Sana'a University Journal of Human Sciences
مجلة جامعة صنعاء للعلوم الإنسانية
Vol. 5 | No. 7 | Page 158 – 194 |2026 |
https://journals.su.edu.ye/index.php/jhs
ISSN : 2958-8677

The Role of Cybersecurity as a Protection Mechanism for E-Government Pillars
"An Applied Study on Yemeni Government Organizations"

Abdulbari Abdullah Mohammed Saeed Al-Atabi [1,*]
[1]Department of Sociology, Faculty of Arts and Humanities - Sana'a University, Sana'a, Yemen.
***Corresponding author:** *alatabiabdalbari@gmail.com*

Keywords

1. Cybersecurity
2. Protection Mechanisms
3. Government
4. Digital Pillars

Abstract:

This study aims to investigate the role of cybersecurity as a protection mechanism for e-government pillars in Yemen. The study adopted a descriptive-analytical methodology, utilizing a questionnaire consisting of (43) items distributed across several Yemeni government organizations for data collection. After verifying the validity and reliability of the instrument, it was applied to a research sample of (320) employees within the targeted organizations.

The study concluded that Financial Services (Bill Payment) is currently the most implemented pillar, with an average score of (4.14). Future aspirations are primarily focused on the establishment of a specialized security apparatus for cybersecurity protection, which received an average score of (4.46). Based on these findings, the study recommends the necessity of integrating cybersecurity strategies into the core of national digital transformation plans.

Sana'a University Journal of Human Sciences
مجلة جامعة صنعاء للعلوم الإنسانية
Vol. 5 | No. 7 | Page 159 – 194 | 2026
https://journals.su.edu.ye/index.php/jhs
ISSN : 2958-8677

دور الأمن السيبراني كآلية حماية لركائز الحكومة الإلكترونية

"دراسة تطبيقية على المنظمات الحكومية اليمنية"

عبدالباري عبدالله محمد سعيد العتابي [1]*،
[1]قسم علم الاجتماع، كلية الآداب والعلوم الإنسانية، جامعة صنعاء ، اليمن.
المؤلف: *alatabiabdalbari@gmail.com*

الكلمات المفتاحية

1. الأمن السيبراني
2. آليات الحماية
3. الحكومة الإلكترونية
4. الركائز الرقمية

الملخص:

تهدف الدراسة إلى استقصاء دور الأمن السيبراني كآلية حماية لركائز الحكومة الإلكترونية في اليمن. واعتمدت الدراسة المنهج الوصفي التحليلي، وطبقت استبانة مكونة من(43)فقرة موزعة على عدد من المنظمات الحكومية اليمنية، وذلك لغرض جمع البيانات، وبعد التأكد من صدقها وثباتها تم تطبيقها على عينة البحث، والتي بلغ عددها (320) موزعة بين الموظفين في تلك المنظمات المستهدفة بالدراسة. وتوصلت الدراسة إلى عدد من النتائج، منها: إن الخدمات المالية (سداد الفواتير) هي الركيزة الأكثر تطبيقاً حالياً بمتوسط (4.14)، بينما تمثلت أبرز المعالجات المستقبلية في إنشاء جهاز أمني متخصص للحماية السيبرانية بمتوسط (4.46). وأوصت الدراسة بضرورة دمج استراتيجيات الأمن السيبراني في صلب خطط التحول الرقمي الوطنية.

المقدمة:

يعد التحول نحو الحكومة الإلكترونية في اليمن ضرورة استراتيجية لضمان استمرارية الخدمات السيادية. ومع ذلك، فإن هذا التحول يواجه تحديات أمنية معقدة تهدد سلامة البيانات المالية والشخصية. وتأتي هذه الدراسة لتبين أن الأمن السيبراني ليس مجرد أداة تقنية تكميلية، بل هو "آلية حماية" جوهرية تضمن استقرار ركائز الحكومة الإلكترونية (المالية، الخدمية، والاجتماعية) في ظل الظروف الاستثنائية التي تمر بها البلاد.

كما تسعى هذه الدراسة إلى تسليط الضوء على الواقع الميداني للأمن السيبراني في المنظمات الحكومية اليمنية، وكيف يمكن لإرساء دعائمه أن يساهم في تأمين التحول الرقمي وضمان استدامته كآلية لخدمة المجتمع وحفظ أمنه القومي.

مشكلة الدراسة وتساؤلاتها:

تكمن المشكلة في الفجوة الواضحة بين التوسع في تقديم الخدمات الرقمية (مثل صرف المرتبات وسداد الفواتير) وغياب أنظمة حماية سيبرانية كافية تحمي هذه القنوات من الاختراق والتعطل. وإن استمرار العمل بالأنظمة الرقمية دون "آلية حماية" واضحة يهدد السيادة المعلوماتية ويفقد المواطن الثقة بالخدمات الحكومية. وتتمثل المشكلة في السؤال التالي: **ما دور الأمن السيبراني في حماية ركائز الحكومة الإلكترونية ومعالجة معوقات تطبيقها في اليمن؟ وتفرعت عنه التساؤلات الفرعية الآتية:**

– ما هو واقع مجالات تطبيق الحكومة الإلكترونية في اليمن حالياً ومستقبلاً؟

– ما هي المعوقات –التشريعية والتقنية– التي تواجه استكمال مشروع الحكومة الإلكترونية؟

– كيف يسهم الأمن السيبراني (كآلية حماية) في معالجة هذه المعوقات وتأمين ركائز الخدمة التي تقدمها الحكومة الإلكترونية؟

أهداف الدراسة:

تسعى الدراسة إلى تحقيق الأهداف التالية:

– تشخيص واقع ركائز الحكومة الإلكترونية في اليمن (الواقع والطموح).

– تحديد المعوقات الجوهرية التي تحول دون التطبيق الكامل لمشروع الحكومة الإلكترونية.

– إبراز دور "الأمن السيبراني" كحل استراتيجي ومعالجة حتمية لضمان استدامة الخدمات الرقمية التي تقدمها الحكومة الإلكترونية.

– تقديم توصيات إجرائية تساهم في إرساء دعائم استراتيجية وطنية للأمن السيبراني في اليمن.

أهمية الدراسة:

تنقسم إلى أهمية علمية وعملية:

1–الأهمية العلمية:

– إثراء المكتبة العربية واليمنية بدراسة حديثة تربط بين الأمن السيبراني والمحور الاجتماعي للرقمنة.

– تقديم إطار نظري وميداني يربط بين الأمن السيبراني واستمرارية الخدمات الحكومية في البيئات غير المستقرة.

2– الأهمية العملية:

– تزويد صناع القرار في المنظمات الحكومية اليمنية(الداخلية، الاتصالات، المالية، الضرائب)

بنتائج ميدانية تساعد في صياغة سياسات حماية للبيانات المالية والوثائق الشخصية للمواطنين.

- تقديم توصيات إجرائية تساهم في وضع استراتيجيات وطنية لإرساء دعائم الأمن السيبراني كآلية حماية للبيانات القومية وحقوق المواطنين.

- تقديم نموذج بحثي مركز (12 فقرة) يتناول قضايا الحماية الرقمية في بيئة استثنائية (اليمن).

أهم مصطلحات الدراسة:

1- تعريف الحكومة الإلكترونية: إن مفهوم الحكومة الإلكترونية يعكس سعي الحكومات إلى إعادة ابتكار نفسها، لكي تؤدي مهامها بشكل فاعل في الاقتصاد العالمي المتصل ببعضه البعض عبر شبكة الاتصالات والحكومات، وهي ليست سوى تحول جذري في الطرق التي تتبعها الحكومات لمباشرة أعمالها، وذلك على نطاق واسع منذ بداية العصر الصناعي (حجازي، بدون تاريخ، 20).

ويعتبر مفهوم الحكومة الإلكترونية من المفاهيم الأساسية والحديثة المرتبطة بالتطور في تكنولوجيا المعلومات والأهمية على القطاع الحكومي، وحسب العلوم الاجتماعية فإنه لا يوجد تعريف شامل لأي مفهوم، ولكن توجد تعاريف تختلف بتخصصات الباحثين واختلاف وجهات نظرهم.

فعرَّف البنك الدولي الحكومة الإلكترونية بأنها: عملية استخدام المؤسسات لتكنولوجيا المعلومات (شبكة الإنترنت، وشبكة المعلومات العريضة، وغيرها)، والتي لديها القدرة على تغيير وتحويل المعاملات مع المواطنين من الوصول للمعلومات، مما يوفر مزيدًا من الشفافية وإدارة أكثر كفاءة للمؤسسات (كمال وهارون، 2014، 5).

وعُرَّف مصطلح الحكومة الإلكترونية من قبل البنك الدولي على أنه « مصطلح حديث النشأة، يشير إلى اكتشاف طرق ووسائل جديدة، من خلال استخدام تكنولوجيا المعلومات والاتصالات، من أجل زيادة كفاءة، فعالية، شفافية ومساءلة الحكومة فيما تقدمه من خدمات للمواطن»(المهتدي، 2011، 25).

وقد توصل الباحث في ضوء تلك الآراء والدراسات ذات الصلة بالحكومة الإلكترونية إلى **تعريف إجرائي للحكومة الإلكترونية؛ بأنها:** الوجه الآخر المتطور للحكومة التقليدية التي تهدف إلى تقديم الخدمات الحكومية المختلفة لجميع فئات المجتمع، باستخدام التقنية الإلكترونية المتطورة، مع ضمان السرية والأمن المعلوماتي، ومؤثرة في المجتمع ومتأثرة به إيجابًا وسلبًا.

2- الأمن السيبراني:

تعريف: الأمن: الأمان والأمانة : بمعنى وقد أمِنْت فأمنا آمِنٌ، وآمنْت غيري من الأمْن والأمان، والأمْن :ضد الخوف(ابن منضور،1414،21).

السيبراني: مشتقة من كلمة "سايبر Cyber" وتعني: كل ما يتعلق أو يرتبط بالحواسيب وتكنولوجيا المعلومات والواقع الافتراضي، وأصل الكلمة يوناني، Kybernetesوتعني القيادة أو التوجيه، ومصدرها Cyberneticsعلم الاتصالات وأنظمة التحكم الآلي في كل من الآلات والأشياء الحية (دحماني،2018، 10).

الأمن السيبراني: يعرف الأمن السيبراني بأنه: "عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة" (Richard,2003. 3).

كما عرفه آخر بأنه: "مجموعة من الإجراءات التقنية والإدارية والتي تشمل العمليات والآليات التي يتم اتخاذها لمنع أي تدخل غير مقصودة أو غير مصرح به للتجسس أو الاختراق لاستخدام أو سوء الاستغلال للمعلومات والبيانات الإلكترونية الموجودة على نظم الاتصالات والمعلومات، كما تضمن تأمين وحماية وسرية وخصوصية البيانات الشخصية للمواطنين، كما تشمل استمرارية عمل حماية معدات الحاسب الآلي ونظم المعلومات والاتصالات والخدمات بمنأى عن أي تغيير أو تلف" (صائغ، 2018، 299).

وفي سياق الدراسة: يُشمل حماية البنى التحتية الرقمية، البيانات الشخصية والحكومية، ومكافحة الجرائم الإلكترونية بمختلف أشكالها.

3- تعريف آليات الحماية:

هي مجموعة من الضوابط التقنية، والإجرائية، والقانونية التي يتم تصميمها لضمان أمن المعلومات وحماية الأصول الرقمية من التهديدات السيبرانية، مع ضمان استمرارية العمل. (القحطاني،2021، 112).

كما عرفها الشمري بأنها: "مجموعة التدابير التقنية والتنظيمية (مثل التشفير، جدران الحماية، وأنظمة كشف التسلل) التي تبنتها المنظمات الحكومية اليمنية لتأمين بيئتها الرقمية ومنع الوصول غير المصرح به للبيانات". (الشمري،2002، 44).

4- الركائز الرقمية للحكومة الإلكترونية: هي المكونات الأساسية والبنية التحتية (التقنية، والخدمية، والبشرية) التي تقوم عليها منظومة التحول الرقمي والحكومة الإلكترونية، وبدون استقرار هذه الركائز لا يمكن تقديم خدمات إلكترونية آمنة. (الزبيدي،2023، 85).

وقصد بها في هذه الدراسة: "البنية التحتية الأساسية التي تُمكّن المنظمة من تقديم خدماتها إلكترونياً، وتشمل الموارد البشرية المؤهلة، والأنظمة البرمجية، وقواعد البيانات، والخدمات المالية (سداد الفواتير) التي تعتمد عليها الحكومة اليمنية في تحولها الرقمي". (بخيت، 2012، 92).

الدراسات السابقة:

1-دراسة (العنوز، 2024) بعنوان: "دور الأمن السيبراني في التقليل من أعداد الجرائم الإلكترونية في محافظة العقبة- باستخدام نظم المعلومات الجغرافية".

هدفت هذه الدراسة إلى توضيح الفرق بين الأمن السيبراني وأمن المعلومات، وعلاقتهم بزيادة أو نقص الجرائم الإلكترونية، من خلال برامج نظم المعلومات الجغرافية التي تساعد في معرفة التدرج اللوني في نسبة الزيادة أو النقص بالجرائم الإلكترونية، حيث إن اللون الغامق يدل على أعلى نسبة، واللون الفاتح أدنى نسبة وذلك خلال فترة الدراسة. حيث إن نظم المعلومات الجغرافية تدرس مجالات الجي معلوماتية بالاعتماد على منهج التحليل المكاني والخرائط الرقمية.

وتعتمد الدراسة على المنهج الوصفي والتحليلي والمنهج التاريخي، للوصول إلى أهم النتائج والحلول التي تحد من الجرائم الإلكترونية التي لا يدرك الشخص مدى خطورتها عليه. كما تنوه هذه الدراسة إلى التعرف على أهم الجرائم الإلكترونية وأهدافها

وعلاقتها بالأمن السيبراني "الجرائم السيبرانية"وتوضيح مدى آثارها وكيفية الوقاية منها. وخلصت الدراسة إلى عدد من النتائج، أهمها:

– توضح الدراسة مدى أهمية الأمن السيبراني وأمن المعلومات ودورها في الحماية والوعي للمحافظة على أمن المعلومات الشخصية الخاصة والعامة.

– قلة وعي المواطنين في استعمال برامج التواصل الاجتماعي.

2– دراسة (عباس، 2024) بعنوان: الحوكمة الرقمية في ظل تهديدات الأمن السيبراني: دولة الإمارات انموذجاً.

هدفت هذه الدراسة إلى عرض وتحليل أهم مخاطر الأمن السيبرانية في ظل تطبيق استراتيجيات التحول الرقمي، ومعرفة طبيعة ومحددات حوكمة تكنولوجيا المعلومات بالمؤسسات الحكومية الاماراتية في ظل تطبيق استراتيجيات الرقمنة، وتحديد طبيعة وأشكال مخاطر الأمن السيبراني في تطبيق استراتيجيات التحول الرقمي بالبيئة الإماراتية، وبيان نماذج وآليات تفعيل التشريعات السيبرانية كركيزة للحد من المخاطر وتحسين جودة العمليات والمنتجات والخدمات العامة بالبيئة الإماراتية. واستخدمت الدراسة المنهج الوصفي لوصف مشكلة الدراسة، ووصف التحول الرقمي للجامعات، وأهم متطلبات تطبيقه، ومعرفة وتحديد العالقات بين مكونات التحول الرقمي، وسياسات الأمن السيبراني، وأهميته، وكيفية تخطيطه في الدول المختلفة، وأهم وسائل التوعية التي يتم تطبيقها في المجتمعات المختلفة، وكيفية التغلب على المخاطر والتهديدات السيبرانية والاستعانة بها لوضع الخطط المستقبلية في الامارات. وخلصت الدراسة إلى عدد من النتائج أهمها:

–الأمن السيبراني هو عملية حماية الأنظمة والشبكات والبرامج ضد الهجمات الرقمية، تهدف هذه الهجمات السيبرانية عادة إلى الوصول إلى المعلومات الحساسة أو تغييرها أو تدميرها؛ بغرض الاستيلاء على المال من المستخدمين أو مقاطعة عمليات الأعمال العادية، ويمثل تنفيذ تدابير الأمن السيبراني تحدياً كبيراً اليوم نظرا لوجود عدد من الأجهزة يفوق أعداد الأشخاص كما أصبح المهاجمون أكثر ابتكاراً.

–إن قضية أمن وحماية المعلومات تعد من أهم قضايا العصر –عصر الثورة الصناعية الرابعة– حيث أصبح نجاح أي مؤسسة يعتمد بشكل كبير علي ما تمتلكه من معلومات، لكن العديد من المعلومات والأنظمة والبنى التحتية المتصلة بالشبكات عرضة للخطر بين الحين والآخر، حيث تواجه بأنواع شتى من الخروقات للمعلومات، كما تتعرض لأنشطة إجرامية (هاكرز) تعطل خدماتها وتدمر ممتلكاتها، وتختلف هجمات الهاكرز من جهة لأخرى ومن مكان لآخر ومن زمن الى زمن مستخدمة أدوات وآليات اختراق متجددة ومتطورة طول الوقت.

3- دراسة (طواهير، 2023) بنعوان: "استراتيجيات الأمن السيبراني كتحدي للتحول الرقمي بالمنظمات الحكومية مع الإشارة لتجربة دولة الإمارات العربية المتحدة.

هدفت الدراسة إلى التعرف على استراتيجيات الأمن السيبراني بالنظر إلى خطورة التهديدات التي يمثلها انعدام الأمن الإلكتروني على الأفراد والمنظمات والدول في ظل الحاجة المتزايدة لضرورة التحول الرقمي في خدمات المنظمات الحكومية. واستخدمت الدراسة المنهج الوصفي التحليلي، وخلصت إلى عدد من النتائج أبرزها:

-إن الجرائم الإلكترونية لن تختفي قريباً. وستكون تحد لتقدم التحول الرقمي ومن المتوقع أن ينمو عدد أكبر من هذه الجرائم في السنوات القادمة ما دام المكان المفضل في جميع أنحاء العالم لهذه الفئة هو الإنترنت. وسيستمر سوق الأمن السيبراني في تحقيق نمو أعلى.

-ضرورة مبادرة الجهات الحكومية والشركات الخاصة لإعادة تقييم استراتيجيات الأمن السيبراني وسياسات أمن شبكة الإنترنت لمواجهة هذه المخاطر.

- استخدام تقنيات جديدة لتطوير منصات الأمن السيبراني الحالية، إذ تبحث العديد من المراكز العالمية في كيفية استخدام الذكاء الاصطناعي لمواجهة التهديدات السيبرانية.

4- دراسة (القحطاني،2021)، بعنوان: "مدى توفر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي – دراسة ميدانية".

هدفت هذه الدراسة إلى التعرف على مدى توفر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي، من خلال التعرف على آرائهم حول المفهوم الأقرب له وأهم الجرائم التي يتعامل معها، وطرق الوقاية المجتمعية من جرائم الفضاء السيبراني والمعوقات المجتمعية لتحقيق الوقاية من هذه الجرائم، وقد استخدمت الدراسة المنهج المسحي الاجتماعي بأسلوب العينة، واعتمدت على الدراسة الوصفية، بالتطبيق على عينة عشوائية من طلاب وطالبات الجامعات السعودية في المستويات الدراسية المختلفة، وبلغت عينة الدراسة (486) طالباً وطالبة، واعتمدت الدراسة على الاستبانة الإلكترونية لتجميع البيانات، وكانت أهم نتائج هذه الدراسة هي: أن أقرب مفهوم للأمن السيبراني من وجهة نظر عينة الدراسة هو "استخدام مجموعة من الوسائل التقنية والتنظيمية والإدارية لمنع الاستخدام غير المصرح به" وكان من النتائج أيضاً وجود معوقات اجتماعية في تحقيق الوقاية للمجتمع السعودي، ومن هذه المعوقات هو التطور الهائل في نظم المعلومات، ووسائل التكنولوجيا التي يتعامل معها أفراد الأسرة، دون المعرفة الكاملة لمشكلات هذه الوسائل وكيفية تجنبها.

5- دراسة (الحميري، 2021) بعنوان: أثر مخاطر تكنولوجيا المعلومات في أمن نظم المعلومات المحاسبية من خلال الضوابط الأمنية (دراسة ميدانية في شركات الاتصالات العاملة في اليمن).

استخدم الباحث المنهج الوصفي التحليلي، وقام بتصميم استبانة لجمع البيانات المتعلقة بالدراسة، وهدفت الدراسة إلى اختبار الضوابط الأمنية كمتغير وسيط بين مخاطر تكنولوجيا المعلومات وأمن نظم المعلومات المحاسبية في شركات الاتصالات العاملة في اليمن. وتوصلت الدراسة إلى عدد من النتائج والتوصيات:

- أهم النتائج التي كشفت عنها الدراسة:

إن مخاطر تكنولوجيا المعلومات تؤثر سلبًا في الضوابط الأمنية، وإن هذه الضوابط لها أهمية إيجابي في أمن نظم المعلومات المحاسبية (الأثر المباشر)، وأشارت النتائج إلى أن مخاطر تكنولوجيا المعلومات لها أهمية سلبية غير مباشرة في أمن نظم المعلومات، وإن وساطة الضوابط الأمنية جزئية.

6- دراسة (حوادسي، 2015) بعنوان: أثر تطبيق الحكومة الإلكترونية على تحسين أداء الموارد البشرية (دراسة حالة بلدية عين مليلة).

هدفت الدراسة إلى محاولة عرض وتقديم الإطار الفكري والنظري للحكومة الإلكترونية، باعتباره مدخلا إداريا حديثا، وبيان الأثر الذي يتركه عند تطبيقه على أداء الموارد البشرية، وتحديد أهداف الحكومة الإلكترونية في الجزائر، من خلال السياسة العامة للدولة في هذا المجال، محاولة إعطاء صورة ميدانية عاكسة لمستوى الحكومة الإلكترونية داخل المنظمات.

وقد استخدمت الدراسة: المنهج الاستنباطي، والاستبانة كأداة للدراسة الميدانية. وتوصلت الدراسة إلى عدد من النتائج والتوصيات.

ومن أهم النتائج التي توصلت لها الدراسة:

- ثبت ضرورة الانتقال من الحكومة التقليدية إلى الحكومة الإلكترونية لمواكبة التطورات الحاصلة في مختلف أنحاء العالم.
- أهمية الاستفادة من التجارب السابقة للدول الأخرى في تطبيق برنامج الحكومة الإلكترونية من خلال دراسة أهم نقاط الضعف ومحاولة تجنبها، وإبراز نقاط القوة والاستفادة منها.
- ثبت أن الحكومة الإلكترونية في هذه الأيام ضرورة حتمية للدولة الساعية إلى تحقيق الكفاءة والفاعلية في تقديم خدماتها.

الفجوة البحثية:

تنفرد هذه الدراسة عن الدراسات السابقة في أنها لا تكتفي برصد معوقات الحكومة الإلكترونية إدارياً، بل تركز بشكل متخصص على (الأمن السيبراني) كآلية حماية ومعالجة لهذه المعوقات، خاصة في ظل تركيز العينة على "إنشاء جهاز أمني متخصص كأهم وسيلة للمعالجة بمتوسط (4.46).

الإطار النظري للدراسة

المحور الأول: الحكومة الإلكترونية (الركائز والماهية) :

إن الأفراد – والمنظمات أو الدول– الذين لا يأخذون بأسباب هذا التطور التكنولوجي الهائل ليسخروا له المصادر لزخم المعلوماتية التي تشكل حجر الأساس للبناء الاقتصادي والاجتماعي والثقافي سيجدون أنفسهم متراجعين إلى الوراء بتسارع، ليصبحوا مغتربين عاجزين في هذا العالم الذي لا ينتظر المتواكلين المتقاعسين (عبد النبي، 2008، 5)، وتم تناول ذلك من خلال الآتي:

أولًا: ماهية الحكومة الإلكترونية: إن مفهوم الحكومة الإلكترونية يعكس سعي الحكومات إلى إعادة ابتكار نفسها، لكي تؤدي مهامها بشكل فاعل في الاقتصاد العالمي المتصل ببعضه البعض عبر شبكة الاتصالات والحكومات، وهي ليست سوى تحول جذري في الطرق التي تتبعها الحكومات لمباشرة أعمالها، وذلك على نطاق واسع منذ بداية العصر الصناعي (حجازي، بدون تاريخ، 20).

ويعتبر مفهوم الحكومة الإلكترونية من المفاهيم الأساسية والحديثة المرتبطة بالتطور في تكنولوجيا المعلومات والأهمية على القطاع الحكومي، وحسب العلوم الاجتماعية فإنه لا يوجد تعريف شامل لأي مفهوم، ولكن توجد تعاريف تختلف بتخصصات الباحثين واختلاف وجهات نظرهم.

فعرَّف البنك الدولي الحكومة الإلكترونية بأنها: عملية استخدام المؤسسات لتكنولوجيا المعلومات (شبكة الإنترنت، وشبكة المعلومات العريضة، وغيرها)، والتي لديها القدرة على تغيير وتحويل المعاملات مع المواطنين من الوصول للمعلومات، مما يوفر مزيدًا من الشفافية وإدارة أكثر كفاءة للمؤسسات (حوشين، 2014، 5).

وعُرَّف مصطلح الحكومة الإلكترونية من قبل البنك الدولي على أنه « مصطلح حديث النشأة، يشير إلى اكتشاف طرق ووسائل جديدة، من خلال استخدام تكنولوجيا المعلومات والاتصالات، من أجل زيادة كفاءة، فعالية، شفافية ومساءلة الحكومة فيما تقدمه من خدمات للمواطن» (المهتدي، 2011، 25).

وَعُرَّفت الحكومة المذكورة بأنها: «استخدام نتاج الثورة التكنولوجية في تحسين مستويات أداء الأجهزة، ورفع كفاءتها وتعزيز فعاليتها في الأهداف المرجوة منها، ويشمل ذلك الاستفادة من تراكم المعرفة والتقدم التقني المرافق لها في توسيع قاعدة المستفيدين من الخدمات العامة، من حيث وفرة هذه الخدمات وتحسين أساليب تقديمها لهم» (العزب، 2018، 305).

ثالثًا: ركائز الحكومة الإلكترونية:

هناك عدد من الركائز التي تتميز فيها الحكومة الإلكترونية، نذكر منها ما يأتي: (حسين، 2013، 445).

– تجميع كافة الأنشطة والخدمات المعلوماتية في موضع واحد، هو موقع الحكومة الرسمي على الإنترنت.

– تحقيق سرعة وفعالية الربط والتنسيق والأداء والإنجاز بين دوائر الحكومة ذاتها وكل دائرة حكومية على حدة، واتصال دائم بين المواطنين (24) ساعة في اليوم و (7) أيام في الأسبوع، و(365) يوم في السنة.

– القدرة على تأمين كافة الاحتياجات الاستعلامية والخدمية للمواطن عن طريق مختلف الخدمات.

– تحقيق وفرة في الإنفاق في كافة العناصر، مع تحقيق عوائد أفضل من الأنشطة الحكومية ذات العائد التجاري.

– تقليل الاعتماد على العمل الورقي واليدوي.

– الشفافية في التعامل.

– وهناك ثمة أوليات من الخدمات تقدمها بعض القطاعات الحكومية للمواطن، مثل خدمات الأحوال المدنية، والتعليم الأساسي والأكاديمي عن بعد، وخدمات الأعمال، والخدمات الاجتماعية، والسلامة العامة والأمن، والضرائب، والرعاية الصحية، وشؤون النقل، والخدمات المالية، ووسائل الدفع (حافظ، 2021، 485).

المحور الثاني: الأمن السيبراني (كآلية الحماية):

يشكل هذا المحور صلب الموضوع، الذي تناولت فيه:

أولاً: مفهوم الأمن السيبراني:

تم تعريف الأمن السيبراني بأنه: «مسؤولية مشتركة بين جميع الجهات الحكومية والشركات والمؤسسات والأفراد»(الاستراتيجية الوطنية، 2014، 16).

ويعرف الأمن السيبراني بأنه: " أمن الشبكات والأنظمة المعلوماتية، والبيانات، والمعلومات، والأجهزة المتصلة بالأنترنت، وعليه فهو المجال الذي يتعلق بإجراءات، ومقاييس، ومعايير الحماية المفروض اتخاذها، أو الالتزام بها، لمواجهة التهديدات، ومنع التعديات، أو على الأقل الحد من آثارها(جبور، 2012، 25).

ثانياً: مبادئ الأمن السيبراني الثلاثة (CIA Triad): وكيف تنطبق على بيانات المواطنين في اليمن.

ذكر كل من (البار والمرحبي 2020، 2) أن هناك ثلاثة مبادئ للأمن السيبراني ويجب أن تتكامل هذه العناصر حتى توفر الحماية المطلوبة وفى حال فقد أي منها سيكون هناك خلل أمنى فى الجانب الذى يغطيه هذا العنصر. وللمحافظة على أمن البيانات والمعلومات في التطبيق أو النظام يجب أن تتوفر ثلاثة عناصر، هي:

–**السرية (Confidentiality):** تعني منع الوصول إلى المعلومات، إلا من الأشخاص المصرح لهم فقط، سواءً عند تخزينها أم معالجتها أم عند نقلها عبر وسائل الاتصال، وكذلك تحديد صلاحية التعديل والحذف والإضافة.

–**التكامل وسلامة المحتوى (Integrity):** المقصود بها أن تكون المعلومة صحيحة عند إدخالها، وكذلك أثناء تنقلها بين الأجهزة في الشبكة، والتأكد أنه لم يمسها أي تغيير، وذلك باستخدام مجموعة من الأساليب والأنظمة.

–**التوافر والإتاحة (Availability):** تعني بقاء المعلومة متوفرة للمستخدم وإمكانية الوصول إليها في أي وقت، وعدم تعطل ذلك نتيجة لخلل في أنظمة إدارة قواعد المعلومات والبيانات، أو وسائل

الاتصال. **كيف تنطبق على بيانات المواطنين في اليمن؟**

لقد ذكر(غيدان والربيعي، 2012) مجموعة من الإجراءات التي يجب على الحكومات بالتعاون مع الأفراد لتحقيق –مبادئ– الأمن السيبراني، نلخصها فيما يأتي:

1– استخدام كلمة مرور قوية للبيانات والمستندات المهمة.

2– عدم تخزين التفاصيل المهمة مثل كلمات المرور للحساب المصرفي أو أسماء المستخدمين.

3– عبر الإنترنت أو الكمبيوتر، فيجب أن نتذكر أن الإنترنت والفضاء الإلكتروني هو شبكة مفتوحة غير آمنة.

4– عدم فتح أية رسائل إلكترونية مجهولة.

5– تجنب استخدام المواقع المحظورة غير الآمنة، حيث تمثل هذه المواقع درجة عالية من المخاطر.

6– تغيير كلمات المرور باستمرار وتثبيت برنامج قوي لمكافحة الفيروسات للحماية من أحصنة طروادة والفيروسات القوية.

7– يجب تأمين الخوادم لضمان الأمن السيبراني المستمر.

8– يجب أن تخضع البيانات الحكومية للتدقيق المستمر، والحرص على عدم تخزين المعلومات السرية جداً على الإنترنت، وعدم تبادل المعلومات السرية.

9– تجنب الاستخدام المستمر لبطاقات الائتمان الخاصة.

10– وضع قوانين صارمة من قبل الحكومات تجاه مجرمي الإنترنت.

ثالثاً: الأمن السيبراني كداعم للثقة الرقمية:

إن توعية وتدريب المستخدمين على المبادئ الأساسية للأمن السيبراني يجب أن تكون جزءًا أساسيًا من أي استراتيجية، أو مبادرة وطنية أو إقليمية لمكافحة الجرائم السيبرانية (ITU, 2012, 18).

وقد تنبهت معظم الدول في العالم إلى ذلك، فعملت على توعية المستخدمين بمخاطر الجرائم السيبرانية وكيفية تفاديها؛ أي أن يكون الهدف من التوعية والتدريب الموجه للأفراد تمكينهم من تعلم الوسائل التي تتيح لهم حماية أنفسهم في الفضاء السيبراني، ومن ثم الوقاية من هذه الجرائم السيبرانية، وكذلك معرفة آليات المساعدة في حال وقوعهم ضحية لجريمة سيبرانية وكيفية التصرف عند حدوث ذلك، والإجراءات القانونية المفروض اتخاذها من قبل الجهات الرسمية المختصة، ويسهم ممثلو القضاء ومكاتب المدعين العامين وأجهزة التحقيق في عدد من الدول في عمليات التوعية والتدريب، باعتبار أن ذلك من شأنه تغيير سلوك الأفراد والتخفيف من أهمية الجرائم السيبرانية الواقعة عليهم ودعم جهود مكافحة هذه الجرائم (University of Mississippi, 47).

والتشجيع على وضع إطار عالمي للتعاون والتوعية على الصعيدين الإقليمي والوطني، من أجل إرساء ثقافة عالمية للأمن السيبراني، ومساعدة المستهلكين على فهم المخاطر والوقاية منها بشكل أفضل، وكذلك المساعدة في توعية المستهلكين في مجال التجارة الإلكترونية والمعاملات المتنقلة، واطلاعهم على التشريعات المالية للمعاملات الإلكترونية ونظم الدفع المتنقلة، وتشجيع وضع آليات مؤسسية وتنظيمية على الصعيدين الوطني والإقليمي لتيسير التنفيذ الفعَّال

لاستراتيجيات الأمن السيبرانى، ووضع تدابير لحماية المستهلكين والأطفال والأشخاص الضعفاء الآخرين عند استعمالهم تكنولوجيات المعلومات والاتصالات، والوعى بالتهديدات السيبرانية وتدابير الأمن السيبراني واعتماد تدابير لحماية الخصوصية والبيانات الشخصية، ووضع استراتيجية منسقة لتحسين أمن المعلومات ومكافحة التهديدات السيبرانية(فوزي، 2009، 117).

لذلك فإن إشكالية الأمن المعلوماتي باتت تشكل إرهابًا قويًا وتحديًا خطيرًا لمختلف الدول، وأصبحت أهمية الإعلام الرقمي والأمني تتزايد يوم تلو الآخر لتحقيق أمان واستقرار الدولة، فأصبح الإعلام بمثابة جيش ودرع للدولة، تتزايد قوته وقدرته على مواجهة تحدي الجرائم الإلكترونية والوقاية منها كلما زادت التقنية والتطبيقات(قرني والمنعم، 2022، 674).

المحور الثالث: العلاقة بين الأمن السيبراني وركائز الحكومة الإلكترونية:

وفي هذ المحور الذي يربط البحث ببعضه، سوف نركز فيه على:

أولاً: الأمن السيبراني كآلية حماية: إن الأمن السيبراني جزء أساسي من أمن الدول، فيرتبط بالمسائل المتعلقة بحماية المعلومات على جميع أنظمة الحوسبة والشبكات الإلكترونية، لعظم أهمية الأمن السبيراني وحاجة الناس إليه، ولارتباطه بواقعنا المعاصر بات حماية الفضاء السيبراني ضرورة لا غني عنها؛ لأن حربه أصبح عبر القارات، وهي أخطر الحروب، وتزداد خطورتها كلما زاد التقدم في المجال المعلوماتي، فالدمار الذي تلحقه هذه الحرب أشد وطأة وشراسة من الحرب التقليدية، فكان لابد من وجود الأمن السيبراني لحماية القطاعات الحيوية، التي تقدم الخدمات للمجتمع عبر نافذة أو بوابة الحكومة الإلكترونية(البشير، بدون تاريخ، 455).

والجدير بالذكر، أن العالم يتجه نحو ما يمكن تسميته بالاستقلال أو السيادة السيبرانية الوطنية –لتعزيز أداء وعمل الحكومات الإلكترونية–، والدول المرشحة حاليًا لتحقيق هذا النوع من السيادة هي الصين، وروسيا، وتركيا، وإيران؛ وذلك لأسباب سياسية، منها دوافع التحرر من كل قيود الهيمنة والسيطرة الأمريكية والغربية.

ولمعرفة دور الأمن السيبراني في حماية ركائز الحكومة الإلكترونية – باعتبارها أبرز مظاهر العولمة في العصر الحديث– يمكن القول: هناك عدد من التجارب الناجحة في ميدان تطبيق الحكومة الإلكترونية على المستوى العالمي عمومًا وفي الدول المتقدمة خصوصًا، ومما لاشك فيه أن هذه التجارب كانت –وماتزال– هدفًا لعدد من الأبحاث والدراسات التي اهتمت في هذا المجال التطبيقي وما رافقها من سلبيات وما حققته من نجاحات، وكان من شأن ذلك ظهور مجتمع معلومات عالمي أتاح فرصًا جديدة لجميع بلدان العالم لتؤدي التكنولوجيا دورًا تكنولوجيًا متزايد الأهمية في التنمية الاجتماعية والاقتصادية، وقد أصبح أداء الخدمات في مجالات الصحة والتعليم والأعمال التجارية والتمويل والإدارة العامة أكثر

سهولة، بفضل تطبيقات تكنولوجيا المعلومات والاتصالات. (المرشد، 2009، iii).

ثانياً: مواجهة التهديدات السيبرانية: (القرصنة، الاختراق، والعبث بالبيانات) التي كشفت عنها الدارسة الميدانية.

وفي الوقت ذاته تزداد الدول شراهة في استخدام الفضاء الإلكتروني، فقد انخرطت في عمليات تجسس على مستويات لم يسبق لها مثيل، وأعدت ساحات المعركة لحروب لم يخطر ببال أحد أنها ستقوم (كلارك وروبرت، 2011، 3).

ومن غير المرجح اليوم أن تؤدي أي أسباب تقنية– كتوقف الإنترنت– إلى الأهمية في الاعتماد على هذه الشبكة، وذلك لطبيعة البنية الأساسية للشبكة، ولبروتوكولات الاتصال بين الأجهزة المتصلة، ولكن ازدياد المخاطر التقنية والجرائم السيبرانية وضعف الأمن السيبراني هو ما قد يضعف الثقة بالإنترنت، ويدفع الناس إلى تجنب استعمالها. (Stein Schjolberg, 2008).

وتشير بعض الإحصاءات إلى أن65% من مستخدمي الإنترنت من الرجال يقعون ضحية هذه الجرائم مقابل 52% من مستخدمي الإنترنت من النساء، وفي دراسة أخرى أجراها الاتحاد الأوروبي عام2014م أظهرت أن4% من النساء ما بين سن 18و 29عامًا قد عانوا خلال السنة السابقة من ملاحقة عبر الفضاء السيبراني (cyberstalking)، في حين أن 11% من النساء اللواتي تمت مقابلتهن لغرض الدراسة وهن بعمر 15 عاماً، قد تلقوا نوعًا من الرسائل غير المرغوب فيها، كالرسائل الجنسية الهجومية عبر البريد الإلكتروني أو الرسائل النصية (SMS)، أو التحرش غير اللائق عبر شبكات التواصل الاجتماعي، وتعد الولايات المتحدة الأمريكية البلد الأول المنتج للبريد الواغل غير المرغوب فيه (spam). وتعبر ما يقارب من نصف مستخدمات الإنترنت في الدول العربية (49%) عن عدم شعورهن بالأمان بسبب التحرش عبر الإنترنت، وأبلغت نسبة 16% من النساء في الدول العربية عن تعرضهن للعنف على الإنترنت على الأقل مرة واحدة في حياتهن، ونسبة 60% من النساء اللاتي تعرضن للعنف على الإنترنت في المطلق (هيئة الأمم المتحدة، بدون تاريخ، 2).

تقدر خسائر منطقة الشرق الأوسط نتيجة الجرائم الإلكترونية بأكثر من مليار دولار، وتعد منطقة الخليج العربي الأكثر تعرضًا للهجمات في الشرق الأوسط...، وقدر الإنفاق العربي على أمن المعلومات نحو 9,2مليار دولار عام 2018، وكذلك قدر حجم الإنفاق العالمي على أمن المعلومات ما يقارب 96,3مليار دولار بنهاية 2018(اتحاد المصارف العربية،2018، 2).

ويعتمد نجاح الجهات الأمنية بصورة أساسية على ما تقوم به من عمل فعال في مجالي جمع وتحليل المعلومات...، وإن الدول الحديثة أصبحت تعتمد في قدراتها الأمنية على المعلومات الاستخباراتية التي تقوم بها الأجهزة الأمنية والمخابراتية...، وكذلك تعتمد على تطور المنظومة الأمنية والاستخباراتية وكفاءة رجالها من خلال قدراتهم الفائقة والسريعة على التحليل والتقييم والمتابعة، وذلك من خلال اعتمادهم على الأساليب العلمية والمنهجية عند دراسة المعلومات وتحليلها، بما يضمن تحقيق وتهيئة أمنية محكمة وسد الثغرات

الأمنية ومكافحة الأنشطة الهدامة لتحقيق لأمن العام وحماية الوطن(اللوزي، 2020، 1)، وذلك يستدعي أهمية تطبيق نظام الحكومة الإلكترونية لكفاءة هذا النظام وقدرته على جمع المعلومات والبيانات وتحليلها وبشكل واسع، نظرًا لمدى انتشار نظام الحكومة الإلكترونية على المستوى المحلي بين أوساط المجتمع أو على الصعيد العالمي؛ أي أن ذلك سيعزز من قدرات الأجهزة الأمنية والاستخباراتية في ضبط الأمن الوطني ومكافحة الجريمة والحد من انتشارها.

ومما يجدر ذكره أن نظام الحكومة الإلكترونية بمقدار ما هو عامل مساعد وداعم للعمل الأمني إلا أنه يخلق ثغرات أمنية من نوع آخر لطبيعة النظام التقني وبنيته الإلكترونية، وهذا يحتاج إلى جهود أمنية متطورة وعناصر مدربة ومسلحة بالعلوم الأمنية الحديثة، ولاسيما العلوم السيبرانية لما لها من ارتباط وثيق بنظم الحكومة الإلكترونية. وخصوصاً في الدول التي تعتمد على استيراد التكنلوجيا من الخارج بشكل كامل، ومنها اليمن.

المحور الرابع: منهجية الدراسة وإجراءاتها الميدانية:

1. منهج الدراسة:

اعتمدت الدراسة على المنهج الوصفي التحليلي، كونه المنهج الأنسب لوصف واقع "الأمن السيبراني" في المنظمات الحكومية اليمنية وتحليل دوره في حماية ركائز الحكومة الإلكترونية، وذلك من خلال جمع البيانات الميدانية وتحليلها إحصائياً لاستخلاص النتائج.

2. مجتمع وعينة الدراسة:

- **مجتمع الدراسة:** تمثل مجتمع الدراسة في الموظفين والكوادر الإدارية والتقنية في مجموعة من المنظمات الحكومية اليمنية التي طبقت نظام الحكومة الإلكترونية (الداخلية، المالية، الاتصالات، الضرائب) بأمانة العاصمة صنعاء لعام 2025م.

- **عينة الدراسة:** تم اختيار عينة عشوائية بلغت (320) فرداً من الفاعلين الحقيقيين والمتعاملين مع المنظومة الرقمية، لضمان الحصول على بيانات تعكس الواقع الفعلي للمخاطر والحماية السيبرانية. وتم توزيع (320) استمارة استبانة في المنظمات الآنفة الذكر وتم استرجاع (273) استمارة، وكان الفاقد منها (47)، وتم استبعاد (23) لأن أفراد العينة قد تخطوا بعض العبارات الموجودة في الاستبانة، وبهذا يكون عدد استمارات الاستبانة الصالحة لتحليل بياناتها واستخراج النتائج وتحليلها (250) استمارة استبانة.

جدول (1) استمارات الاستبانة الموزعة والمسترجعة والمفقودة والصالحة

	الموزعة	المسترجعة	المفقودة	غير الصالحة	الصالحة
العدد	320	273	47	23	250
النسبة	%100	%85.31	%14.69	%7.19	%78.12

3- أداة الدراسة:

أ-بناء الأداة:

بعد الاطلاع على الأدبيات والدراسات السابقة والتقارير والندوات والمؤتمرات العلمية ذات العلاقة بمتغيرات الدراسة الحالية، تم بناء استبانة تحتوي على البيانات الديموغرافية والوظيفية لأفراد العينة، محور أساسي: دور الأمن السيبراني كآلية حماية لركائز الحكومة الإلكترونية، وقد اتبع الباحث لبناء أداة الدراسة الخطوات الآتية:

- الصورة الأولية للأداة:

تكونت الصورة الأولية للأداة (الاستبانة) من: الجزء الأول البيانات الديموغرافية والوظيفية لأفراد عينة الدراسة، تضمنت المتغيرات (العمر، المؤهل العلمي، سنوات الخبرة، جهة العمل، الدرجة الوظيفية)، والجزء الثاني البيانات الأساسية وتكونت من محورين رئيسين تضمنت في صورتها الأولية (43) فقرة موزعة على (2) محورين والجدول(2) يوضح محاور وأبعاد الدراسة:

جدول رقم (2) محاور وأبعاد الاستبانة وعدد فقرات كل بعد في صورتها الأولية

المحور	الأبعاد	عدد الفقرات
دور الأمن السيبراني كآلية حماية لركائز الحكومة الإلكترونية.	دور الأمن السيبراني في تعزيز ركائز الحكومة الإلكترونية.	8
	التحديات والمخاطر السيبرانية التي تواجه المنظمات اليمنية.	4
واقع ركائز الحكومة الإلكترونية في اليمن ومتطلبات حمايتها سيبرانياً.	مجالات تطبيقها حاليًا	5
	المجالات التي يمكن تطبيقها مستقبلًا.	9
	معوقاتها.	8
	معالجتها.	9
الإجمالي		43

ب- ضبط أداة الدراسة: صدق الأداة:

لقد قام الباحث بالتأكد من صدق أداة جمع المعلومات من خلال ما يأتي:

- الصدق الظاهري (صدق المحتوى):

بعد انتهاء الباحث من إعداد الاستبانة وتحديد وصياغة فقرات المحاور، تم عرض الاستبانة على (8) أساتذة محكّمين من ذوي الخبرة والمعرفة في مجال الدراسة والبحث العلمي؛ من أجل الاستفادة من خبراتهم ومعارفهم. وقد استجاب الباحث لآراء هؤلاء المحكمين؛ فتم إجراء ما يلزم من حذف وتعديل في ضوء المقترحات المقدمة.

– **صدق الاتساق الداخلي:** يقصد بالصدق الداخلي للأداة، مدى ارتباط كل عبارة من عبارة المحور مع الدرجة الكلية للمحور الذي تنتمي إليه، وللتأكد من ذلك تم استخدام معامل الارتباط بيرسون للتأكد من ارتباط الفقرات بعد تطبيق الاستبانة على عينة استطلاعية قوامها (36) من عينة الدراسة، وكانت النتائج كما هي مبينة بالجداول الآتية:

المحور الأول: دور الأمن السيبراني كآلية حماية لركائز الحكومة الإلكترونية:

جدول(3) معامل ارتباط فقرات أبعاد المحور مع الدرجة الكلية للبُعد الذي تنتمي إليه

الفقرة	معامل الارتباط R	مستوى الدلالة Sig.	الدلالة الإحصائية	الفقرة	الارتباط مع المحور R	مستوى الدلالة Sig.	الدلالة الإحصائية
دور الأمن السيبراني في تعزيز ركائز الحكومة الإلكترونية.				التحديات والمخاطر السيبرانية التي تواجه المنظمات اليمنية.			
1	.749**	.000	دالة إحصائيًا عند(0.01)	1	.716**	.000	دالة إحصائيًا عند(0.01)
2	.736**	.000	دالة إحصائيًا عند(0.01)	2	.772**	.000	دالة إحصائيًا عند(0.01)
3	.770**	.000	دالة إحصائيًا عند(0.01)	3	.825**	.000	دالة إحصائيًا عند(0.01)
4	.676**	.000	دالة إحصائيًا عند(0.01)	4	.704**	.000	دالة إحصائيًا عند(0.01)
5	.814**	.000	دالة إحصائيًا عند(0.01)				
6	.813**	.000	دالة إحصائيًا عند(0.01)				
7	.771**	.000	دالة إحصائيًا عند(0.01)				
8	.622**	.000	دالة إحصائيًا عند(0.01)				

(**) وجود ارتباط ذي دلالة إحصائية عند مستوى الدلالة ($\alpha \leq 0.01$)

بينت نتائج التحليل بالجدول(3) أن كافة فقرات المحور (دور الأمن السيبراني كآلية حماية لركائز الحكومة الإلكترونية) ذات علاقة ارتباطية مع الدرجة الكلية للبعد الذي تنتمي إليه.

وبين الجدول أن معامل ارتباط فقرات المحور الأول: دور الأمن السيبراني في تعزيز ركائز الحكومة الإلكترونية مع الدرجة الكلية للبعد تتراوح بين(**.622-**.814)، وهي دالة إحصائيًا لكافة الفقرات عند مستوى دلالة (0.01)، وكذلك تراوح معامل ارتباط فقرات المحور الثاني: مخاطر وتحديات الأمن السيبراني الميدانية مع الدرجة الكلية للبعد بين(**.704-**.825)، وهي دالة إحصائيًا لكافة الفقرات عند مستوى دلالة (0.01).

المحور الثاني: واقع ركائز الحكومة الإلكترونية في اليمن ومتطلبات حمايتها سيبرانياً. (مجالاتها- معوقاتها- معالجتها):

جدول (4) معامل ارتباط فقرات أبعاد المحور الثاني مع الدرجة الكلية للبُعد الذي تنتمي إليه

الفقرة	معامل الارتباط R	مستوى الدلالة Sig.	الدلالة الإحصائية	الفقرة	الارتباط مع المحور R	مستوى الدلالة Sig.	الدلالة الإحصائية
المجالات التي يطبق فيها نظام الحكومة الإلكترونية حاليًا.				**المجالات التي يمكن أن يطبق فيها نظام الحكومة الإلكترونية مستقبلًا.**			
1	.640**	.000	دالة إحصائيًا عند(0.01)	1	.756**	.000	دالة إحصائيًا عند(0.01)
2	.752**	.000	دالة إحصائيًا عند(0.01)	2	.814**	.000	دالة إحصائيًا عند(0.01)
3	.781**	.000	دالة إحصائيًا عند(0.01)	3	.804**	.000	دالة إحصائيًا عند(0.01)
4	.722**	.000	دالة إحصائيًا عند(0.01)	4	.756**	.000	دالة إحصائيًا عند(0.01)
5	.733**	.000	دالة إحصائيًا عند(0.01)	5	.752**	.000	دالة إحصائيًا عند(0.01)
معوقات تطبيق نظام الحكومة الإلكترونية				6	.735**	.000	دالة إحصائيًا عند(0.01)
1	.595**	.000	دالة إحصائيًا عند(0.01)	7	.662**	.000	دالة إحصائيًا عند(0.01)
2	.614**	.000	دالة إحصائيًا عند(0.01)	8	.683**	.000	دالة إحصائيًا عند(0.01)
3	.660**	.000	دالة إحصائيًا عند(0.01)	9	.660**	.000	دالة إحصائيًا عند(0.01)
4	.785**	**.000**	**دالة إحصائيًا عند(0.01)**	**معالجة معوقات تطبيق نظام الحكومة الإلكترونية**			
5	.636**	.000	دالة إحصائيًا عند(0.01)	1	.655**	.000	دالة إحصائيًا عند(0.01)
6	.681**	.000	دالة إحصائيًا عند(0.01)	2	.676**	.000	دالة إحصائيًا عند(0.01)
7	.774**	.000	دالة إحصائيًا عند(0.01)	3	.725**	.000	دالة إحصائيًا عند(0.01)
8	.760**	.000	دالة إحصائيًا عند(0.01)	4	.747**	.000	دالة إحصائيًا عند(0.01)
(**)وجود ارتباط ذي دلالة إحصائية عند مستوى الدلالة (α.≤ 0.01)				5	.734**	.000	دالة إحصائيًا عند(0.01)
				6	.733**	.000	دالة إحصائيًا عند(0.01)
				7	.742**	.000	دالة إحصائيًا عند(0.01)

الفقرة	معامل الارتباط R	مستوى الدلالة Sig.	الدلالة الإحصائية	الفقرة	الارتباط مع المحور R	مستوى الدلالة Sig.	الدلالة الإحصائية
				8	.763**	.000	دالة إحصائيًا عند(0.01)
				9	.711**	.000	دالة إحصائيًا عند(0.01)

بينت نتائج التحليل بالجدول(4) أن كافة فقرات المحور الثاني "واقع ركائز الحكومة الإلكترونية في اليمن ومتطلبات حمايتها سيبرانياً. (مجالاتها – معوقاتها– معالجتها)" ذات علاقة ارتباطية مع الدرجة الكلية للبعد الذي تنتمي إليه.

فقد تبين أن معامل ارتباط فقرات: المجالات التي يطبق فيها نظام الحكومة الإلكترونية حاليًا مع الدرجة الكلية للبعد تتراوح بين(**640.–**781.)، وهي دالة إحصائيًا لكافة الفقرات عند مستوى دلالة (0.01)، وكذلك تتراوح معامل ارتباط فقرات: المجالات التي يمكن أن يطبق فيها نظام الحكومة الإلكترونية مستقبلًا مع الدرجة الكلية للبعد تتراوح بين(**660.–**814.)، وهي دالة إحصائيًا لكافة الفقرات عند مستوى دلالة(0.01)، وكذلك تتراوح معامل ارتباط فقرات: معوقات تطبيق نظام الحكومة الإلكترونية مع الدرجة الكلية للبعد تتراوح بين(**595.–**774.)، وهي دالة إحصائيًا لكافة الفقرات عند مستوى دلالة(0.01)، إضافة إلى أن معامل ارتباط فقرات: معالجة معوقات تطبيق نظام الحكومة الإلكترونية مع الدرجة الكلية للبعد تتراوح بين(**655.–**763.)، وهي دالة إحصائيًا لكافة الفقرات عند مستوى دلالة (0.01).

وتشير النتائج المبينة بالجداول السابقة أن كافة فقرات أداة الدراسة ذات اتساق داخلي، أي أن الفقرات تتمتع بدرجة صدق عالية، وأن أداة الدراسة صادقة لقياس ما أُعدت لقياسه، وبهذا يكون الباحث قد تأكد من صدق أداة الدراسة.

4– ثبات الأداة:

تم إجراء اختبار الفا كرونباخ (s Cronbac'Alpha) لمعرفة ثبات عبارات الاستبانة ومصداقيتها وأسلوب ألفا كرونباخ يعتمد على مدى تقارب استجابات عينة البحث على عبارات الأداة، فكلما تقاربت الإجابات لعينة البحث ارتفعت درجة الثبات، ويتبع ذلك درجة الصدق الذاتي وهي عبارة عن الجذر التربيعي للثبات، وكانت النتائج كما هي مبينة بالجدول الآتي:

جدول(5) معامل الثبات (ألفا كرونباخ) والصدق الذاتي لمحاور وأبعاد أداة الدراسة

المحور	الأبعاد	قيمة ألفا كرونباخ	الصدق الذاتي
دور الأمن السيبراني كآلية حماية لركائز الحكومة الإلكترونية.	دور الأمن السيبراني في تعزيز ركائز الحكومة الإلكترونية.	0.800	0.894
	التحديات والمخاطر السيبرانية التي تواجه المنظمات اليمنية.	0.820	0.906
واقع ركائز الحكومة الإلكترونية في اليمن ومتطلبات حمايتها سيبرانياً (مجالاتها– معوقاتها– معالجتها).	مجالات تطبيقها حاليًا	0.823	0.908
	المجالات التي يمكن أن يطبق فيها مستقبلًا.	0.816	0.903
	معوقات تطبيقها.	0.827	0.909
	معالجة معوقاتها.	0.814	0.902

يتبين من الجدول (5) أن قيمة معامل ثبات محاور أداة الدراسة عالية، فقد تراوح معامل الثبات من وجهة نظر العاملين بالمنظمات بين (0.800 – 0.827)، وهي معاملات ثبات عالية، وتراوح الصدق الذاتي لأبعاد أداة الدراسة بين (0.894 – 0.909)، وهي عالية جدًا، وهذا يعني أن الاستبانة تتمتع بثبات عالٍ، ويوحي هذا بأن العينة متجانسة في الاستجابة على الاستبانة، ويمكن الاعتماد على نتائج تطبيقها في تعميمها على مجتمع الدراسة بدرجة كبيرة.

ومن خلال ما سبق يكون الباحث قد تأكد من صدق وثبات أداة الدراسة. وبهذه الإجراءات خرجت الأداة بصورتها النهائية مكونة من (43) فقرة موزعة على محورين وأبعاد الدراسة. كما هي موضحة بالجدول الآتي:

الجدول رقم (6) فقرات وأبعاد ومحاور أداة الدراسة في صورتها النهائية

المحور	الأبعاد	عدد الفقرات
دور الأمن السيبراني كآلية حماية لركائز الحكومة الإلكترونية.	**دور الأمن السيبراني في تعزيز ركائز الحكومة الإلكترونية.**	8
	التحديات والمخاطر السيبرانية التي تواجه المنظمات اليمنية.	4
إجمالي فقرات المحور الأول		12
	مجالات تطبيقها حاليًا	5

واقع ركائز الحكومة الإلكترونية في اليمن ومتطلبات حمايتها سيبرانياً (مجالاتها- معوقاتها- معالجتها).	المجالات التي يمكن تطبيقها مستقبلًا.	9
	معوقاتها	8
	معالجتها	9
إجمالي فقرات المحور الثاني		31
الإجمالي		43

6-التوزيع الطبيعي لاستجابات أفراد عينة الدراسة:

للتأكد من الأساليب الإحصائية المناسبة سواء الاختبارات المعلمية أو اللامعلمية، تأكد الباحث من التوزيع الطبيعي لمتوسط استجابات عينة الدراسة على أبعاد الأداة، وكانت النتائج كما هي مبينة بالجدول الآتي:

جدول(7) نتائج معاملي(الالتواء والتفلطح) للتأكد من التوزيع الطبيعي لبيانات الدراسة

المحور	الأبعاد	معامل الالتواء Skewness	معامل التفلطح Kurtosis
دور الأمن السيبراني كآلية حماية لركائز الحكومة الإلكترونية.	دور الأمن السيبراني في تعزيز ركائز الحكومة الإلكترونية.	0,751-	1,627
	التحديات والمخاطر السيبرانية التي تواجه المنظمات اليمنية.	0,294-	0,045
واقع ركائز الحكومة الإلكترونية في اليمن ومتطلبات حمايتها سيبرانياً (مجالاتها- معوقاتها- معالجتها).	مجالات تطبيقها حاليًا	0,426-	0,649
	المجالات التي يمكن تطبيقها مستقبلًا	0,676-	0,977
	معوقاتها	0,655-	0,612
	معالجتها	1,227-	1,755

بينت نتائج الجدول(8) أن معامل الالتواء(Skewness) لمتوسطات استجابات أفراد عينة الدراسة كانت بين (0.294-، 1.227-) وهي ضمن الفترة المسموح بها والمحددة بين ± 2.58، وهذا يشير إلى أن البيانات تتبع التوزيع الطبيعي، وعليه فإن الباحث سوف يعتمد على الاختبارات المعلمية في الأساليب الإحصائية المستخدمة للإجابة عن أسئلة وفرضيات الدراسة.

6- مقياس الدراسة:

تم قياس درجة الاستجابات المحتملة على الفقرات إلى تدرج خماسي حسب مقياس ليكرت الخماسي (Likart Scale)، فى توزيع أوزان إجابات أفراد العينة، والذى يتوزع من أعلى وزن له والذى أعطيت له (5) درجات، والذي يمثل في حقل الإجابة (موافق بشدة) إلى أدنى وزن له والذى أعطي له (1) درجة واحدة وتمثل في حقل الإجابة (غير موافق أبدًا) وبينهما ثلاثة أوزان. وقد كان الغرض من ذلك هو إتاحة المجال أمام أفراد العينة لاختيار الإجابة الدقيقة حسب تقدير أفراد العينة.

7- الأساليب الإحصائية لمعالجة بيانات الدراسة:

اعتمد الباحث على برنامج الحزم الإحصائية للعلوم الاجتماعية Statistical Package for (spss) Social Sciences في عملية تحليل البيانات، وقد استخدم الباحث الأساليب الإحصائية الآتية:

- معامل ارتباط بيرسون Correlation 's Person: لمعرفة مدى وجود علاقة من نوع الارتباط بين محاور الدراسة وفقراتها، وقد استخدمه الباحث لقياس الاتساق الداخلي لعبارات الاستبانة.
- اختبار ألفا كرونباخ Cronbac's Alpha: للتأكد من ثبات أداة الدراسة.
- التكرارات والنسب المئوية: لوصف المتغيرات الديموغرافية لعينة الدراسة.
- المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية لاستجابات أفراد عينة الدراسة على عبارات الاستبانة.

وقد تم تفسير المتوسطات الحسابية لاستجابة أفراد عينة الدراسة، من خلال حساب طول الفئة كالتالي: حساب المدى(5-1=4)، وتقسيمة على عدد خلايا المقياس أي (5/4 =0,8)، وبعد الحصول على طول الفئة تم إضافتها لأقل قيمة في المقياس. والذي أعطي له (1) درجة واحدة، والتي تمثلت في جعل الإجابة (غير موافق أبدًا)، وتم تحديد فئات المقياس وفقًا للجدول الآتي:

جدول(8) كيفية احتساب التقدير اللفظي لاستجابات أفراد عينة الدراسة.

كيفية احتساب التقدير اللفظي		درجة الموافقة	الدلالة اللفظية
من1.00 إلى 1,80	من20%- إلى 36%	غير موافق أبدًا	ضعيفة جدًا
من 1,81- إلى 2,60	من 36,1%- إلى 52%	غير موافق	ضعيفة
من 2,61- إلى 3,40	من 52,1%- إلى 68%	موافق إلى حد ما	متوسطة
من 3,41- إلى 4,20	من 68,1%- إلى 84%	موافق	عالية
من 4,21-إلى 5	من 84,1%- إلى 100%	موافق بشدة	عالية جدًا

اختبار التباين الأحادي للفروق بين متوسطات استجابات عينة الدراسة نحو محاور الأداة للمتغيرات (المؤهل العلمي، الدرجة الوظيفية، سنوات الخبرة، العمر).

اختبار المقارنة المحورية (LSD) لمعرفة اتجاه الفروق الناتجة عن اختبار التباين الأحادي.

-عرض مؤشرات الدراسة التطبيقية وتحليلاتها: يعد تحديد المؤشرات وتحليلها جزءًا أساسيًا من أي دراسة تطبيقية، إذ تسهم في قياس مدى تحقيق أهداف الدراسة، وتقييم فعالية التدخلات أو البرامج التي تم تنفيذها. وفي هذا القسم من الدراسة، تم توضيح المؤشرات التي تم اختيارها لقياس المتغيرات المختلفة، وكيفية تحليل هذه المؤشرات للوصول إلى نتائج دقيقة وموثوقة.

ويمكن تقسيم هذا الجزء من الدراسة إلى الآتي:

أولاً: دور الأمن السيبراني في تعزيز ركائز الحكومة الإلكترونية: الحكومة الإلكترونية هي سلاح ذو حدين، فهي تحمل في طياتها إمكانات هائلة لتحسين حياة المواطنين، ولكنها في الوقت نفسه تحمل بعض التحديات التي يجب معالجتها. لتحقيق أقصى استفادة من الحكومة الإلكترونية، ويجب أن يتم تصميمها وتنفيذها بطريقة تضمن تحقيق التوازن بين الفوائد والتحديات، مع التركيز على بناء مجتمع رقمي عادل ومتكامل.

تعد الحكومة الإلكترونية ركيزة أساسية لتحقيق التنمية المستدامة والشفافية والمساءلة. وعلى الرغم من التحديات التي تواجهها، إلا أن الاستثمار في تطويرها وتذليل العقبات التي تعترض طريقها يعد استثمارًا في المستقبل.

جدول(9) المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية لاستجابات أفراد عينة الدراسة حول دور الأمن السيبراني في تعزيز ركائز الحكومة الإلكترونية.

م	الفقرة	الترتيب	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	مستوى الأهمية
1	تساهم تدابير الأمن السيبراني في تطوير وسرعة إنجاز العمل الإداري الرقمي بالمنظمات الحكومية.	1	4,17	0.77	%83.40	عالية
2	يعمل الأمن السيبراني كصمام أمان لتسهيل التعاون الرقمي بين الأجهزة العدلية لمكافحة الجرائم الإلكترونية.	4	3.92	0.83	%87.40	عالية
3	يؤدي تطبيق معايير الحماية السيبرانية إلى رفع كفاءة أداء الأجهزة الحكومية في	3	3.93	0.90	%78.60	عالية

م	الفقرة	الترتيب	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	مستوى الأهمية
	ظل الظروف الاستثنائية التي تمر بها اليمن.					
4	تساهم أنظمة التشفير والحماية في تعزيز الثقة الاجتماعية بالخدمات التي تقدمها الحكومة الإلكترونية.	8	3.66	1.11	%73.20	عالية
5	يوفر الأمن السيبراني بيئة آمنة تضمن استدامة التحول الرقمي ومنع توقف الخدمات الحكومية.	5	3.91	0.81	%78.20	عالية
6	تساعد آليات التحقق الرقمي في الحد من عمليات التزوير والتلاعب بالهوية الرقمية للمواطنين.	2	4.00	0.85	%80.00	عالية
7	يعزز الأمن السيبراني من القدرة على التنبؤ بالهجمات التقنية قبل وقوعها، مما يحمي الأمن القومي.	7	3.86	0.89	%77.20	عالية
8	تساهم حماية البيانات وسريتها في زيادة إقبال المواطنين على استخدام تطبيقات الحكومة الإلكترونية.	6	3.89	0.84	%77.80	عالية
المتوسط الإجمالي لفقرات المحور			3.92	0.65	%78.40	عالية

بينت نتائج التحليل الإحصائي بالجدول (9) السابق أن المتوسطات الحسابية لاستجابات أفراد عينة الدراسة حول دور الأمن السيبراني في تعزيز ركائز الحكومة الإلكترونية أن الترتيب العام للأهمية النسبية لفقرات هذا المحور تراوحت بين (3.66– 4.17) وبنسبة (73.20% – 83.40%)، مما يشير إلى مستوى أهمية عالٍ لكافة فقرات المحور بمتوسط إجمالي قدره (3.92). وقد جاءت التفاصيل على النحو الآتي:

– احتلت الفقرة رقم (1) المرتبة الأولى بمتوسط حسابي (4.17) بانحراف معياري (0.77)، وبنسبة أهمية (83.40%)، وتقابل مستوى أهمية عالٍ، والتي تنص على أن: "تساهم تدابير الأمن السيبراني في تطوير وسرعة إنجاز العمل الإداري الرقمي بالمنظمات الحكومية". وتعكس هذه النتيجة المرتفعة أن الأمن السيبراني هو المحرك الأساسي لرفع كفاءة الأداء الحكومي الرقمي.

– جاءت الفقرة رقم (6) في المرتبة الثانية بمتوسط حسابي (4.00) بانحراف معياري (0.85)، وبنسبة أهمية (80.00%)، وتقابل مستوى أهمية عالٍ، والتي تنص على أن: "تساعد آليات التحقق الرقمي في الحد من عمليات التزوير والتلاعب بالهوية الرقمية

للمواطنين". ويشير ذلك إلى الدور الجوهري للأمن السيبراني كآلية حماية سيادية تضمن موثوقية الهوية الرقمية في اليمن.

– حصلت الفقرة رقم (3) على المرتبة الثالثة بمتوسط (3.93) بانحراف معياري (0.90)، وبنسبة أهمية (78.60%)، وتقابل مستوى أهمية عالٍ، والتي نصها: "يؤدي تطبيق معايير الحماية السيبرانية إلى رفع كفاءة أداء الأجهزة الحكومية في ظل الظروف الاستثنائية التي تمر بها اليمن". وهذا يثبت أن الأمن السيبراني هو صمام أمان لاستمرارية الدولة رقمياً في الأزمات.

وفي المرتبة الرابعة، جاءت الفقرة (2) بمتوسط (3.92) وانحراف معياري (0.83)، ونسبة أهمية (78.40%)، وتقابل مستوى أهمية عالٍ، والتي تنص على أن: "يعمل الأمن السيبراني كصمام أمان لتسهيل التعاون الرقمي بين الأجهزة العدلية لمكافحة الجرائم الإلكترونية". مما يؤكد دوره الفعال في إرساء دعائم العدالة الرقمية.

– كشفت النتائج الميدانية عن وعي مرتفع لدى أفراد العينة بدور الأمن السيبراني في تأمين التحول الرقمي، حيث حصلت الفقرة رقم (5) التي نصها: "يوفر الأمن السيبراني بيئة آمنة تضمن استدامة التحول الرقمي ومنع توقف الخدمات الحكومية" على المرتبة الخامسة بمتوسط حسابي (3.91) وانحراف معياري (0.81)، وبلغت أهميتها النسبية (78.20%). وتقابل مستوى أهمية عالٍ، ويعكس ذلك إدراك الكوادر في المنظمات السيادية اليمنية بأن الحماية السيبرانية هي الضامن الوحيد لاستمرارية العمل المؤسسي.

– فيما يتعلق بحماية الخصوصية، نالت الفقرة (8) التي تنص على أن: "تساهم حماية البيانات وسريتها في زيادة إقبال المواطنين على استخدام تطبيقات الحكومة الإلكترونية" أهمية نسبية بلغت (77.80%) وبمتوسط حسابي (3.89) وانحراف معياري (0.84)، وتقابل مستوى أهمية عالٍ، وتؤكد هذه النتيجة أن الأمن السيبراني يمثل الركيزة الأساسية لتعزيز الثقة الرقمية والقبول الاجتماعي للخدمات الإلكترونية في اليمن.

– كما أظهرت النتائج دور الأمن السيبراني كآلية حماية استباقية؛ حيث حصلت الفقرة (7) الخاصة بـ "تعزيز القدرة على التنبؤ بالهجمات التقنية قبل وقوعها مما يحمي الأمن القومي" على متوسط حسابي (3.86) وانحراف معياري (0.89)، وأهمية نسبية (77.20%). وتقابل مستوى أهمية عالٍ.

بينما ساهمت أنظمة التشفير والحماية في تعزيز الثقة الاجتماعية بالخدمات الرقمية الفقرة رقم (4) بمتوسط (3.66) ونسبة أهمية بلغت (73.20%). وإجمالاً، تشير هذه الأرقام إلى توافق كبير بين أفراد العينة على أن الأمن السيبراني هو آلية الدفاع الأولى لحماية ركائز الحكومة الإلكترونية في البيئة اليمنية."

–كما بينت النتائج أن الفقرة (4) المتعلقة بـ "مساهمة أنظمة التشفير والحماية في تعزيز الثقة الاجتماعية بالخدمات التي تقدمها الحكومة الإلكترونية"، قد حصلت على متوسط حسابي (3.66) وانحراف

معياري (1.11)، وبأهمية نسبية بلغت (73.20%). ويرى الباحث أن هذه النتيجة، رغم كونها في المرتبة الأخيرة ضمن هذا المحور، إلا أنها تظل ذات مستوى أهمية– عالٍ، مما يبرز الأثر الاجتماعي المباشر للأمن السيبراني كأداة لبناء جسور الثقة بين المواطن والمؤسسات الحكومية الرقمية. وإجمالاً، تشير هذه الأرقام إلى توافق كبير بين أفراد العينة على أن الأمن السيبراني هو آلية الدفاع الأولى لحماية ركائز الحكومة الإلكترونية في البيئة اليمنية.

وإجمالًا كان المتوسط العام لاستجابات عينة الدراسة على دور الأمن السيبراني كآلية حماية لركائز الحكومة الإلكترونية (3.92) بانحراف معياري (0.65)، وبنسبة (78.40%) ويقابل مستوى أهمية عالٍ.

ويعزو الباحث تلك النتيجة إلى أهمية دور الأمن السيبراني –الجانب الأمني– الذي بات يشكل هاجسًا وأولوية لدى المنظمات الحكومية اليمنية، سواء كان بصيغته الحالية التقليدية أم الحديثة التي بات لها حضور كبير في ظل الاستخدام المتزايد للتقنية الحديثة في المنظمات اليمنية العامة والخاصة؛ من أجل إنجاز الكثير من أعمالها الإدارية، أو تقديم خدماتها المجتمعية، وكذلك الاستخدام المجتمعي لوسائل التكنلوجيا في قضاء الكثير من احتياجاته ومتطلباته الحياتية، وهذا ما عزز الحضور الأمني لدى المنظمة الأمنية اليمنية ونهجها المتواضع، لتعزيز دورها الأمني عبر الاستعانة بالكثير من الوسائل، ولا سيما منها الوسائل التقنية الحديثة التي باتت تستعين بها الأجهزة الأمنية اليمنية بمختلف تشكيلاتها، من أجل تنفيذ الكثير من مهامها الأمنية، مما انعكس إيجابًا على دورها ورفع كفاءتها في تحقيق الأمن والاستقرار في أوساط المجتمع اليمني، بالرغم من غياب تكامل نظم المعلومات لدى المنظمات الحكومية اليمنية، وكذلك التحديات الراهنة التي تواجهها الأجهزة الأمنية اليمنية.

وتتفق نتائج الدراسة الحالية مع ما توصلت إليه دراسة القحطاني 2010 (إحدى الدراسات السابقة التي رجع إليها الباحث)، والتي تضمنت توافر تطبيق الحكومة الإلكترونية في المديرية العامة للدفاع المدني.

ثانياً: التحديات والمخاطر السيبرانية التي تواجه المنظمات اليمنية.

جدول (10) المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية لاستجابات أفراد عينة الدراسة حول التحديات والمخاطر السيبرانية التي تواجه المنظمات اليمنية

م	الفقرة	الترتيب	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	مستوى الأهمية
1	يواجه نظام الحكومة الإلكترونية في اليمن تحديات سيبرانية حقيقية تمس أمن البيانات السيادية.	1	3.90	0.84	%78.00	عالية
2	تتعرض الوثائق الرسمية والمراسلات الحكومية لمخاطر القرصنة والوصول غير المصرح به.	3	3.60	0.99	%72.00	عالية

م	الفقرة	الترتيب	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	مستوى الأهمية
3	يؤدي ضعف البنية التحتية للأمن السيبراني إلى احتمالية تعطيل الخدمات الرقمية المقدمة للجمهور.	2	3.70	0.95	%74.00	عالية
4	تشكل احتمالية اختراق والعبث ببيانات طالبي الخدمة عائقاً أمام نجاح ركائز الحكومة الإلكترونية.	4	3.45	0.97	%69.00	عالية
المتوسط الإجمالي لفقرات المحور			3.66	0.71	%73.20	عالية

بينت نتائج التحليل بالجدول (10) السابق أن المتوسطات الحسابية لاستجابات أفراد عينة الدراسة حول التحديات والمخاطر السيبرانية التي تواجه المنظمات اليمنية. تراوحت بين (3.45–3.90) وبنسبة (69.00%– 78.00%) وتمثل أهمية بمستوى عالٍ لكافة فقرات المحور، وأظهرت النتائج أن ترتيب التحديات والمخاطر السيبرانية التي تواجه المنظمات اليمنية. كانت على النحو الآتي:

حصلت الفقرة رقم (1) والتي نصها " يواجه نظام الحكومة الإلكترونية في اليمن تحديات سيبرانية حقيقية تمس أمن البيانات السيادية. " على أعلى أهمية، فقد حصلت على متوسط حسابي (3.90) بانحراف معياري (0.84) وبنسبة أهمية (78.00%)، وتقابل مستوى أهمية عالٍ.

وحصلت الفقرة رقم (3) والتي نصها " يؤدي ضعف البنية التحتية للأمن السيبراني إلى احتمالية تعطيل الخدمات الرقمية المقدمة للجمهور".على الترتيب الثاني؛ بمعنى حصلت على متوسط حسابي (3.70) بانحراف معياري (0.95) وبنسبة أهمية (74.00%)، وتقابل مستوى أهمية عالٍ.

وحصلت الفقرة رقم (2) والتي نصها " تتعرض الوثائق الرسمية والمراسلات الحكومية لمخاطر القرصنة والوصول غير المصرح به" على الترتيب الثالث؛ أي حصلت على متوسط حسابي (3.60) بانحراف معياري (0.99) وبنسبة أهمية (72.00%)، وتقابل مستوى أهمية عالٍ.

وحصلت الفقرة رقم (4) والتي نصها "تشكل احتمالية اختراق والعبث ببيانات طالبي الخدمة عائقاً أمام نجاح ركائز الحكومة الإلكترونية" على الترتيب الرابع، فقد حصلت على متوسط حسابي (3.45) بانحراف معياري (0.97) وبنسبة أهمية(69.00%)، وتقابل مستوى أهمية عالٍ.

وإجمالًا كان المتوسط العام لاستجابات أفراد عينة الدراسة على التحديات والمخاطر السيبرانية التي تواجه المنظمات اليمنية. (3.66) بانحراف

معياري (0.71)، وبنسبة (73.20%) ويقابل مستوى أهمية عالٍ.

ويعزو الباحث ذلك إلى وجود تحديات أمنية تواجهها ركائز الحكومة الإلكترونية الراهنة المرتبطة بالتطور التكنولوجي، ولا سيما التحديات السيبرانية، والجريمة الإلكترونية، والجريمة المنظمة، ومدى انعكاس تلك التحديات على المنظمات الحكومية اليمنية، بالإضافة إلى تأخر المنظمات الحكومية اليمنية– بما فيها المنظمة الأمنية– في تبني وحدات متخصصة وسياسات أمنية واضحة لمجابهة تلك التهديدات الأمنية المتعلقة بالجانب الإلكتروني، والتي باتت تدق ناقوس الخطر في أوساط المنظمات وانعكاس ذلك على الثقافة الأمنية لدى المجتمع اليمني.

وتتفق نتائج الدراسة الحالية مع ما توصلت إليه دراسة عباس، 2024 الحميري 2021 ، فقد توصلتا إلى أن مخاطر تكنولوجيا المعلومات لها أهمية سلبية غير مباشرة في أمن نظم المعلومات.

ثالثاً: واقع ركائز الحكومة الإلكترونية في اليمن ومتطلبات حمايتها سيبرانياً:

على الرغم من الإمكانات الهائلة التي توفرها الحكومة الإلكترونية، إلا أنها تواجه العديد من التحديات التي تعيق تطبيقها بنجاح. من البنية التحتية الرقمية المحدودة إلى التحديات الثقافية والمؤسساتية، ويواجه هذا التحول عقبات كبيرة. وهذ ما سوف نوضحه من خلال الآتي:

أ- مجالات ركائز الحكومة الإلكترونية(الواقع والمستقبل).

ب- الحماية السيبرانية كمعالج لمعوقات تطبيق نظام الحكومة الإلكترونية.

1- المجالات التي تطبق ركائز الحكومة الإلكترونية حاليًا (المستهدفة بالحماية):

جدول (11) المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية لاستجابات أفراد عينة الدراسة حول المجالات التي تطبق ركائز الحكومة الإلكترونية حاليًا

م	الفقرة	الترتيب	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	مستوى التطبيق
1	يستلم موظفو الدولة مرتباتهم عبر البريد.	3	3.84	1.09	%76.80	عالية
2	يحصل المواطن على بعض الخدمات عبر البوابة الإلكترونية، مثل: سداد فواتير الكهرباء، والغاز، ودفع الضريبة والرسوم الجمركية.	1	4.14	0.80	%82.80	عالية
3	يحصل المواطن على بعض الخدمات المرورية، مثل: معرفة المخالفات، والإرشادات المرورية.	2	3.99	0.89	%79.80	عالية
4	تقدم الحكومة الإلكترونية خدمات الصناعة والتجارة(السجل التجاري، تسجيل وقيد الوكالات التجارية، تسجيل وقيد أسماء المنشآت التجارية...إلخ).	4	3.70	0.94	%74.00	عالية

5	تقدم الحكومة الإلكترونية خدمات التعليم بنسبة محدودة (البحث العلمي، التعليم الفني والتدريب المهني، الجامعة المفتوحة... إلخ).	5	3.65	0.97	%73.00	عالية
المتوسط الإجمالي لفقرات المحور			**3.86**	**0.68**	**%77.20**	**عالية**

بينت نتائج التحليل بالجدول (11) السابق أن المتوسطات الحسابية لاستجابات أفراد عينة الدراسة حول المجالات التي تطبق ركائز الحكومة الإلكترونية حاليًا، تراوحت بين (3.65 -4.14) وبنسبة (73.00% -82.80%)، وأن مستوى التطبيق الحالي لركائز الحكومة الإلكترونية في المنظمات السيادية اليمنية جاء بدرجة (عالية) لكافة فقرات المحور، بمتوسط إجمالي (3.86). وقد تصدر مجال سداد الفواتير والرسوم العامة الترتيب الأول بمتوسط حسابي (4.14)، يليه مجال الحصول على بعض الخدمات المرورية بمتوسط حسابي (3.99) ومن ثم مجال صرف المرتبات والمستحقات بمتوسط (3.84). وتشير هذه النتائج إلى أن التحول الرقمي الحالي يتركز بشكل أساسي في الركائز المالية والخدمية، مما يضع عبئاً حيوياً على أنظمة الأمن السيبراني لضمان حماية هذه التدفقات المالية والبيانات الشخصية للموظفين والمواطنين من أي اختراقات محتملة.

وكما يعزو الباحث تلك النتيجة إلى نهج عدد من المنظمات الحكومية اليمنية إلى أتمتة عملها الإداري والكثير من الخدمات التي تقدمها للمجتمع، سواء كان ذلك بالشكل الجزئي أم المكتمل، وكذلك تعامل الكثير من العاملين بتلك المنظمات مع النظام الإلكتروني للقيام بواجباتهم تجاه أفراد المجتمع المتردد على تلك المنظمات لطلب خدماتها التي تقدمها.

2- المجالات التي يمكن أن تطبق فيها ركائز الحكومة الإلكترونية مستقبلاً (المستهدفة بالحماية):

جدول (12) المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية لاستجابات عينة الدراسة حول المجالات التي يمكن أن تطبق فيها ركائز الحكومة الإلكترونية مستقبلاً

م	الفقرة	الترتيب	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	إمكانية التطبيق
1	يمكن أن يحصل المواطن عبر البوابة الإلكترونية الحكومية على خدمات الأحوال المدنية (شهادة الميلاد، البطاقة الشخصية، البطاقة العائلية، وثيقة قيد الزواج، وثيقة قيد الطلاق، شهادة الوفاة...).	4	3,92	1,02	%78.40	عالية
2	يستطيع المواطن الحصول على جواز سفر عبر البوابة الإلكترونية.	9	3,74	1,15	%74.80	عالية

م	الفقرة	الترتيب	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	إمكانية التطبيق
3	بإمكان المواطن أن يحصل عبر البوابة الإلكترونية الحكومية على خدمات المرور (رخصة قيادة، كرت الملكية، تسديد المخالفات والغرامات المرورية...).	5	3,90	0,97	%78.00	عالية
4	يستطيع المواطن تقديم البلاغات الأمنية و الشكاوي وطلب النجدة والإغاثة عبر النافذة الإلكترونية.	3	3,96	0,97	%79.20	عالية
5	يمكن أن تتوفر بعض الخدمات القضائية عبر النافذة الإلكترونية، فيحصل عليها الموطن في أي وقت.	7	3,85	1,02	%77.00	عالية
6	يمكن أن تقدم بعض الخدمات الاجتماعية عبر الحكومة الإلكترونية (التوظيف، التأمينات، والرعاية الاجتماعيين للمتقاعدين...).	1	4,04	0,90	%80.80	عالية
7	يمكن أن تقدم الحكومة الإلكترونية الخدمات الصحية (مثل العلاج، التأمين الصحي، خدمات المستشفى).	8	3,80	1,04	%76.00	عالية
8	يستطيع مديرو الأعمال مستقبلًا استخراج كافة الوثائق التي تحدد نوع الاستثمارات المتاحة في الدولة، وشروط الاستثمار ومزاياه، وذلك عبر البوابة الإلكترونية.	2	4,02	0,81	%80.40	عالية
9	يمكن تطبيق نظام الحكومة الإلكترونية في مجال توفير السلع الحكومية، وسداد قيمتها، ومنح القروض.	6	3,86	0,87	%77.20	عالية
المتوسط الإجمالي لفقرات المحور			**3,90**	**0,72**	**%78.00**	**عالية**

بينت نتائج التحليل بالجدول (12) السابق أن المتوسطات الحسابية لاستجابات أفراد عينة الدراسة حول المجالات التي يمكن أن تطبق فيها ركائز الحكومة الإلكترونية مستقبلاً (المستهدفة بالحماية). تراوحت بين (3.74–4.04) وبنسبة (74.80%– 80.80%) وتمثل إمكانية تطبيق بمستوى عالٍ لكافة فقرات المحور وبمتوسط إجمالي (3.90). وقد جاءت الخدمات الاجتماعية والمساعدات بمتوسط (4.04)، تليها مجالات استثمارات الدولة بمتوسط (4.02). وتعكس هذه النتائج وعياً بأهمية التحول الرقمي الشامل، مع ضرورة اقتران هذا التوسع

بآليات حماية سيبرانية استباقية لضمان سلامة البيانات السيادية في هذه القطاعات الحيوية. ويؤكد الباحث أن التوسع نحو "تقديم البلاغات الأمنية" و"استخراج الوثائق السيادية" مستقبلاً يضع الأمن السيبراني في قلب العملية، حيث تصبح الحماية من تزوير الهوية الرقمية أو تسريب البلاغات الأمنية هي الركيزة الأساسية لنجاح هذه الخدمات.

وتتفق نتائج الدراسة مع ما توصلت إليه دراسة حوادسي2015 (إحدى الدراسات السابقة التي رجع إليها الباحث)، التي أثبتت أن الحكومة الإلكترونية في هذه المرحلة العصرية ضرورة حتمية للدولة الساعية إلى تحقيق الكفاءة والفاعلية في تقديم خدماتها.

ب- الحماية السيبرانية كمعالج لمعوقات استدامة ركائز الحكومة الإلكترونية.

1-معوقات استدامة ركائز الحكومة الإلكترونية (المستهدفة بالحماية):

جدول (13) المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية لاستجابات أفراد عينة الدراسة حول معوقات استدامة ركائز الحكومة الإلكترونية

م	الفقرة	الترتيب	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	مستوى العائق
1	غياب تشريعات يمنية كافية لتنظيم كيفية تطبيق الحكومة الإلكترونية.	2	4.08	0.94	%81.60	**عالٍ**
2	تأخير تقديم الخدمات للناس في حالة انقطاع الإنترنت أو عطل في الحواسيب.	1	4.11	0.93	%82.20	**عالٍ**
3	ظاهرة الفساد المالي والإداري تعيق تطبيق نظام الحكومة الإلكترونية.	4	3.99	0.98	%79.80	**عالٍ**
4	ارتفاع نسبة الأمية الرقمية في أوساط المجتمع اليمني، يعيق تطبيق نظام الحكومة الإلكترونية.	3	4.04	0.99	%80.80	**عالٍ**
5	لا تمتلك الحكومة اليمنية الكوادر البشرية المؤهلة والكافية لتطبيق نظام الحكومة الإلكترونية.	8	3.30	1.25	%66.00	**متوسط**
6	الخوف من التغيير في أوساط بعض الموظفين يسهم في إعاقة تطبيق نظام الحكومة الإلكترونية.	7	3.58	0.98	%71.60	**عالٍ**

م	الفقرة	الترتيب	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	مستوى العائق
7	عدم توفر البنية التحتية المناسبة لتطبيق نظام الحكومة الإلكترونية.	6	3.80	1.03	%76.00	عالٍ
8	عدم توفر نظام الحماية السيبرانية للبيانات والمعلومات يعيق تطبيق نظام الحكومة الإلكترونية.	5	3.90	1.03	%78.00	عالٍ
المتوسط الإجمالي لفقرات المحور			**3.85**	**0.70**	**%77.00**	**عالٍ**

بينت نتائج التحليل بالجدول (13) السابق أن المتوسطات الحسابية لاستجابات أفراد عينة الدراسة حول معوقات استدامة ركائز الحكومة الإلكترونية تراوحت بين (3.30– 4.11) وبنسبة (66,00%– 82,80%) وتمثل معوقات بمستوى متوسط إلى عالٍ لكافة فقرات المحور، حيث تصدرت المعوقات التقنية والتشريعية بمتوسطات بلغت (4.11) و (4.08) على التوالي. وتتمثل أبرز هذه التحديات في ضعف البنية التحتية للاتصالات وغياب قانون خاص بجرائم المعلوماتية، مما يعكس حاجة المنظمات (المؤسسات) السيادية اليمنية لبيئة قانونية وتقنية تحمي التحول ارقمي من التهديدات السيبرانية.

كما جاء عدم توفر نظام الحماية السيبرانية للبيانات كعائق أساسي بمتوسط (3.90). وبالربط مع عائق غياب التشريعات الكافية (4.08)، يستنتج الباحث أن التحدي الأكبر في اليمن ليس تقنياً فحسب، بل هو تحدي بيئة آمنة ومنظمة. فبدون تشريعات تحمي الفضاء السيبراني وتوفر أنظمة دفاعية، تظل ركائز الحكومة الإلكترونية عرضة للتهديدات المستمرة.

وتتفق نتائج الدراسة الحالية مع ما توصلت إليه دراسة طواهير، 2023 ودراسة القحطاني 2021 (إحدى الدراسات السابقة اليمنية التي تم رجوع الباحث إليها)، من ضعف دعم الإدارة العليا لسياسة الأخذ بتطبيقات الحكومة الإلكترونية، وتدني قدرة مهارات العاملين في التعامل مع التكنولوجيا الحديثة التي منها أجهزة إلكترونية في العمل الإداري.

2– معالجة معوقات استدامة ركائز الحكومة الإلكترونية (الأمن السيبراني كآلية حماية):

جدول (14) المتوسطات الحسابية والانحرافات المعيارية والنسب المئوية لاستجابات عينة الدراسة حول معالجة معوقات استدامة ركائز الحكومة الإلكترونية

م	الفقرة	الترتيب	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	يسهم بمستوى
1	سن التشريعات الإلكترونية الكافية التي تنظم الحكومة الإلكترونية.	5	4,28	0,75	%85,60	عالٍ جدًا
2	القيام بالإصلاح الإداري والمالي قبل وأثناء تطبيق نظام الحكومة الإلكترونية.	7	4,23	0,78	%84,60	عالٍ جدًا

م	الفقرة	الترتيب	المتوسط الحسابي	الانحراف المعياري	النسبة المئوية	يسهم بمستوى
3	ضرورة التأهيل والتدريب النوعي للموظفين الذين سيوكل إليهم تطبيق نظام الحكومة الإلكترونية.	1	4,48	0,69	%89,60	عالٍ جدًا
4	تساعد تنمية الوعي الوظيفي والمجتمعي في تطبيق نظام الحكومة الإلكترونية.	8	4,22	0,73	%84.40	عالٍ جدًا
5	إنشاء جهاز أمني متخصص يوفر الحماية السيبرانية للبيانات والمعلومات، ويعزز تطبيق نظام الحكومة الإلكترونية.	2	4,46	0,71	%89.20	عالٍ جدًا
6	تحديث البنية التحتية للاتصالات التي تساعد على تطبيق نظام الحكومة الإلكترونية بشكل أوسع.	3	4,37	0,75	%87.40	عالٍ جدًا
7	تبادل الخبرات مع الدول الأخرى وبما يخدم تطبيق نظام الحكومة الإلكترونية.	4	4,30	0,75	%86.00	عالٍ جدًا
8	تبني استراتيجية مزمنة لتطبيق الحكومة الإلكترونية.	9	4,16	0,77	%83.20	عالٍ
9	إنشاء هيئة مختصة بتطبيق نظام الحكومة الإلكترونية والأمن السيبراني.	6	4,24	0,80	%84.80	عالٍ جدًا
المتوسط الإجمالي لفقرات المحور			**4,30**	**0,54**	**%86.00**	**عالٍ**

بينت نتائج التحليل بالجدول (14) السابق أن المتوسطات الحسابية لاستجابات أفراد عينة الدراسة حول معالجة معوقات استدامة ركائز الحكومة الإلكترونية (الأمن السيبراني كآلية حماية) (4.16– 4.48) وبنسبة (83.20%– 89.60%)، فمثلت إسهام بالمعالجات بمستوى عالٍ إلى عالٍ جدًا لكافة فقرات المحور، وقد حلت "ضرورة التأهيل والتدريب النوعي للموظفين الذين سيوكل إليهم تطبيق نظام الحكومة الإلكترونية" أعلى وسيلة لمعالجة معوقات استدامة ركائز الحكومة الإلكترونية، فقد حصلت على متوسط حسابي (4.48) تلاها "إنشاء جهاز أمني متخصص يوفر الحماية السيبرانية للبيانات والمعلومات، ويعزز تطبيق نظام الحكومة الإلكترونية" بمتوسط حسابي (4.46). وتؤكد هذه النتائج أن الحل الجذري لاستدامة الركائز الرقمية في اليمن يكمن في أن الأمن السيبراني هو الآلية الحتمية والمدخل الوحيد لمعالجة معوقات الحكومة الإلكترونية في اليمن وضمان حماية ركائزها. وفي إيجاد غطاء قانوني

ومؤسسي يحمي الخدمات السيادية التي تقدمها الحكومة الإلكترونية من الهجمات المتطورة.

وتتفق نتائج الدراسة الحالية مع ما توصلت إليه دراسة العنوز 2024، في أن تطبيق الحكومة الإلكترونية يتطلب إعادة هيكلة الأدوات بما يلائم متطلبات تطبيقها، ومع ما توصلت إليه دراسة حوادسي2015 التي أشارت إلى أن من معالجات المعوقات هو الاستفادة من التجارب السابقة للدول الأخرى التي تطبق برنامج الحكومة الإلكترونية، ودراسة أهم نقاط الضعف ومحاولة تجنبها، وإبراز نقاط القوة والاستفادة منها.

تحليل النتائج ومناقشتها:

تُشير القراءة التحليلية لنتائج الدراسة الميدانية إلى وجود ترابط عضوي بين وعي أفراد العينة بآليات الأمن السيبراني وواقع تطبيق الحكومة الإلكترونية في اليمن، ويمكن تفصيل هذا التكامل وفقاً للآتي:

1. الأمن السيبراني كضمانة لاستدامة الخدمات الرقمية الحالية:

كشفت النتائج أن الخدمات الأكثر نضجاً في الواقع اليمني هي سداد الفواتير (4.14) واستلام المرتبات (3.84). وبالربط مع المحور الأول، نجد أن هذه الخدمات هي التي قصدها أفراد العينة حين منحوا فقرة توفير بيئة آمنة تضمن استدامة التحول متوسطاً قدره (3.91). ويرى الباحث أن هذا الدمج يثبت أن نجاح الرقمنة المالية في اليمن مرهون كلياً بآليات الحماية السيبرانية التي تمنع توقف هذه الخدمات السيادية أو اختراق خصوصية بيانات الموظفين والمواطنين.

2. الحماية السيبرانية كآلية لمواجهة معوقات البنية التحتية:

أظهرت نتائج المحور الثاني أن ضعف البنية التحتية والتشريعات يمثل عائقاً رئيساً بمتوسط (3.82). وهنا تبرز أهمية فقرات المحور الأول الـ (12)؛ حيث منح أفراد العينة القدرة على التنبؤ بالهجمات أهمية نسبية قدرها (77.20%). وهذا يعني أن الكادر اليمني يرى في الأمن السيبراني الاستباقي الوسيلة الأنجع لمعالجة فجوات البنية التحتية، وتحويلها من نقاط ضعف إلى نقاط قوة محمية ببروتوكولات تشفير وتحقق رقمي عالية.

3. أثر الأمن السيبراني في بناء الثقة الاجتماعية بالمجالات المستقبلية:

عند تحليل التطلعات المستقبلية (كالتصويت الإلكتروني وإصدار الوثائق الشخصية)، نجد ارتباطاً وثيقاً بفقرة المحور الأول المتعلقة بتعزيز الثقة الاجتماعية (3.66). ويخلص الباحث إلى أن التوسع في ركائز الحكومة الإلكترونية في اليمن لن يكتب له النجاح ما لم يرتكز على آلية حماية سيبرانية تحمي الهوية الرقمية من التزوير، وهو ما أكدته نتائج المحور.

وفي ختام هذه الدراسة، يمكن القول إن الانتقال نحو الحكومة الإلكترونية في اليمن لم يعد مجرد مشروع تقني لتطوير الأداء، بل هو ضرورة استراتيجية تفرضها التحديات الراهنة. وقد أثبتت النتائج الميدانية أن الأمن السيبراني يمثل العمود الفقري الذي يحمي هذا التحول؛ فبدون بيئة سيبرانية آمنة، تظل الخدمات السيادية –كصرف المرتبات وسداد الفواتير– عرضة للانهيار أو القرصنة، مما قد يؤدي إلى فقدان الثقة الاجتماعية بالمنظومة الحكومية برمتها.

وتكمن القيمة المضافة لهذا البحث في تقديمه نموذجاً يربط بين 'آليات الحماية السيبرانية ومعوقات الواقع الميداني في الوزارات اليمنية الأكثر حساسية (الداخلية، المالية، الاتصالات، والضرائب). وبذلك، فإن الدراسة تضع أمام صناع القرار في اليمن خارطة طريق عملية؛ تبدأ من تأمين البنية التحتية القائمة، وتنتهي ببناء سيادة رقمية قادرة على استيعاب التطلعات المستقبلية كالتصويت الإلكتروني والهوية الرقمية، بما يضمن استدامة الخدمات وحماية حقوق المواطنين في ظل أصعب الظروف.

الخاتمــة:

واشتملت على الآتي:

نتائج الدراسة:

– أثبتت الدراسة الميدانية أن الأمن السيبراني يمثل الركيزة الأساسية والضمانة الحقيقية لاستمرارية تقديم الخدمات عبر الحكومة الإلكترونية في المنظمات اليمنية (بمتوسط 3.92).

– هناك وعي جمعي لدى الكوادر في وزارات (الاتصالات، المالية، والضرائب) بأن الرقمنة لا تكتمل إلا بوجود منظومة دفاع سيبراني تحمي الهوية الرقمية والوثائق الرسمية من التزوير.

– كشفت النتائج عن وجود تحديات سيبرانية حقيقية ومخاطر قرصنة (بمتوسط 3.66) تهدد الأمن القومي والبيانات السيادية، مما يستدعي الانتقال من الحلول التقنية التقليدية إلى استراتيجيات الأمن الاستباقي.

– أظهرت النتائج أن حماية بيانات المواطنين وسريتها هي المحرك الأساسي لتعزيز (الثقة الاجتماعية) في التعاملات الإلكترونية، مما يربط الأمن السيبراني بالأهداف الاجتماعية للدولة.

– بينت الدراسة أن الركيزة الأكثر نضجاً هي سداد الفواتير والرسوم بمتوسط (4.14)، تليها الخدمات المرورية وصرف المرتبات.

– أكدت الدراسة أن غياب التشريعات السيبرانية المنظمة وتأخر الخدمات عند الأعطال التقنية هي أبرز العوائق بمتوسطات تتجاوز (4.00).

– أجمعت العينة بمستوى "عالٍ جداً" على أن الحل يكمن في إنشاء هيئة مختصة بالأمن السيبراني وتأهيل الكوادر وتحديث البنية التحتية.

التوصيات:

هناك عدد من التوصيات الإجرائية التي توصلت إليها الدراسة:

– الإسراع في صياغة استراتيجية وطنية للأمن السيبراني خاصة بالمنظمات الحكومية اليمنية، تعمل كآلية حماية لركائز الحكومة الإلكترونية ضد هجمات القرصنة المتزايدة.

– إنشاء وحدات إدارية وتقنية متخصصة داخل الوزارات السيادية (الاتصالات والمالية) لضمان مراقبة البيانات وحمايتها على مدار الساعة.

– تكثيف برامج التدريب والتوعية للكوادر البشرية حول مخاطر الهندسة الاجتماعية وأساليب حماية البيانات، باعتبار العنصر البشري هو خط الدفاع الأول في منظومة الأمن السيبراني.

– ضرورة تحديث التشريعات القانونية اليمنية لتشمل عقوبات رادعة لجرائم الفضاء السيبرانية لحماية

التعاملات الرقمية السيادية، وبما يضمن حقوق طالبي الخدمة ويحمي بياناتهم من الاختراق والعبث.

– إنشاء مركز وطني للأمن السيبراني يتولى حماية بوابات دفع الفواتير وصرف المرتبات لضمان عدم توقفها.

– استباق التوسع في الخدمات المستقبلية (كالهوية الرقمية) بوضع بروتوكولات حماية مشددة تمنع تزوير البيانات الشخصية.

قائمة المراجع والمصادر

أولاً: المراجع باللغة العربية:

[1] العزب، حسين. (2018). **المتطلبات الإدارية للأتمتة لتطبيق الحكومة الإلكترونية وأثرها في جودة الخدمات المقدمة من جهة الخدمة المدنية من وجهة نظر العاملين**. جامعة مؤتة، كلية إدارة الأعمال قسم الإدارة العامة، مجلة المنارة، مجلد24، عدد1.

[2] الشمري، فهد. (2020). **استراتيجيات الأمن السيبراني في العصر الرقمي**. دار المناهج، عمان.

[3] القحطاني، محمد. (2021). **الأمن السيبراني في المنظمات الحكومية: استراتيجيات الحماية والمواجهة**. دار المسيرة للنشر والتوزيع، عمان.

[4] الزبيدي، عبدالله. (2022). **حوكمة التحول الرقمي في المؤسسات العامة**. المركز العربي للبحوث والدراسات، القاهرة.

[5] حسين، مريم خالص. (2013). **الحكومة الإلكترونية**. بحث منشور، مجلة كلية بغداد للعلوم الاقتصادية الجامعية، العدد الخاص بمجموعة الكلية، بغداد.

[6] عبدالنبي، زين الدين عابد. (2008). **العلاقة بين تطبيق الحكومة الإلكترونية الفلسطينية المرجوة والأداء من منظور الوكلاء والمديرين العامين**. رسالة ماجستير منشورة، إدارة أعمال، الجامعة الأردنية، الأردن.

[7] كافي، مصطفى يوسف. (2009). **الحكومة الإلكترونية في ظل الثورة العلمية التكنولوجية المعاصرة**. دار مؤسسة رسلان للطباعة والنشر والتوزيع، دمشق، سوريا.

[8] بو مروان، سمية. (2014). **الحكومة الإلكترونية ودورها في تحسين أداء الإدارات الحكومية (دراسة مقارنة)**. مكتبة القانون والاقتصاد، المغرب، ط1.

[9] إبراهيم ناصر، إبراهيم. (بدون تاريخ). **علم الاجتماع التربوي**. مكتبة الرائد العلمية، عمان–الأردن، دار الجيل، بيروت–لبنان.

[10] غيدان، سري غضبان، ومحمد منذر جلال الربيعي . (2020). **الامن السيبراني وسياسات المواجهة الدولية**. بحث منشور، في مجلة الدراسات الاستراتيجية والعسكرية المركز الديمقراطي العربي – برلين، المجلد الثاني– العدد التاسع، ديسمبر.

[11] جبور، منى الأشقر. (2012). **الأمن السيبراني التحديات ومستلزمات المواجهة**. اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني، جامعة الدول العربية: المركز العربي للبحوث القضائية والقانونية، بيروت، أغسطس27–28.

[12] صائغ، بنت حسن عبدالوهاب. (2018). **وعي أفراد الاسرة بمفهوم الامن السيبراني وعلاقته باحتياطاتهم الأمنية من الجرائم الإلكترونية**. المجلة العربية للعلوم الاجتماعية، المؤسسة العربية للاستشارات العلمية وتنمية الموارد البشرية ع 14، م 3.

[13] الديحاني، ناصر سعيد على محسن. (2021). **متطلبات تطبيق الأمن السيبراني في الجامعات اليمنية من وجهة نظر الخبراء**. مجلة الجامعة الوطنية، اليمن، ع18.

[14] حميد، إسماعيل عبدالله حسن. (2021). **الأمن السيبراني**. صنعاء، الجيل الجديد ناشرون، ط1.

[15] **الاستراتيجية الوطنية للأمن السيبراني(2014).** وزارة الاتصالات وتكنولوجيا المعلومات، قطر.

[16] البشير، آمنة علي البشير. (بدون تاريخ). **الأمن السيبراني في ضوء مقاصد الشريعة.** بحث منشور بمجلة كلية الدراسات الإسلامية بالإسكندرية، مصر، م1، ع 37.

[17] المرشد، سامي البشير. (2009). **دليل الأمن السيبراني للبلدان النامية.** الاتحاد الدولي للاتصالات.

[18] الأمم المتحدة. (2015). **الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية توصيات سياساتية.** اللجنة الاقتصادية والاجتماعية لغربي آسيا (الإسكوا)، نيويورك.

[19] تقديرات الاتحاد الدولي للاتصالات. 1524. **قياس مجتمع المعلومات.** ISBN 978-92-61-15291-8.

[20] كلارك، ريتشارد، وروبرت .(2011). **حماية الفضاء الإلكتروني في دول مجلس التعاون الخليجي.** مركز الإمارات للدراسات والبحوث الاستراتيجية، سلسلة محاضرات، الإمارات، ط1.

[21] هيئة الأمم المتحدة. (بدون تاريخ). **العنف ضد المرأة في الفضاء الرقمي – رؤى من دراسة متعددة الأقطار في الدول العربية.**

[22] اتحاد المصارف العربية. (2018). الأمانة العامة، إدارة الدراسات والبحوث، **أمن المعلومات المخاطر وتحديات المستقبل.**

[23] اللوزي، إبراهيم عبدالله. (2020). **تحليل المعلومات ودوره في دعم العمل الأمني.** بحث لاستكمال متطلبات الحصول على درجة دبلوم الأمن العام، كلية الدراسات العليا، أكاديمية الشرطة، اليمن، صنعاء.

[24] أصلان، كمال. (2024). **تداعيات الهجوم السيبراني على لبنان والمنطقة.** مقال منشور، موقع الشرق الإخباري، 23 سبتمبر 2024.

[25] فوزي، إسلام. (2019). **الأمن السيبرانى (الأبعاد الاجتماعية والقانونية تحليل سوسيولوجى).** المجلة الاجتماعية القومية، مصر، م 56، ع 2.

[26] قرني، أماني حمدي. (2022). إيمان عبد المنعم خطاب، **دور مواقع الإعلام الرقمي في حماية الأمن السيبراني (دراسة تحليلية لعينة من المواقع الخاصة بالأمن السيبراني).** المجلة المصرية لبحوث الإعلام، مصر، ج 2، ع 80.

[27] عبد الجبوري، سامر سلمان. (2014) . **جريمة الاحتيال الإلكتروني- دراسة مقارنة.** رسالة ماجستير، قسم القانون العام، كلية الحقوق، جامعة النهرين، العراق.

[28] العنوز، سوزان. (2024). **دور الأمن السيبراني في التقليل من أعداد الجرائم الإلكترونية في محافظة العقبة- باستخدام نظم المعلومات الجغرافية.** بحث منشور. Journal of Human and Social Sciences (JHSS) •.

[29] طواهير، عبدالجليل.(2023). **استراتيجيات الأمن السيبراني كتحدي للتحول الرقمي بالمنظمات الحكومية مع الإشارة لتجربة دولة الإمارات العربية المتحدة.** مجلة الرسالة للدراسات الإعلامية، م7، ع1.

[30] خليل، مولاي و شنوفي، نور الدين. (2021). **الحكومة الإلكترونية كمدخل لتحقيق جودة الخدمة العمومية-الحكومة الإلكترونية في البحرين إنموذجاً.** الأكاديمية للدراسات الاجتماعية والإنسانية، م13، ع1.

[31] الحميري، نبيل حسان. (2021). **أثر مخاطر تكنولوجيا المعلومات في أمن نظم المعلومات**

المحاسبية من خلال الضوابط الأمنية (دراسة ميدانية في شركات الاتصالات العاملة في اليمن). رسالة دكتوراه منشورة، جامعة العلوم والتكنولوجيا، اليمن.

[32] حوادسي، زينب. (2015). **أثر تطبيق الحكومة الإلكترونية على تحسين أداء الموارد البشرية(دراسة حالة بلدية عين مليلة)**. رسالة ماجستير منشورة، قسم إدارة أعمال، كلية العلوم الاقتصادية والعلوم التجارية وعلوم التيسير، جامعة أم البواقي، الجزائر.

[33] عباس، سجى فاضل. (2024). **الحوكمة الرقمية في ظل تهديدات الأمن السيبراني: دولة الامارات انموذجاً**. بحث منشور، مجلة حمورابي للدراسات، ع49.

[34] القحطاني، نورة بنت ناصر.(2021). **مدى توفر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي – دراسة ميدانية**. بحث منشور في المنهل للبحوث الدراسات، الشارقة.

[35] غيدان، سري غضبان، ومحمد منذر جلال الربيعي .(2020) .**الامن السيبراني وسياسات المواجهة الدولية**. دراسة منشورة، مجلة الدراسات الاستراتيجية والعسكرية المركز الديمقراطي العربي – برلين، المجلد الثاني– العدد التاسع، ديسمبر.

[36] حجازي، عبد الفتاح بيومي. (بدون تاريخ). **الحكومة الإلكترونية ونظامها القانوني**. دار الفكر الجامعي، الإسكندرية.

[37] كمال، حوشين، وهارون سميرة. (2014). **دور الإدارة المؤسساتية في تحسين جودة الخدمة العامة.** الملتقى العلمي الدولي حول: جودة الخدمة العامة في ظل الحوكمة الإلكترونية دراسة حالة البلدان العربية.

[38] المهتدي، سوسن زهير. (2011). **تكنولوجيا الحكومة الإلكترونية**. الأردن، دار أسامة.

[39] ابن منظور، محمد بن مكرم بن علي .(1414هـ). **لسان العرب**. ط 3، دار صادر، بيروت، ج13.

[40] بخيت، صالح. (2021). **الحكومة الإلكترونية: الرؤية والآليات**. مكتبة المتنبي، الدمام–السعودية.

[41] عبيدات، ذوقان، وآخرون. (2001). **البحث العلمي مفهومه وأدواته وأساليبه**. دار الفكر للطباعة والنشر والتوزيع، عمّان، الأردن، ط7.

[42] دحماني، سليم. (2018). **أثر التهديدات" السيبرانية "على الأمن القومي الولايات المتحدة الأمريكية – أنموذجا**– 2001–2017 رسالة ماجستير غير منشورة، جامعة محمد بوضياف – المسيلة، كلية الحقوق والعلوم السياسية، قسم العلوم السياسية، الجزائر.

[43] صائغ، بنت حسن عبدالوهاب. (2018). **وعي أفراد الأسرة بمفهوم الأمن السيبراني وعلاقته باحتياطاتهم الأمنية من الجرائم الإلكترونية**. المجلة العربية للعلوم الاجتماعية المؤسسة العربية للاستشارات العلمية وتنمية الموارد البشرية ع 14م (3).

ثانياً: المراجع باللغة الأجنبية:

[1] Richard A. Kemmerer(2003), Cyber security, University of California Santa Barbara, Department of Computer Science

[2] ITU,(2012) Marco Gercke, Understanding Cybercrime: Phenomena, Challenges and Legal Response. September.

[3] University of Mississippi, School of Law, National Center for Justice and the 4. Rule of law, Combating cyber, crimeessential tools and effective organizational structures, A guide for policy makers and managers, CyberCrimebooklet.pdf.

[4] United Nations(2013), Office on Drugs and Crime,

[5] Net Losses;(2014) Estimating the Global cost of Cybercrime. Economic Impact of Cybercrime11. Report Summary. Intel http://.www.macfee.com.

[6] Schjolberg, Stein,(2008) The History of Global Harmonization Cybercrime Legislation - The Road to Geneva, December http://www.cybercrimelaw.net/documents/

[7] Hair, H. J. Explatory factor analysis: A review of research from 1993 to 2003.