

جهود مملكة البحرين في مواجهة المخاطر السيبرانية في المؤسسات الحكومية - دراسة تطبيقية

The Efforts of the Kingdom of Bahrain in Addressing Cyber Risks in Government Institutions – An Applied Study

د. محمد عيسى البوعينين¹

Mohd39599874 @gmail.com

تاريخ النشر: 2026/03/15

Received: 09/07/2025

تاريخ الاستلام: 2025/07/09

published: 15/03/2026

ملخص المقال:

هدفت هذه الدراسة إلى التعرف على واقع المخاطر السيبرانية في مملكة البحرين و العقبات التي تواجهها و دراسة الاتجاهات التي يلعبها الأمن السيبراني ومدى الاستفادة منها في مملكة البحرين، وقد أستخدم الباحث المنهج الوصفي التحليلي وتكونت عينة الدراسة من (414) مفردة، حيث تم اختيار العينة من الإدارات العليا والوسطى في مؤسسات مملكة البحرين من خلال أسلوب العينة الطبقية التناسبية . وتكون عينة البحث من (335) فرداً، حيث تكون العينة ممثلة للمجتمع البالغ عدده (2680) موظفاً وموظفة. وقد أظهرت نتائج البحث أن إدارة المخاطر السيبرانية في المؤسسات الحكومية بمملكة البحرين بمستوى متوسط، وجود علاقة ارتباطية موجبة ومتوسطة القوة ودالة إحصائياً بين وعي العاملين بالمخاطر السيبرانية وقدرتها على إدارة هذه المخاطر، وأوصت الدراسة بالكثير من التوصيات وكان أبرزها العمل على بناء الكوادر الوطنية في مجالات تكنولوجيا المعلومات والأمن السيبراني من خلال تشجيع الابتكارات العلمية في مجال الأمن السيبراني.

الكلمات المفتاحية: المخاطر السيبرانية، أمن المعلومات، تقييم المخاطر، مملكة البحرين.

Abstract

This study aimed to identify the reality of cybersecurity risks in the Kingdom of Bahrain, the obstacles it faces, and to examine the trends played by cybersecurity and the extent to which it is utilized in the Kingdom of Bahrain. The researcher used a descriptive analytical approach, and the study sample consisted of 414 individuals, selected from senior and middle management in institutions in the Kingdom of Bahrain using a stratified proportional sampling method. The research sample comprised 335 individuals, representing a population of 2,680 employees. The results of the research indicated that the management of cybersecurity risks in government institutions in the Kingdom of Bahrain is at a moderate level, and there is a statistically significant positive correlation of medium strength between employees' awareness of cybersecurity risks and their ability to manage these risks. The study recommended several suggestions, the most prominent of which is to work on building national capacities in the fields of information technology and cybersecurity by encouraging scientific innovations in the field of cybersecurity.

Keywords: cybersecurity risks, information security, risk assessment, Kingdom of Bahrain.

¹ - آرياس للتعليم والتدريب البحرين

مقدمة:

يعتبر أمن المعلومات لا غنى عنه لمواجهة الجرائم الإلكترونية المتزايدة في جميع أنحاء العالم، الناتجة عن تطورات التقنية وزيادة استخدام التكنولوجيا الرقمية وتعتبر مملكة البحرين إحدى الدول الرائدة في تطوير البنية التحتية لتكنولوجيا المعلومات، الأمر الذي يزيد من التوقعات حول التهديدات الإلكترونية التي قد تشكل خطر كبير على المصلحة العامة، ولذلك فقد اتخذت حكومة البحرين الإجراءات اللازمة للتصدي هذه المخاطر من أجل تحسين جاهزية أمن المعلومات في الجهات الحكومية. (عجاج، 2017)

ولكن كثرة البيانات والمعلومات والكيانات الافتراضية داخل شبكة الإنترنت برز مصطلح القرصنة الإلكترونية وتتمثل مهامه في عملية اختراق الأنظمة وسرقة المعلومات لتداولها بين المهتمين بمقابل مادي، ومع مرور الأيام والتطور التكنولوجي وزيادة المهتمين بجمع البيانات توسعت أنشطة القرصنة حتى شملت الاختراقات والابتزاز والتجسس الدولي وسرقة معلومات حساسة، وتوجب على المؤسسات حماية القطاع التكنولوجي الخاص بها من الهجمات الإلكترونية على مناطق ضعيفة في أنظمة تشغيل الحاسب وهو ما يطلق عليه الثغرة السيبرانية. ومنها انبثق مصطلح إدارة الثغرات السيبرانية على أنها عملية مستمرة واستباقية ووقائية، تحافظ على أنظمة الحاسوب والشبكات وتطبيقات المؤسسة في مأمن من الهجمات عبر الإنترنت وعمليات خرق البيانات وهنالك أساليب متعددة لاختراق الأنظمة ومنها البرمجيات الخبيثة، الاختراقات. على هذا النحو فهي جزء مهم من برنامج الأمان الشامل وعليه تم استحداث أساليب جديدة في علوم التكنولوجيا للحماية ومن أهم الأساليب المتبعة هي التشفير والتي تعد الطريقة الأولى والأهم، وتليها الحماية بالبرمجيات ومن ثم الحماية بالسياسات السيبرانية (طالة، 2020)

وعلى ما تم ذكره أولت حكومة مملكة البحرين أهمية قصوى في هذا المجال كونه صمام الأمان حيث أقدمت على إنشاء المركز الوطني للأمن السيبراني بمرسوم ملكي رقم (65) لسنة 2017، وقامت بتجهيزه بأحدث المعدات مع مراعاة تحديثها بما يتناسب مع التطور التكنولوجي، وفي هذا الصدد سيتم إجراء هذه الدراسة لتسليط الضوء على جهود مملكة البحرين في مواجهة المخاطر السيبرانية في المؤسسات الحكومية.

مشكلة البحث

إن الدول التي لا تمتلك التكنولوجيا السيبرانية المحصنة أمنياً سيصبح فضاءها السيبراني عرضة للمخاطر السيبرانية من التلاعب والاختراق والقرصنة والتخريب وبينت التقرير الصادر من هيئة المعلومات والحكومة الإلكترونية لمملكة البحرين (2023) أن مملكة البحرين تتعرض للهجمات السيبرانية ما نسبته 70 % من الهجمات الإلكترونية المستهدفة للجهات الحكومية عبر رسائل تصيد البريد الإلكتروني، وإشارة الإحصائيات كذلك إلى رصد ما يقارب 50 مليون محاولة استغلال لثغرات أمنية، وبالتالي فإن مشكلة البحث تتمحور في تحديد جهود مملكة البحرين في مواجهة المخاطر السيبرانية؟

وينتفع من التساؤل الرئيس ، عدة أسئلة فرعية:

1. ماهي المخاطر السيبرانية التي يمكن استغلالها في مهاجمة مملكة البحرين في مجال المخاطر السيبرانية؟
- 2- هل هناك اختصاص لإدارة المخاطر السيبرانية في مملكة البحرين؟
- 3- ما هو الدور الذي يلعبه الأمن السيبراني ومدى الاستفادة منه في مملكة البحرين؟

أهداف البحث

- التعرف على واقع المخاطر السيبرانية في مملكة البحرين.
- معرفة العقبات التي تواجه مملكة البحرين في المخاطر السيبرانية.
- دراسة الاتجاهات التي يلعبها الأمن السيبراني ومدى الاستفادة منها في مملكة البحرين.

فروض البحث

- توجد علاقة دالة بين المخاطر السيبرانية (تحديد المخاطر، تحليل المخاطر، تقييم المخاطر، الاستجابة للمخاطر، التحكم بالنشاطات، المراقبة والمتابعة) في مملكة البحرين.

وينبثق عنها الفروض الفرعية التالية:

- توجد علاقة دالة بين تحديد المخاطر في المؤسسات الحكومية بمملكة البحرين.
- توجد علاقة دالة بين تحليل المخاطر في المؤسسات الحكومية بمملكة البحرين.
- توجد علاقة دالة بين تقييم المخاطر في المؤسسات الحكومية بمملكة البحرين.
- توجد علاقة دالة بين الاستجابة للمخاطر في المؤسسات الحكومية بمملكة البحرين.
- توجد علاقة دالة بين التحكم بالنشاطات في المؤسسات الحكومية بمملكة البحرين.
- توجد علاقة دالة بين المراقبة والمتابعة في المؤسسات الحكومية بمملكة البحرين.

أهمية البحث

- تكمن أهمية البحث في مملكة البحرين والتي تعتبر من أهم الدول في استخدام التكنولوجيا والمعاملات الحكومية والخاصة على مستوى العالم.
- تنبع أهمية الدراسة كونها تبحث في أحد المواضيع الحديثة وهو إدارة المخاطر السيبرانية في المؤسسات الحكومية.
- التوصل إلى أهم النتائج التي يمكن أن تشكل مرجعاً علمياً وعملياً، يفيد أصحاب القرار في وضع الخطط والإجراءات والتي يمكن أن تسهم في إدارة المخاطر السيبرانية في المؤسسات الحكومية.

مصطلحات البحث

- الأمن السيبراني: يُعرف بأنه: “أمن الشبكات والأنظمة المعلوماتية، والبيانات والأجهزة المتصلة بالإنترنت، فهو المجال الذي يتعلق بإجراءات ومقاييس، ومعايير الحماية المفروض اتخاذها أو الالتزام بها لمواجهة التهديدات ومنع التعديات أو على الأقل الحد من آثارها” (جبور، 2016).
- المخاطر السيبرانية: تُعرف على أنها المخاطر التشغيلية لأصول المعلومات والتقنية التي تؤثر على سرية، أو توافر، أو سلامة المعلومات، أو أنظمة المعلومات (جبور، 2016)

تعريف المخاطر السيبرانية في اللغة والاصطلاح

1.2 تاريخ المخاطر السيبرانية ومفهومها:

في عام 1969م أطلقت وزارة الدفاع الأمريكية مشروعاً يعرف باسم (ARPANET) وهو أول شبكة تحويلية تم تطويرها بتوصيل أجهزة الحاسوب الموجودة في معاهد البحوث والجامعات وكان الهدف الرئيسي من هذه الشبكة تبادل المعلومات والبيانات بين الأجهزة المختلفة. مع مرور الوقت توسعت وانضمت إليها شبكات أخرى مماثلة، وتطورت لتصبح الشبكة تعرف الآن بشبكة الإنترنت. وفي عام 1983م تم تبني نظام للاتصال يعرف ببروتوكول الإنترنت (IP) الذي يعتبر أساس عمل الإنترنت حتى اليوم. وهو ما مهد لولادة علم جديد مارس في بادئ الأمر حتى وصل لصورته الحالية ويتمثل في أفراد ومؤسسات وجهات خارجية والذين هم يمتلكون مهارات تقنية متقدمة في مجال الحوسبة والأنظمة الالكترونية ويستخدمون هذه المهارات لاكتشاف واختبار امن الأنظمة والشبكات ويمتازون بقدراتهم على فهم عمل الأنظمة التكنولوجية واكتشاف الثغرات والضعف فيها، سواء للتحسين وتعزيز الأمان أو لاستغلال هذه الثغرات بأغراض غير قانونية وهم القراصنة (طالة، 2022) ويعد مفهوم المخاطر مفهوماً رئيسياً في الصراع السيبراني، وذلك بسبب طبيعة الفضاء السيبراني العابر للدول، والتي لا تعترف بالسيادة الوطنية و بالحدود الجغرافية، فالهجمات السيبرانية يمكن تنظيمها بصورة تمر بالأقاليم الجغرافية لعدد كبير من الدول بما فيها الدولة المستهدفة بالأساس، حيث تلجأ الدول عادة في صراعاتها السيبرانية أو حتى الفاعلين من غير

الدول من قرصنة المعلومات للسيطرة على عدد كبير من أجهزة الكمبيوتر وكل جهاز متصل بالإنترنت في عدد كبير من الدول حول العالم بهدف تحقيق الخداع والتضليل وصعوبة تعقب مصدر الهجمة الرئيسية (عجاج، 2017)

وتعرف السبيرانية في اللغة وهي مأخوذة من كلمة (سير) وتعني صفة آلي شيء مرتبط بثقافة الحواسيب أو تقنية المعلومات أو الواقع الافتراضي، فالسبيرانية تعني فضاء الإنترنت وهي كلمة مشتقة من الكلمة اليونانية Sybernetes، والتي وردت بداية في مؤلفات الخيال العلمي وكان يقصد بها قيادة ربان السفينة (فراس، 2011).

2.2 مظاهر المخاطر السبيرانية في مملكة البحرين

أولاً: اختراق الأنظمة

حيث يتم استخدام تقنيات مختلفة لتنفيذ اختراق الأنظمة من خلال التحايل على الأنظمة المعلوماتية، ومن أخطر هذه البرامج "برنامج حصان طروادة" وهو عبارة عن شفرة أو برنامج صغير مختبئ في برنامج أكبر، حيث تكون مهمته إطلاق فيروس يقوم بإرسال البيانات عن الثغرات الموجودة في النظام وإرسال كلمة المرور السرية الخاصة بالهدف.

وتتسبب هذه النوعية من الاختراقات بخسائر كبيرة للمؤسسات والشركات المتمثلة في الخسائر المادية والخسائر في النظم، بحيث يقوم المجرم باختراق أنظمة الشبكات الخاصة بالمؤسسات والشركات والحصول على معلومات قيمة وخاصة بأنظمة الشركات (عجاج، 2017).

ثانياً: تدمير الأنظمة

يكون هذا النوع من التدمير باستخدام الطرق الشائعة وهي الفيروسات الإلكترونية والتي تنتشر في النظام وتسبب الفوضى والتدمير، ويتسبب ذلك في العديد من الخسائر المرتبطة بالملفات المدمرة ومدى أهميتها في إدارة وتنظيم الشركات والمؤسسات.

ومن أشهر هذه البرامج برنامج "ستاكس نت" والذي يقوم بمهاجمة أنظمة التحكم الصناعي المستخدمة على نطاق واسع في المنشآت الهامة مثل خطوط نقل النفط ومحطات توليد الكهرباء وغيرها من المنشآت الإستراتيجية الحساسة حيث تقوم بالانتقال بين الأجهزة عبر أجهزة USB مستغلة إحدى نقاط الضعف في برنامج التشغيل ويندوز (أبو عامود، 2014).

ثالثاً: الجرائم المالية

تقع الجرائم المالية بهدف الاستيلاء على حسابات البنوك من خلال اختراق الحسابات البنكية والحسابات المتعلقة بمؤسسات الدولة وغيرها من المؤسسات الخاصة، كما يتم أيضاً سرقة البطاقات الائتمانية، ومن ثم الاستيلاء عليها وسرقة ما بها من أموال، حيث واكب التطور الهائل في استخدام بطاقات الدفع الإلكتروني والتنوع في أنواع المشتريات والخدمات التي يمكن الحصول عليها إقليمياً ودولياً تنوع في أساليب وطرق التلاعب والتحايل في استخدام البطاقات مما يمثل تهديداً مباشراً وفورياً وسريعاً للاقتصاد العالمي والمحلي ولحقوق الأفراد بغض النظر عن مواقعهم في العالم (أبو عامود، 2014).

رابعاً: التهديدات السبيرانية بالحرمان من الخدمة

إن الهدف الرئيسي من هجمات الحرمان من الخدمة هو إجبار النظام الإلكتروني المستهدف على الاستجابة لعدد كبير من الطلبات والأوامر الخدمية بشكل يفوق قدرته، مما يعوقه عن تقديم الخدمات المطلوب منه تقديمها، غير أن هذه الهجمات التقليدية قد لا تستطيع إحداث تأثير كبير في الأنظمة أو المواقع المجهزة للاستجابة لكم ضخم من الأوامر مما يستدعي شكلاً أكثر تعقيداً من هذه الهجمات وهو ما يعرف بهجمات الحرمان من الخدمة الموزعة (طالة، 2020).

أسباب تبني مملكة البحرين لمواجهة التهديدات السبيرانية

أولاً: الفضاء السبيرياني يمثل أحد مصادر التهديد:

أصبح الفضاء الإلكتروني وسيطاً ووسيلة معاً لشن الهجوم وتنفيذ الأعمال العدائية بين الخصوم، وظهور استخدام لأسلحة جديدة ترتبط بالفضاء السبيرياني في مجال الحماية الهجوم وتطوير القدرات داخل الفضاء السبيرياني لشن عمليات الهجوم على أنظمة الحاسبات التابعة للدول الأخرى، وانعكس

ذلك بالتهديد بعسكرة الفضاء السيبراني، وجعله جزءاً هاماً من تكتيكات الحروب على خلاف طبيعته المدنية السلمية وأهميته في عمل البنية التحتية الكونية للمعلومات . (الجور، 2016)

ثانياً: اعتماد مملكة البحرين على تكنولوجيا الاتصالات

تعتبر مملكة البحرين من أوائل الحكومات العربية تحولاً إلى الحكومة الإلكترونية إعتباراً من أكتوبر 2001م حيث تحولت الخدمات العامة للإدارات الحكومية بالمملكة من شكلها الروتيني التقليدي إلى أشكال جديدة إلكترونية بواسطة الحاسب عبر شبكة الإنترنت، كما تم إدخال الحاسبات في التطبيقات المختلفة واستخدامها في معالجة البيانات والمعلومات في المنظمات والمصالح الحكومية. (الموقع الرسمي للمركز السيبراني، 2025)

ثالثاً: زيادة الهجمات السيبرانية

إن مملكة البحرين كإحدى دول مجلس التعاون الخليجي وكمركز للتمويل والطاقة والعقارات وتجارة البيع التجزئة والسياحة والطيران قد جعلتها في مقدمة الوجهات المستهدفة بشكل واسع من قبل مجرمي الإنترنت، كما إن قدرات الاتصال عالية المستوى في المنطقة تجعلها بيئة خصبة للهجمات السيبرانية، ووفقاً لتقرير شركة "إن جي إن" العالمية لأنظمة المعلومات المتكاملة ومقرها البحرين أن 60% من المؤسسات في البحرين والمنطقة تعرضت لهجمات سيبرانية هدفت بشكل أساسي إلى سرقة بياناتها الحساسة، إضافة إلى الابتزاز والتخريب، وبما يؤثر بدرجات متفاوتة من الخطورة على سير العمل في تلك المؤسسات وأدائها وسرية وخصوصية بياناتها وبيانات عملائها، فيما أشار 51% منها إلى أن عدم وجود إطار عمل مناسب في تلك الجهات للحماية يساعد الأخطار السيبرانية. (شركة إن جي إن، 2021).

رابعاً: الاستعمال الواسع لشبكات التواصل الاجتماعي

حيث ساهم انتشار شبكات التواصل الاجتماعي بشكل كبير في ظهور أنواع متعددة من الجرائم الإلكترونية مثل القذف، التحرش الجنسي، استغلال القصر، حيث أصبحت شبكات التواصل الاجتماعي الوسيلة الوحيدة التي فرضت سيطرتها على جميع المجتمعات، وأصبح مستخدموها يتجاوزون المليارات، وأصبحت وسيلة شديدة التأثير في المجتمعات والأسر العربية بشكل كبير وخطير، ذلك أنها أصبحت تستخدم أساليب جذب لا حصر لها، فهي تستهوي متابعيها من جميع الفئات والأعمار، وهو ما يجعلها سلاحاً ذا حدين . (الموقع الرسمي للمركز السيبراني، 2025)

خامساً: غياب التنسيق بين الدول والحكومات

حيث أن الجرائم التي ترتكب من خلال الفضاء السيبراني هي جرائم عابرة للحدود والقارات، وهو ما يعني أن مرتكبيها يمكنهم النفاذ إلى أنظمة الحاسوب في أحد الدول، ويتم التلاعب واختراق البيانات في بلد آخر، وتسجل النتائج في بلد ثالث، فضلاً عن قدرة المجرم الإلكتروني على إخفاء هويته ونقل الموارد من خلال قنوات موجودة في بلدان مختلفة (الموقع الرسمي للمركز السيبراني، 2025).

إجراءات البحث

مجتمع وعينة البحث

تكونت عينة الدراسة من (414) مفردة، منهم (63) موظفاً وموظفة في الإدارة العليا بنسبة (15.2%) من عينة الدراسة، و(351) موظفاً وموظفة في الإدارة الوسطى بنسبة (84.8%) من عينة الدراسة، وهي نسب مطابقة لنسبة الإدارات الوسطى والعليا في مجتمع الدراسة، حيث تم اختيار العينة من الإدارات العليا والوسطى في وزارات مملكة البحرين من خلال أسلوب العينة الطبقية التناسبية حتى تكون العينة ممثلة للمجتمع، بحيث تكون نسب الإدارات في مجتمع الدراسة مطابقة لنسبتها في عينة الدراسة. وقد تم اختيار هذا العدد بناءً على جدول مورغان، والذي يوضح أن أدنى عدد مطلوب حتى تكون العينة ممثلة للمجتمع (335) فرداً، حيث تكون العينة ممثلة للمجتمع البالغ عدده (2680) موظفاً وموظفة.

إجراءات الصدق والثبات:

تكونت عينة استطلاعية ضمت (200) موظفًا في الوزارات البحرينية، بغرض إجراء اختبار الصدق والثبات للاستبانة، أما عينة البحث الأساسية فهي طبقية نسبية من (414) موظفًا وموظفة باختلاف درجاتهم الوظيفية بنسبة (15.5%) تقريبًا من مجتمع الدراسة.

أسلوب الدراسة:

طبقت الدراسة المنهج الوصفي التحليلي وذلك لكونه منهجاً يساعد على التحليل الشامل والعميق للمشكلة قيد الدراسة ولكونه المنهج الذي يمتاز بالوصف التفصيلي الدقيق للمعلومات ذات العلاقة ويصنفها تصنيفاً شاملاً وباعتباره المنهج المناسب القادر على وصف الظواهر الإنسانية وصفاً دقيقاً، فضلاً عن سماته من حيث إمكانياته في الجمع بين أكثر من أسلوب بحثي في آن واحد، إذ يتمثل بالملاحظة والاستفسار والإجابة التي تؤدي للوصول إلى المعلومات بشكل مباشر (محبوب، 2002).

أداة الدراسة:

تمثلت أداة البحث المستخدمة في الدراسة الحالية باستمارة الاستقصاء. وقد تم إعداد هذه الاستمارة الخاصة بالدراسة للحصول على البيانات الخاصة بالجانب العملي والاعتماد على المقاييس المتوفرة في المتراكم المعرفي لمتغيرات الدراسة حيثما تسنى إيجادها التي تضم مقاييس خاصة في ضوء المؤشرات الواردة في الدراسات الميدانية.

وقد تم استخدام مقياس ليكرت Likert الخماسي وكانت حركة المقياس كالآتي: (غير موافق بشدة، غير موافق، محايد، موافق، موافق بشدة) وقد أعطيت درجات للإجابات الخمس السابقة الذكر على التوالي (1، 2، 3، 4، 5).

جدول (1)

درجات إجابة عينة الدراسة على عبارات ومفردات الاستبانة

5	4	3	2	1
موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة

خطوات إجراءات الدراسة:

- 1- إعداد الإطار العام للدراسة من حيث مشكلة الدراسة وتساؤلاته وأهميته وأهدافه وفرضياته والتعريفات الإجرائية للدراسة وهيكلية البحث.
- 2- إعداد الإطار النظري للبحث والذي اشتمل متغيرات البحث.
- 3- إعداد منهجية البحث من حيث تحديد مجتمع وعينة البحث، وكذلك تصميم أداة البحث المتمثلة في قائمة استقصاء لجمع البيانات وتطبيق أداة البحث على عينة البحث محل الدراسة، وإجراء اختبار الصدق والثبات لها.
- 4- إجراء التحليل الإحصائي للبيانات والتحقق من فرضيات البحث وعرض نتائج البحث ومناقشتها من خلال مقارنتها مع نتائج الدراسات السابقة.
- 5- تقديم بعض التوصيات في ضوء النتائج التي توصلت إليها الدراسة

الأساليب الإحصائية:

1- الإحصاء الوصفي:

المتوسطات الحسابية Means لتحديد مستوى الاستجابة لمتغيرات الدراسة.

الانحراف المعياري Standard Deviation لمعرفة مدى تشتت قيم الاستجابة عن أوساطها الحسابية.

2- الإحصاء التحليلي:

أ) اختبار كرونباخ ألفا: لاختبار قياس مستوى اتساق أسئلة الاستبانة المستخدمة في جمع البيانات وقياس ثبات مقياس المتغيرات التي اشتمل عليها البحث.

- ب) استخراج معامل ارتباط بيرسون (Pearson Correlation Coefficient (PCC) لقياس درجة الارتباط للتحقق من مستوى العلاقة الارتباطية بين أبعاد المتغير المستقل والمتغير التابع.
- ج) تحليل الانحدار المتعدد (Multiple Regression Analysis (MRA) للتحقق من وجود تأثير من عدمه لأبعاد المتغير المستقل على المتغير التابع التوجه الاستراتيجي، ومعامل التحديد (R^2) المعدل ومعامل بيتا B.
- د) تحليل الانحدار البسيط ويكون الغرض من استخدامه هو دراسة وتحليل أثر المتغير المستقل على المتغير التابع.
- هـ) حساب الدرجة التائية: t-test للتحقق من دلالة الفروق بين متوسطات درجات المجموعات المستقلة للمتغيرات الديمغرافية المتعلقة بمتغير الجنس لأنه يتكون من مستويين: ذكر، أنثى.
- و) اختبار تحليل التباين الأحادي Analysis of Variance ANOVA: للتحقق من دلالة الفروق بين متوسطات درجات المجموعات للمتغيرات الديمغرافية التي تتكون من أكثر من مستويين مثل المستوى التعليمي والعمر.
- ز) مستوى الدلالة المعنوية (الاحتمالية): في حالة كون قيمة مستوى الدلالة المعنوية ($p \leq 0.01$) فيرمز لهذه الحالة بعلامة (***) وفي حالة كون قيمة مستوى الدلالة المعنوية ($p \leq 0.05$) فقد وضعت العلامة (*) للدلالة على ذلك، وسيتم اعتماد هذه العلامات للتعبير عن مستوى الدلالة، عند عرض النتائج وتحليلها وتفسيرها لاحقاً.
- ثبات الاتساق الداخلي:

جدول (2)

مؤشرات ثبات الاتساق الداخلي لأبعاد أداة الدراسة

الرقم	الأبعاد	قيم ثبات كورنباخ-الفا
1	البعد الأول: الوعي بالمخاطر	0.91
2	البعد الثاني: تحديد المخاطر	0.85
3	البعد الثالث: تحليل المخاطر	0.90
4	البعد الرابع: تقييم المخاطر	0.91
5	البعد الخامس: الاستجابة للمخاطر	0.88
6	البعد السادس: التحكم بالنشاطات	0.87
7	البعد السابع: المراقبة والمتابعة	0.92
	الدرجة الكلية	0.94

نتائج أسئلة الدراسة:

جدول (3)

المتوسطات الحسابية والانحرافات المعيارية والأهمية النسبية لمستوى إدارة المخاطر السيبرانية في

الرقم	الفقرات	المتوسطات الحسابية	الانحرافات المعيارية	الأهمية النسبية	الترتيب
1	البعد الأول: الوعي بالمخاطر	4.123	0.478	82.5%	1
7	البعد السابع: المراقبة والمتابعة	3.593	0.790	71.9%	2
5	البعد الخامس: الاستجابة للمخاطر	3.579	0.814	71.6%	3
6	البعد السادس: التحكم بالنشاطات	3.537	0.745	70.7%	4
3	البعد الثالث: تحليل المخاطر	3.465	0.699	69.3%	5
4	البعد الرابع: تقييم المخاطر	3.367	0.935	67.3%	6
2	البعد الثاني: تحديد المخاطر	3.221	0.785	64.4%	7
	الدرجة الكلية	3.555	0.628	71.1%	

- ما مستوى الوعي بالمخاطر السيبرانية في المؤسسات الحكومية في مملكة البحرين ؟

جدول (4)

المتوسطات الحسابية والانحرافات المعيارية والأهمية النسبية لمستوى الوعي بالمخاطر السيبرانية في

الرقم	الفقرات	المتوسطات الحسابية	الانحرافات المعيارية	الأهمية النسبية	الترتيب
1	هل تعتبر نفسك على دراية بمفاهيم الأمن السيبراني؟	3.747	0.901	74.9%	4
2	هل تقوم بالنسخ الاحتياطي للملفات الهامة بشكل منتظم؟	4.087	0.809	81.7%	3
3	هل تعتقد أنه يجب زيادة التوعية بمسائل الأمن السيبراني في المجتمع؟	4.867	0.341	97.3%	1
4	هل تعتقد أنه يجب تكثيف التعاون الدولي لمكافحة جرائم الإنترنت والتهديد السيبراني؟	4.787	0.485	95.7%	2
5	هل يتم تقديم دورات وورش عمل بشكل دوري بشأن الأمن السيبراني؟	3.130	1.174	62.6%	5
	الكلية	4.123	0.478	82.5%	

- ما مستوى تحديد المخاطر السيبرانية في شئون الجنسية والجوازات والإقامة بمملكة البحرين؟

جدول (5)

المتوسطات الحسابية والانحرافات المعيارية والأهمية النسبية لمستوى تحديد المخاطر السيبرانية في شئون الجنسية والجوازات والإقامة بمملكة البحرين

الرقم	الفقرات	المتوسطات الحسابية	الانحرافات المعيارية	الأهمية النسبية	الترتيب
1	تقوم المؤسسات الحكومية بالكشف والتعرف إلى المخاطر السيبرانية وتسجيلها.	3.293	0.918	65.9%	1
2	تعتمد المؤسسات الحكومية على أساليب علمية في تحديد المخاطر السيبرانية.	3.203	0.855	64.1%	4
3	تمتلك المؤسسات قائمة بالمخاطر السيبرانية المحتملة التي تهدد بيئتها الداخلية والخارجية.	3.230	0.891	64.6%	2
4	لدى المؤسسات الحكومية فريق من الخبراء متخصص في تحديد المخاطر السيبرانية.	3.157	0.950	63.1%	5
5	يشارك فريق عمل المخاطر مع المسؤولين بالمؤسسات الحكومية في تحديد المخاطر السيبرانية.	3.220	0.921	64.4%	3
	الكلية	3.221	0.785	64.4%	

ما مستوى تحليل المخاطر السيبرانية في المؤسسات الحكومية في مملكة البحرين؟

جدول (6)

المتوسطات الحسابية والانحرافات المعيارية والأهمية النسبية لمستوى تحليل المخاطر السيبرانية في المؤسسات الحكومية في مملكة البحرين

الرقم	الفقرات	المتوسطات الحسابية	الانحرافات المعيارية	الأهمية النسبية	الترتيب
1	تستعين المؤسسات الحكومية بالخبراء في مجال الأمن السيبراني لتحليل المخاطر.	3.737	0.704	74.7%	1
2	تعمل المؤسسات الحكومية على تصنيف المخاطر السيبرانية وفقاً لمصادرها وطبيعتها.	3.390	0.804	67.8%	4
3	يتم تحليل المخاطر السيبرانية التي تهدد بيئة العمل على أساس كمي ونوعي.	3.437	0.674	68.7%	2
4	تقوم المؤسسات الحكومية بقياس أي ثغرة أمنية من خلال قياس احتمالية وقوع الخطر ودرجة تأثيره.	3.327	0.736	66.5%	5
5	تضع المؤسسات الحكومية مقاييس دقيقة لكل من احتمال وقوع الخطر وتأثيره لتحديد مستوى وأهمية الخطر.	3.433	0.974	68.7%	3
	الكلية	3.465	0.699	69.3%	

ما مستوى تقييم المخاطر السيبرانية في المؤسسات الحكومية في مملكة البحرين؟

جدول (7)

المتوسطات الحسابية والانحرافات المعيارية والأهمية النسبية لمستوى تقييم المخاطر السيبرانية في المؤسسات الحكومية في مملكة البحرين

الرقم	الفقرات	المتوسطات الحسابية	الانحرافات المعيارية	الأهمية النسبية	الترتيب
1	تعتمد المؤسسات الحكومية على نتائج عملية تحليل المخاطر في تقييم المخاطر السيبرانية.	3.297	0.912	65.9%	4
2	تجرى المؤسسات الحكومية عمليات تقييم منظمة لبرامجها وعملياتها بإداراتها المختلفة لتقيم بشكل فعال المخاطر السيبرانية.	3.313	1.019	66.3%	3
3	تقوم المؤسسات الحكومية بتحديد مستويات المخاطر السيبرانية وترتيبها وفقاً لاحتمالية حدوثها ودرجة تأثيرها.	3.263	1.057	65.3%	5
4	تحدد المؤسسات الحكومية أولويات المخاطر لكي يتخذ قرار بشأن معالجتها.	3.417	0.923	68.3%	2
5	هل يتم تحديث التدابير والإجراءات الاحترازية بشكل دوري في المؤسسات الحكومية	3.543	1.032	70.9%	1
	الكلية	3.367	0.935	67.3%	

- ما مستوى الاستجابة للمخاطر السيبرانية في المؤسسات الحكومية في مملكة البحرين ؟

جدول (8)

المتوسطات الحسابية والانحرافات المعيارية والأهمية النسبية لمستوى الاستجابة للمخاطر السيبرانية في المؤسسات الحكومية في مملكة البحرين

الرقم	الفقرات	المتوسطات الحسابية	الانحرافات المعيارية	الأهمية النسبية	الترتيب
1	تضع المؤسسات الحكومية استراتيجية محددة وسياسات تفصيلية للاستجابة للمخاطر السيبرانية.	3.537	0.878	70.7%	4
2	تقوم المؤسسات الحكومية بدراسة البدائل المحتملة لمواجهة المخاطر السيبرانية (تجنب، تحويل، تحكم، تحمل).	3.427	0.753	68.5%	5
3	تستخدم المؤسسات الحكومية وسائل تكنولوجية للتعامل مع المخاطر السيبرانية.	3.640	0.924	72.8%	2
4	تقوم المؤسسات الحكومية باتخاذ القرار المناسب في مواجهة المخاطر.	3.717	0.909	74.3%	1
5	تعتمد المؤسسات الحكومية خطة محددة لضمان استمرارية الأعمال حال حدوث الخطر.	3.577	0.990	71.5%	3
	الكلية	3.579	0.814	71.6%	

- ما مستوى التحكم بنشاطات إدارة المخاطر السيبرانية في المؤسسات الحكومية في مملكة البحرين؟

جدول (9)

المتوسطات الحسابية والانحرافات المعيارية والأهمية النسبية لمستوى التحكم بنشاطات إدارة المخاطر السيبرانية في المؤسسات الحكومية في مملكة البحرين

الرقم	الفقرات	المتوسطات الحسابية	الانحرافات المعيارية	الأهمية النسبية	الترتيب
1	تعمل المؤسسات الحكومية على السيطرة على الخطر لمنع أو التقليل من آثاره من خلال معرفة سمات ومظاهر الخطر.	3.680	0.913	73.6%	1
2	تمتلك المؤسسات الحكومية الأساليب المثلى للتحكم بالنشاطات من خلال التغذية الراجعة.	3.403	0.922	68.1%	4
3	تستخدم المؤسسات الحكومية السجلات والتقارير الدقيقة للتحكم بالنشاطات.	3.603	0.974	72.1%	3
4	تعمل المؤسسات الحكومية على تنفيذ خطط الاستجابة للمخاطر السيبرانية.	3.607	0.805	72.1%	2
5	لدى المؤسسات الحكومية الوسائل والأدوات اللازمة لتعقب المخاطر السيبرانية التي تم اكتشافها ومراقبة المخاطر المتبقية.	3.393	0.928	67.9%	5
	الكلية	3.537	0.745	70.7%	

ما مستوى مراقبة ومتابعة المخاطر السيبرانية في المؤسسات الحكومية في مملكة البحرين ؟

جدول (9)

المتوسطات الحسابية والانحرافات المعيارية والأهمية النسبية لمستوى مراقبة ومتابعة المخاطر السيبرانية في المؤسسات الحكومية في مملكة البحرين

الرقم	الفقرات	المتوسطات الحسابية	الانحرافات المعيارية	الأهمية النسبية	الترتيب
1	تقوم المؤسسات الحكومية بالمراقبة والمتابعة للتأكد من تحقيق الأهداف الاستراتيجية في مواجهة المخاطر السيبرانية.	3.603	0.985	72.1%	3
2	تعمل المؤسسات الحكومية في الرقابة وبشكل مستمر وذلك لمتابعة النتائج المتعلقة في المخاطر السيبرانية بشكل ديناميكي ومنظم.	3.597	1.019	71.9%	4
3	تقوم المؤسسات الحكومية في متابعة تنفيذ الإجراءات المتعلقة بالمخاطر السيبرانية.	3.697	0.730	73.9%	1
4	تعمل المؤسسات الحكومية على تسجيل المخاطر السيبرانية التي تواجهها بشكل دوري ليتسنى لها دراستها ووضع الخطط البديلة لها.	3.653	1.015	73.1%	2
5	تقوم المؤسسات الحكومية بمشاركة معلومات الأمن السيبراني في إطار مشترك مع دول الخليج.	3.417	0.879	68.3%	5
	الكلية	3.593	0.790	71.9%	

نتائج الفروض:

الفرض الأول: توجد علاقة ارتباطية دالة إحصائياً بين وعي العاملين بالمخاطر السيبرانية وقدرتها على إدارة هذه المخاطر. تم استخدام معامل الارتباط بيرسون:

جدول (10)

دلالة العلاقة الارتباطية بين وعي العاملين في قدرتها على إدارة هذه المخاطر

قيمة معامل الارتباط	عدد العينة	مستوى الدلالة
0.43(**)	335	0.01

* الارتباط دال إحصائياً عند $(\alpha = 0.05)$.

** الارتباط دال إحصائياً عند $(\alpha = 0.01)$.

الفرض الثاني: توجد علاقة ارتباطية دالة إحصائياً بين مستوى تحديد العاملين في للمخاطر السيبرانية وقدرتها على إدارة هذه المخاطر. تم استخدام معامل الارتباط بيرسون:

جدول (11)

دلالة العلاقة الارتباطية بين مستوى تحديد العاملين للمخاطر وقدرتها على إدارة هذه المخاطر

قيمة معامل الارتباط	عدد العينة	مستوى الدلالة
0.85(**)	335	0.01

* الارتباط دال إحصائياً عند $(\alpha = 0.05)$.

** الارتباط دال إحصائياً عند $(\alpha = 0.01)$.

الفرض الثالث: توجد علاقة ارتباطية دالة إحصائياً بين مستوى تحليل العاملين للمخاطر السيبرانية وقدرتها على إدارة هذه المخاطر. تم استخدام معامل الارتباط بيرسون:

جدول (12)

دلالة العلاقة الارتباطية بين مستوى تحليل العاملين للمخاطر وقدرتها على إدارة هذه المخاطر

قيمة معامل الارتباط	عدد العينة	مستوى الدلالة
0.88(**)	335	0.01

* الارتباط دال إحصائياً عند $(\alpha = 0.05)$.

** الارتباط دال إحصائياً عند $(\alpha = 0.01)$.

الفرض الرابع: توجد علاقة ارتباطية دالة إحصائياً بين مستوى تقييم العاملين في للمخاطر السيبرانية وقدرتها على إدارة هذه المخاطر. تم استخدام معامل الارتباط بيرسون:

جدول (13)

دلالة العلاقة الارتباطية بين مستوى تقييم العاملين للمخاطر وقدرتها على إدارة هذه المخاطر

قيمة معامل الارتباط	عدد العينة	مستوى الدلالة
0.90(**)	335	0.01

* الارتباط دال إحصائياً عند $(\alpha = 0.05)$.

** الارتباط دال إحصائياً عند $(\alpha = 0.01)$.

الفرض الخامس: توجد علاقة ارتباطية دالة إحصائياً بين الاستجابة للمخاطر لدى العاملين وقدرتها على إدارة المخاطر السيبرانية.
تم استخدام معامل الارتباط بيرسون:

جدول (14)

دلالة العلاقة الارتباطية بين الاستجابة للمخاطر لدى العاملين وقدرتها على إدارة المخاطر السيبرانية

قيمة معامل الارتباط	عدد العينة	مستوى الدلالة
0.89(**)	335	0.01

* الارتباط دال إحصائياً عند $(\alpha = 0.05)$.

** الارتباط دال إحصائياً عند $(\alpha = 0.01)$.

النتائج:

توصلت الدراسة للعديد من النتائج أهمها ما يلي:

- 1- جاءت إدارة المخاطر السيبرانية في المؤسسات الحكومية بمملكة البحرين بمستوى متوسط، وأن أعلى جوانب إدارة المخاطر السيبرانية في المؤسسات الحكومية هي الوعي بالمخاطر السيبرانية، تلاه المراقبة والمتابعة، ثم الاستجابة للمخاطر السيبرانية.
- 2- إن مستوى الوعي بالمخاطر السيبرانية في المؤسسات الحكومية جاء بدرجة كبيرة، وتبين أعلى جوانب الوعي بالمخاطر السيبرانية هي زيادة التوعية بمسائل الأمن السيبراني في المجتمع، تلاها تكثيف التعاون الدولي لمكافحة جرائم الإنترنت والتهديد السيبراني. كما أن مستوى تحديد المخاطر السيبرانية جاء بدرجة متوسطة، وكانت أعلى جوانب تحديد المخاطر السيبرانية هي قيام المؤسسات الحكومية بالكشف والتعرف إلى المخاطر السيبرانية وتسجيلها، تلاها امتلاك المؤسسات الحكومية قائمة بالمخاطر السيبرانية المحتملة التي تهدد بيئتها الداخلية والخارجية.
- 3- يتبين مستوى تحليل المخاطر السيبرانية في المؤسسات الحكومية جاء بدرجة متوسطة، واحتلت أعلى جوانب تحليل المخاطر السيبرانية هي استعانة المؤسسات الحكومية بالخبراء في مجال الأمن السيبراني لتحليل المخاطر، تلاها تحليل المخاطر السيبرانية التي تهدد بيئة العمل على أساس كمي ونوعي. ومستوى تقييم المخاطر السيبرانية في المؤسسات الحكومية بمملكة البحرين جاء بدرجة متوسطة، وكانت أعلى جوانب تقييم المخاطر السيبرانية هي تحديث التدابير والإجراءات الاحترازية بشكل دوري في المؤسسات الحكومية، تلاها تحديد المؤسسات الحكومية أولويات المخاطر لكي يتخذ قرار بشأن معالجتها.
- 4- تبين من النتائج أن الاستجابة للمخاطر السيبرانية جاء بدرجة متوسطة، وكانت أعلى جوانب الاستجابة للمخاطر السيبرانية هي قيام المؤسسات الحكومية باتخاذ القرار المناسب في مواجهة المخاطر، كما تستخدم المؤسسات وسائل تكنولوجية للتعامل مع المخاطر السيبرانية. حيث كان مستوى التحكم بنشاطات إدارة المخاطر السيبرانية في المؤسسات الحكومية البحرين جاء بدرجة متوسطة، وكانت أعلى جوانب التحكم بنشاطات إدارة المخاطر السيبرانية هي عمل المؤسسات الحكومية على السيطرة على الخطر لمنع أو التقليل من آثاره من خلال معرفة سمات ومظاهر الخطر، تلاها عمل المؤسسات الحكومية على تنفيذ خطط الاستجابة للمخاطر السيبرانية.
- 5- أوضح أفراد العينة أن مراقبة ومتابعة المخاطر السيبرانية جاء بدرجة متوسطة، و أعلى جوانب مراقبة ومتابعة المخاطر السيبرانية هي المؤسسات الحكومية في متابعة تنفيذ الإجراءات المتعلقة بالمخاطر السيبرانية، تلاها عمل المؤسسات الحكومية على تسجيل المخاطر السيبرانية التي تواجهها بشكل دوري ليتسنى لها دراستها ووضع الخطط البديلة لها.
- 6- وجود علاقة ارتباطية موجبة ومتوسطة القوة ودالة إحصائياً بين وعي العاملين بالمخاطر السيبرانية وقدرتها على إدارة هذه المخاطر. ووجود علاقة ارتباطية موجبة ومرتفعة ودالة إحصائياً بين مستوى تحديد العاملين في المؤسسات الحكومية للمخاطر وقدرتها على إدارة هذه المخاطر.

- 7- وجود علاقة ارتباطية موجبة ومرتفعة ودالة إحصائياً بين مستوى تحليل العاملين للمخاطر وقدرتها على إدارة هذه المخاطر. ووجود علاقة ارتباطية موجبة ومرتفعة ودالة إحصائياً بين مستوى تقييم العاملين في المؤسسات الحكومية للمخاطر وقدرتها على إدارة هذه المخاطر.
- 8- وجود علاقة ارتباطية موجبة ومرتفعة ودالة إحصائياً بين الاستجابة للمخاطر لدى العاملين في المؤسسات الحكومية بمملكة البحرين وقدرتها على إدارة المخاطر السيبرانية، فكلما زاد مستوى وعي العاملين في المؤسسات الحكومية بمملكة البحرين بالمخاطر السيبرانية، زادت قدرتها على إدارة هذه المخاطر.
- التوصيات:**

تقدم الدراسة التوصيات التالية، وذلك وفي ضوء ما توصلت إليه من نتائج:

1. تبني مبادرات بالاشتراك مع مؤسسات المجتمع المدني ترسيخ الثقافة والوعي من خلال الندوات الثقافية والبرامج التدريبية في المؤسسات التعليمية والقطاعات الحيوية في مملكة البحرين.
2. العمل على بناء الكوادر الوطنية في مجالات تكنولوجيا المعلومات والأمن السيبراني من خلال تشجيع الابتكارات العلمية في مجال الأمن السيبراني.
3. أهمية متابعة تحديث المنظومة التشريعية المعنية بالأمن السيبراني وفقاً للمستجدات في تكنولوجيا الأمن السيبراني والتي تشهد تطورات متلاحقة.
4. زيادة التعاون والتنسيق بين المركز الوطني للأمن السيبراني في مملكة البحرين مع المراكز المماثلة في دول مجلس التعاون الخليجي لتبادل المعلومات والزيارات.
5. العمل على ترسيخ نهج استشراف المستقبل في حماية الأمن السيبراني بوصفه يمثل إحدى المداخل العلمية للتعامل مع مصادر التهديد الأمني بمستوياتها ونوعياتها المختلفة، لتعزيز الحماية ورفع الجاهزية الأمنية.
6. تحديث وتطوير الهيكل التنظيمي للمؤسسات الحكومية في مملكة البحرين باستحداث إدارة معنية بتحديد مخاطر الأمن السيبراني بهدف زيادة وعي العاملين والتصدي للهجمات السيبرانية.
7. العمل على الاستثمار في دعم إجراء الدراسات والبحوث المتعمقة حول الجرائم السيبرانية بصفة عامة والجرائم الإرهابية بصفة خاصة وصورها وآثارها ورفع التوصيات اللازمة إلى الإدارة العليا بالمؤسسات الحكومية في مملكة البحرين.
8. ضرورة إنشاء مختبر وطني للأدلة الجنائية الرقمية وذلك للإسراع في الكشف عن الجرائم السيبرانية العابرة للحدود والماسة بالأمن الوطني.
9. أهمية وضع استراتيجية وطنية متكاملة متعلقة بالمخاطر السيبرانية وبكيفية مواجهة التهديدات بما يتناسب مع المتغيرات السريعة.
10. ضرورة دعم وتشجيع وتمويل البحث العلمي في موضوعات المخاطر السيبرانية والاستفادة من النتائج.

المراجع والمصادر:

- أبو عامود، محمد (2014) استشراف المستقبل وأهميته للأجهزة الأمنية، مطبوعات الأكاديمية الملكية للشرطة، مملكة البحرين.
- الجبور، منى (2016)، السيبرانية هاجس العصر، المركز العربي للبحوث القانونية والفضائية، بيروت.
- درار، نسيم (2017) الأمن المعلوماتي وسبل المواجهة مخاطر في التعامل الإلكتروني، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق قسم القانون، جامعة أبو بكر بلقايد، الجزائر.
- سعيد، رؤى (2022)، الحماية الجنائية للبيانات الشخصية الرقمية - دراسة مقارنة، رسالة ماجستير، جامعة العلوم التطبيقية، مملكة البحرين.
- طالة، لامية (2020)، "التهديدات والجرائم السيبرانية وتأثيرها على الأمن القومي للدول واستراتيجيات مكافحتها"، مجلة معالم للدراسات القانونية والسياسية، المجلد 4، العدد 2، كلية علوم الإعلام والاتصال، جامعة الجزائر 3، الجزائر.
- عجّاح، خليفة (2017)، مكافحة جريمة الاحتيال الإلكتروني، رسالة ماجستير، الأكاديمية الملكية للشرطة، مملكة البحرين.
- فراس، طحان (2011) الإرهاب الإلكتروني وسبل مكافحته، مجلة جامعة دمشق للعلوم الاقتصادية والقانونية، المجلد 28، العدد الثاني.

- فرحات، علاء الدين (2021)، "من الردع النووي إلى الردع السيبراني، دراسة مدى تحقق الردع في الفضاء السيبراني"، مجلة الفكر، المدرسة الوطنية للعلوم العسكرية، المجلد 16، العدد 1، الجزائر.
- كلاع، شريفة (2022) الأمن السيبراني وتحديات الجوسسة والاختراقات الإلكترونية للدول عبر الفضاء السيبراني، مجلة الحقوق والعلوم الإنسانية، المجلد (15)، العدد (1) جامعة الجزائر، الجزائر.
- الموقع الرسمي لهيئة الإفتاء والتشريع القانوني في مملكة البحرين ([/https://www.lloc.gov.bh](https://www.lloc.gov.bh))
- ندوة عن بُعد بعنوان، "تطور التهديدات السيبرانية في البحرين"، 28 مارس، شركة إن جي إن بالتعاون مع شركة "جروب أي بي" العالمية، مملكة البحرين، 2021م.

References :

- Abū 'Āmūd, Muḥammad (2014) istishrāf al-mustaqbal wa-ahammīyatuhu lil-Ajhizah al-Amnīyah, Maṭbū'āt al-Akādīmīyah al-Malakīyah lil-shurṭah, Mamlakat al-Baḥrayn.
- al-Jubūr, Muná (2016), al-sybrānyh Hājis al-'aṣr, al-Markaz al-'Arabī lil-Buḥūth al-qānūnīyah wālfda'yh, Bayrūt.
- Dirār, Nasīmah (2017) al-amn al-ma'lūmātī wa-subul al-muwājahah mkhātrh fī al-ta'āmul al-iliktrūnī, dirāsah muqāranah, Risālat Duktūrah, Kullīyat al-Ḥuqūq Qism al-qānūn, Jāmi'at Abū Bakr Balqāyid, al-Jazā'ir.
- Sa'īd, Ru'ā (2022), al-Ḥimāyah al-jinā'īyah llbyānāt al-shakhṣīyah al-raqmīyah – dirāsah muqāranah, Risālat mājistīr, Jāmi'at al-'Ulūm al-taṭbīqīyah, Mamlakat al-Baḥrayn.
- ṭāh, Lāmīyah (2020), "al-tahdīdāt wa-al-jarā'im al-sybrānyh wa-ta'thīruhā 'alā al-amn al-Qawmī lil-duwal wa-istīrātijīyāt mukāfahatihā", Majallat Ma'ālim lil-Dirāsāt al-qānūnīyah wa-al-siyāsīyah, almjld4, al'dd2, Kullīyat 'ulūm al-I'lām wa-al-Ittiṣāl, Jāmi'at aljzā'r3, al-Jazā'ir.
- 'jāh, Khalīfah (2017), Mukāfahat Jarīmat al-iḥtiyāl al-iliktrūnī, Risālat mājistīr, al-Akādīmīyah al-Malakīyah lil-shurṭah, Mamlakat al-Baḥrayn.
- Firās, Ṭaḥḥān (2011) al-irhāb al-iliktrūnī wa-subul mukāfahatih, Majallat Jāmi'at Dimashq lil-'Ulūm al-iqtisādīyah wa-al-qānūnīyah, al-mujallad 28, al-'adad al-Thānī.
- Farahāt, 'Alā' al-Dīn (2021), "min al-rad' al-Nawawī ilā al-rad' al-sybrāny, dirāsah li-madā taḥqīq al-rad' fī al-fadā' al-sybrāny", Majallat al-Fikr, al-Madrasah al-Waṭanīyah lil-'Ulūm al-'askarīyah, al-mujallad 16, al'dd1, al-Jazā'ir.
- klā', Sharīfah (2022) al-amn al-sybrāny wa-taḥaddiyāt aljwssh wālākhtrāqāt al-iliktrūnīyah lil-duwal 'abra al-fadā' al-sybrāny, Majallat al-Ḥuqūq wa-al-'Ulūm al-Insānīyah, al-mujallad (15), al-'adad (1) Jāmi'at al-Jazā'ir, al-Jazā'ir.
- al-mawqī' al-rasmī li-Hay'at al-Iftā' wa-al-tashrī' al-qānūnī fī Mamlakat al-Baḥrayn (<https://www.lloc.gov.bh/>)
- Nadwat 'an bu'd bi-'unwān, "Taṭawwur al-tahdīdāt al-sybrānyh fī al-Baḥrayn", 28 Mārs, Sharikat Inna Jī Inna bi-al-ta'āwun ma'a Sharikat "Jrūb Ayy Bī" al-'Ālamīyah, Mamlakat al-Baḥrayn, 2021m.