، إلى جانب بناء قدرات وطنية رائدة في مجالات البحث والتطوير والابتكار في الأمن السيبراني.

3.4-مبادرات الوعي والامتثال

1.3.4-الحملة الوطنية للتوعية بالأمن السيبراني (Cyber Aware)

حملة مستمرة تم إطلاقها مؤخراً في 2026لرفع مستوى الوعي بالمخاطر الرقمية والوقاية منها.(الهيئة الوطنية للأمن السيبراني، 2025)

2.3.4- مبادرة "وعي رقمي. وطن آمن"

تشمل تنفيذ برامج وورش عمل توعية داخل الإدارات الحكومية، وبث رسائل مرئية عبر الشاشات والوسائل الرقمية في المنطقة، إضافة إلى تفعيل الحملة عبر منصات التواصل الاجتماعي، بمشاركة عدد من الجهات الحكومي، كما تستهدف رفع مستوى الاستخدام الآمن للتقنية لدى الموظفين، الأسر، وطلاب المدارس.(مجلة عالم التكنولوجيا، 2025).

3.3.4-إلزامية الضوابط الأساسية للأمن السيبراني (NCA ECC)

فرض ضوابط الأمن السيبراني الأساسية (ECC) على جميع الجهات الحكومية والجهات ذات الأهمية الحيوية لضمان الامتثال.(الكيان السيبراني ، 2026)

4.4-مبادرات دولية وشراكات

1.4.4-المبادرة العالمية لبناء القدرات في الفضاء السيبراني

أطلقتها المملكة العربية السعودية بالشراكة مع الأمم المتحدة ضمن المنتدى الدولي للأمن السيبراني(GCF 2025) المنعقد في الرياض، بهدف توحيد الجهود الدولية لمواجهة التحديات الاستراتيجية في هذا المجال(الهيئة الوطنية للأمن السيبراني، 2025).

2.4.4-منصة "حصين"

تُعد منصة متكاملة تُعنى بحماية الفضاء الرقمي، وذلك عبر تقديم خدمات توعوية وإتاحة معايير ومؤشرات أمنية مرجعية تسهم في دعم المؤسسات والأفراد وتعزيز مستويات الحماية الرقمية لديهم. كما توفر 14 خدمة متخصصة صُممت خصيصًا للارتقاء بمستوى الأمن السيبراني لدى الأفراد، وكذلك في القطاعين العام والخاص.(منصة حصين، 2026)

5. الأمن السيبراني ورؤية المملكة العربية السعودية 2030

يعدّ الأمن السيبراني أحد الدعائم الجوهرية لتحقيق مستهدفات رؤية السعودية 2030، لاسيما في مجالي التحول الرقمي وتعزيز النمو الاقتصادي، فقد أبرزت التقارير الرسمية السنوية للرؤية الأهمية الاستراتيجية للأمن السيبراني باعتباره عنصرًا محوريًا في دعم مسار التحول الوطني الرقمي، حيث يسهم تبنّي أنظمة حماية متقدمة في ترسيخ ثقة المستثمرين والمستخدمين في البيئة الرقمية، ويفتح المجال أمام القطاعات التنموية للاستفادة من الفرص الرقمية المتاحة.(رؤية السعودية 2030، 2026)

إذ حققت "رؤية السعودية 2030 " تطورا ملحوظا على مختلف الأصعدة، حيث أظهرت بيانات رسمية أن 93% من مؤشرات الأداء بنهاية عام 2024 قد

حققت مستهدفاتها أو تجاوزتها أو اقتربت منها، شملت محاور إستراتيجية المملكة 2030 ثلاث محاوررئيسية وهي(CNBC عربية، 2025):

- **مجتمع حيوي** :من خلال حماية بيانات الأفراد وضمان خصوصيتهم في التعاملات الرقمية.
- **اقتصاد مزدهر** :عبر توفير بيئة رقمية آمنة تشجع الاستثمار في التقنيات الحديثة والتجارة الإلكترونية.
- **وطن طموح** :من خلال تعزيز كفاءة المؤسسات الحكومية ورفع مستوى جاهزيتها لمواجهة المخاطر السيبرانية.

1.5- برامج تحقيق الرؤية

أسهمت برامج تحقيق الرؤية، بوصفها كيانات مرحلية متوسطة الأجل أُنشئت في المرحلة الأولى لإطلاق رؤية السعودية 2030، في تعزيز مستوى التنسيق والتكامل بين مكونات المنظومة، كما أدت دورًا محوريًا في تسريع وتيرة الإنجاز. وقد تمكنت هذه البرامج من تجاوز عدد من المستهدفات الطموحة، إلى جانب إسهامها في تنمية القدرات البشرية والمؤسسية، وتزويد الجهات الحكومية بالأدوات والمنهجيات اللازمة لدعم استدامة النمو وتعزيز كفاءة الأداء المؤسسي.

شهدت هذه البرامج مسارًا تطوريًا مستمرًا، بهدف ضمان اتساقها مع الأهداف الإستراتيجية واستجابتها للتحولات الاقتصادية والتنموية، وفي هذا الإطار، جرى إعادة هيكلة بعض البرامج من خلال دمج بعضها و إغلاق أخرى، إلى جانب استحداث برامج جديدة تتلاءم مع متطلبات المرحلة. ومن أبرز هذه التحولات اكتمال الخطة التنفيذية لبرنامج الاستدامة المالية، الذي نجح في تحقيق مستهدفاته وإثبات فاعليته في إحداث أثر مستدام، وذلك عبر دمج اختصاصاته ضمن الجهات ذات العلاقة. وبناءً على ذلك، استقر عدد برامج تحقيق الرؤية حاليًا عند 10 برامج وهم برنامج تطوير القطاع المالي، برنامج الإسكان، برنامج التحول الوطني، برنامج التخصيص، برنامج تنمية القدرات البشرية، برنامج خدمة ضيوف الرحمن، برنامج جودة الحياة، برنامج تحول القطاع الصحي، برنامج تطوير

الصناعة الوطنية والخدمات اللوجستية، برنامج صندوق الاستثمارات العامة. (التقرير السنوي لرؤية السعودية 2030 لعام 2024، 2024، صفحة 8)

2.5- الاستراتيجيات الوطنية لرؤية2030

تعتبر الاستراتيجيات الوطنية القطاعية والمناطقية أدوات أساسية لتنفيذ رؤية السعودية 2030، حيث تلعب دورًا حيويًا في تحقيق النمو المستدام وتوجيه التحول الاقتصادي على المدى الطويل، تركز هذه الاستراتيجيات على تطوير القطاعات وتنمية المناطق، مما يضمن تحقيق الازدهار على جميع المستويات.

منذ إطلاق الرؤية في عام 2016، وضعت الرؤية الأسس اللازمة للتنمية من خلال برامج تحقيق الرؤية ومبادرات استراتيجية تهدف إلى إحداث إصلاحات هيكلية وتحسين بيئة الأعمال. ومع مرور السنوات، تم إطلاق إمكانات واعدة في قطاعات متنوعة، مما زاد الحاجة إلى تطوير استراتيجيات وطنية متخصصة في قطاعات معينة واستراتيجيات تنموية لمناطق مختلفة، وقد ساهم ذلك في تعزيز مسيرة التحول الشاملة، والتنويع الاقتصادي، وتحقيق فوائد اقتصادية واجتماعية في مختلف أرجاء المملكة.

تشهد المملكة العربية السعودية اليوم تحولًا غير مسبوق، يظهر من خلال تنوع القطاعات ونموها المتزايد، بدءًا من السياحة والثقافة، وصولًا إلى الطاقة المتجددة والتعدين، ومع وجود استراتيجيات محكمة تنفذها منظومة حكومية فعالة، يتوقع أن تشهد المرحلة القادمة إطلاق المزيد من الاستراتيجيات الوطنية والقطاعية والمناطقية، بما يعزز القدرة على إستثمار الفرص الناشئة ومواكبة التحولات العالمية، مما يجعل المملكة مركزًا حيويًا لكل فرصة جديدة وحاضنة لكل طموح يسعى ليكون جزءًا من مستقبل مزدهر يتشكل يومًا بعد يوم على أرضنا.(التقرير السنوي لرؤية السعودية 2030 لعام 2024، 2024، صفحة 9)

الخاتمة

يخلص هذا المقال إلى أن الأمن السيبراني لم يعد مجرد مسألة تقنية، بل أصبح عنصرًا استراتيجيًا محوريًا في دعم التنمية الاقتصادية وتعزيز الأمن الوطني،

وقد أظهرت المملكة العربية السعودية تقدمًا ملحوظًا في هذا المجال، سواء من خلال تحسين ترتيبها في المؤشرات الدولية أو عبر إطلاق مبادرات وطنية طموحة.

غير أن التحديات السيبرانية المتزايدة، الناتجة عن التطور التكنولوجي السريع تفرض على المملكة ضرورة الاستمرار في تطوير قدراتها البشرية والتقنية، وتعزيز التعاون الدولي، وتبني سياسات مرنة وفعالة.

وفي ضوء رؤية 2030، يظل الأمن السيبراني أحد الأعمدة الأساسية لضمان نجاح التحول الرقمي وتحقيق اقتصاد معرفي مستدام، مما يستدعي مواصلة الاستثمار في هذا المجال الحيوي وتعزيز الوعي المجتمعي بأهميته.

نتائج الدراسة

توصلت هذه الدراسة إلى مجموعة من النتائج الأساسية التي تعكس واقع الأمن السيبراني في المملكة العربية السعودية ودوره في دعم التنمية، من أبرزها:

- **تزايد الأهمية الإستراتيجية للأمن السيبراني:**أصبح الأمن السيبراني عنصرًا محوريًا في حماية الاقتصاد الرقمي وضمان استمرارية الأنشطة الحيوية، خاصة في ظل الاعتماد المتزايد على التقنيات الحديثة.
- **تطور ملحوظ في أداء المملكة دوليًا:**حققت المملكة العربية السعودية تقدمًا واضحًا في مؤشرات الأمن السيبراني العالمية، بما في ذلك مؤشر المعهد الدولي للتنمية الإدارية، وهو ما يعكس فاعلية السياسات والاستراتيجيات المتبعة.
- **تعدد التهديدات والمخاطر السيبرانية:**تواجه المملكة تحديات متزايدة تشمل الهجمات الإلكترونية، والاختراقات، والجرائم السيبرانية، والتي تستهدف القطاعات الحيوية مثل الطاقة والمالية.
- **فعالية المبادرات الوطنية:**أسهمت البرامج والمبادرات الوطنية في تعزيز البنية التحتية للأمن السيبراني، ورفع مستوى الجاهزية والاستجابة للحوادث السيبرانية.

- **ارتباط وثيق بين الأمن السيبراني ورؤية 2030:**يمثل الأمن السيبراني ركيزة أساسية لتحقيق التحول الرقمي وتنويع الاقتصاد، مما يجعله عاملًا حاسمًا في نجاح رؤية المملكة 2030.
- **الحاجة المستمرة لتطوير الكفاءات البشرية:**رغم التقدم المحقق، لا يزال هناك طلب متزايد على الكوادر الوطنية المؤهلة في مجال الأمن السيبراني.

التوصيات:

بناءً على النتائج المتوصل إليها، يمكن تقديم مجموعة من التوصيات لتعزيز الأمن السيبراني في المملكة العربية السعودية:

- **تعزيز الاستثمار في رأس المال البشري:**من خلال تطوير البرامج التعليمية والتدريبية المتخصصة في الأمن السيبراني، وربطها باحتياجات سوق العمل.
- **تحديث التشريعات والسياسات باستمرار:**لضمان مواكبة التطورات السريعة في التهديدات السيبرانية، مع تعزيز الأطر القانونية الرادعة للجرائم الإلكترونية.
- **تعزيز الشراكات الدولية:**عبر التعاون مع المنظمات والدول المتقدمة لتبادل الخبرات وأفضل الممارسات في مجال الأمن السيبراني.
- **رفع مستوى الوعي المجتمعي:**من خلال حملات توعوية تستهدف الأفراد والمؤسسات حول مخاطر الفضاء السيبراني وطرق الوقاية.
- **دعم الابتكار والتقنيات الحديثة:**الاستثمار في مجالات مثل الذكاء الاصطناعي وتحليل البيانات لتعزيز قدرات الكشف المبكر عن التهديدات.
- **تعزيز حماية البنى التحتية الحيوية:**عبر تبني أنظمة متقدمة للحماية والاستجابة السريعة، خاصة في القطاعات الحساسة مثل الطاقة والمصارف.

الهوامش

1. أكاديمية الأمن السيبراني، "أكثر هجمات الأمن السيبراني شيوعاً"، (28 مارس، 2025)، استُرد من: cyberscourse.com
2. مجلة عالم التكنولوجيا، "للحماية من المخاطر الرقمية: تدشين مبادرة..."، (02 ديسمبر، 2025)، استُرد من: tech-mag.net

3. الهيئة الوطنية للأمن السيبراني، الموقع الرسمي، (2025)، استُرد من: nca.gov.sa
4. CNBC عربية، "ما أبرز ما جاء في التقرير السنوي لرؤية السعودية 2030"، (25 أبريل، 2025)، استُرد من: cnbcarabia.com
5. منصة بكة (Bakkah)، "الأمن السيبراني في السعودية"، (جانفي، 2025)، استُرد من: bakkah.com
6. chobixo Tech، "Cybersecurity threats Saudi Arabia 2026"، 28) مارس، 2026)، استُرد من: chobixo.com
7. IBM، "Cybersecurity trends: IBM predictions 2025"، 28) مارس، 2026)، استُرد من: ibm.com
8. منصة حصين، الموقع الرسمي، (28 مارس، 2026)، استُرد من: haseen.gov.sa
9. الكيان السيبراني، "الضوابط الأساسية للأمن السيبراني ("NCA-ECC"، 30) مارس، 2026)، استُرد من: csentity.com
10. أسماء بن جدو، سلاف بوصبع، "أثر سياسات الأمن السيبراني على الأمن القومي الأمريكي: قراءة في التجربة وفي إمكانية التطبيق على الحالة الجزائرية"، مجلة الدراسات، المجلد 08، العدد 02، (22 ديسمبر، 2024).
11. رؤية السعودية 2030، "التقرير السنوي لرؤية السعودية 2030 لعام 2024"، (2024)، استُرد من: vision2030.gov.sa
12. رؤية السعودية 2030، البوابة الرسمية، (26 مارس، 2026)، استُرد من: vision2030.gov.sa
13. ساعد بوقرص، "الأمن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات وإستراتيجيات خاصة"، المجلد 03، العدد 01، (22 جوان، 2022).
14. علاء الدين حميدي، "الأمن السيبراني: خط الدفاع الأول"، الجزيرة نت - تكنولوجيا، (10 ديسمبر، 2025)، استُرد من: aljazeera.net
15. قطاف سليمان، عبد الحليم بوقرين، "الأمن السيبراني والمضامين المفاهيمية المرتبطة به"، مجلة طبنة للدراسات العلمية الأكاديمية، المجلد 05، العدد 02، (2022)، ص 47.
16. محمد حسن المهندي، "الإطار القانوني للأمن السيبراني في المحافظة على الصحة العامة في القانون القطري: دراسة مقارنة"، المجلد 14، العدد 02، (16 جوان، 2025).
17. ندى بنت خالد المرداس، "الأمن السيبراني في المملكة العربية السعودية بين الواقع والمأمول (دراسة نظرية تحليلية)"، المجلة الدولية لنشر البحوث والدراسات، المجلد 5، العدد 49، (20 نوفمبر، 2023)، ص 215.

18. Adel, K & ,.Miloud, H. (2025, June 02). "Mechanisms Anti Crimes Electronic and its role in ."*Researcher Journal for Academic Studies* ,(02)12 ,p. 70.
19. Aljedaani, B., Ahmad, A., Zahedi, M & ,.Babar, M. (2020, August 29). Retrieved from arXiv :https://arxiv.org/abs/2008.13009
20. Tadjeddine, H & ,.Benazza, S. (2025, December 7). "The Algerian Legislator's Strategy in Addressing Cyber Crimes ."*Journal of Science and Knowledge Horizons* , .(2)5
21. International Institute for Management Development. (2020-2024 .(*World Competitiveness Yearbook* .Lausanne, Switzerland.

قائمة المصادر والمراجع

1- المراجع باللغة العربية

- المجلات العلمية والدوريات

- أسماء بن جدو، وسلاف بوصبع .(2024) .أثر سياسات الأمن السيبراني على الأمن القومي الأمريكي: قراءة في التجربة وفي إمكانية التطبيق على الحالة الجزائرية .مجلة الدراسات والبحوث القانونية، .(02)08
- ساعد بوقرص .(2022) .الأمن السيبراني: مخاطر وتهديدات وتحديات تتطلب ممارسات وتوصيات وإستراتيجيات خاصة .مجلة البحوث العلمية، .(01)03
- قطاف سليمان، وعبد الحليم بوقرين .(2022) .الأمن السيبراني والمضامين المفاهيمية المرتبطة به .مجلة طبنة للدراسات العلمية الأكاديمية، .(02)05
- محمد حسن المهندي .(2025) .الإطار القانوني للأمن السيبراني في المحافظة على الصحة العامة في القانون القطري: دراسة مقارنة .مجلة القانون، .(02)14
- ندى بنت خالد المرداس .(2023) .الأمن السيبراني في المملكة العربية السعودية بين الواقع والمأمول (دراسة نظرية تحليلية .(المجلة الدولية لنشر البحوث والدراسات، 5(49).

- التقارير الرسمية والوثائق الحكومية

- رؤية السعودية 2030 .(2024) .التقرير السنوي لرؤية السعودية 2030 لعام 2024 . المملكة العربية السعودية.
- الهيئة الوطنية للأمن السيبراني .(2025) .الموقع الرسمي للهيئة. المملكة العربية السعودية.
- رؤية السعودية 2030 .(2026) .الموقع الرسمي للرؤية.

- المواقع الإلكترونية، المنصات، والمدونات

- أكاديمية الأمن السيبراني .(2025) .أنواع الهجمات السيبرانية الأكثر شيوعاً.
- علاء الدين حميدي .(2025) .الأمن السيبراني خط الدفاع الأول .الجزيرة نت - تكنولوجيا.
- الكيان السيبراني .(2026) .التنظيمات والسياسات: الضوابط الأساسية للأمن السيبراني.
- مجلة عالم التكنولوجيا .(2025) .للحماية من المخاطر الرقمية: تدشين مبادرات سيبرانية.
- منصة بكة .(2025) .(Bakkah) الأمن السيبراني في السعودية: مركز المعرفة.
- منصة حصين .(2026) .خدمات الأمن السيبراني الوطني.
- CNBCعربية .(2025) .ما أبرز ما جاء في التقرير السنوي لرؤية السعودية.

2- المراجع باللغة الأجنبية

-Journals & Papers

- Adel, K., & Miloud, H. (2025). Mechanisms Anti Crimes Electronic and its role in. *Journal of Researcher for Academic Studies*, 12(02).
- Aljedaani, B., Ahmad, A., Zahedi, M., & Babar, M. (2020). *Empirical study on cybersecurity*. (Research Paper via arXiv).
- Tadjeddine, H., & Benazza, S. (2025). The Algerian Legislator's Strategy in Addressing Cyber Crimes. *Journal of Science and Knowledge Horizons*, 5(02).

-Books & Annual Reports

- International Institute for Management Development (IMD). (2020-2024). *World Competitiveness Yearbook*. Lausanne, Switzerland.

- Websites & Tech Insights

- Chobixo Tech. (2026). Cybersecurity threats in Saudi Arabia 2026.
- IBM Think. (2026). Cybersecurity trends and predictions 2025.