Electronic Media Cybersecurity Strategies in Kuwait

Mutlaq Saad Alomairi *

Abstract

The study aims to know the strategies of the electronic media in Kuwait towards cybersecurity, and to study the differences between them according to the personal variables of the sample to achieve cybersecurity. The need for the study has emerged, not only because these cyber-piracy is launched by individuals but also because there are companies that specialize in this. Thus, there is an urgent need to control these attacks and get rid of their consequences. This is what the State of Kuwait seeks to achieve. In order to achieve this goal, the descriptive approach has been adopted, and a questionnaire has been built as a tool for data collection. The research sample consisted of 150 individuals working in Kuwaiti electronic newspapers, the Kuwait News Agency (KUNA), and Kuwaiti government media websites and those in charge of them.

The study has made several conclusions, the most important of which is that the schemes employed by the electronic media towards cyber security came at a high level. This reflects the increase in the schemes employed by the electronic media in Kuwait towards cyber security, where community media training is conducted to report on websites that embody false news, uncover hotbeds and plotting of terrorist organizations, and inform the public of penalties and deterrent laws for perpetrators of cyber threats. The schemes adopted by the Kuwaiti newspapers and Kuwaiti governmental media workforce towards cybersecurity indicates a high degree use of them, as such bodies seek technical support as one of the basics of cybersecurity for administrative systems, and they may provide a special department for cybersecurity.

Among the most important recommendations: increasing the awareness of electronic media workers about the dangers of relying on personal devices, such as mobile phones to store confidential data related to work, and having a technical governance system to provide cyber security for electronic transactions, and tightening penalties for cyberspace crimes, and more technical support must be provided as one of fundamentals for achieving cyber security of administrative data.

Keywords: schemes, media, cybersecurity, strategies, cyber-piracy.

* Assistant Professor, Ministry of Interior, Saad Al-Abdullah Academy for Security Sciences, Kuwait.
al-3mairi@hotmail.com

Submitted: 30/3/2023, **Revised**: 12/7/2023, **Accepted**: 24/7/2023.
https://doi.org/10.34120/0117-042-165-001

To cite this article/ الإشارة المرجعية للبحث

العميري، مطلق: "استراتيجيات الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني"، **المجلة العربية للعلوم الإنسانية**، جامعة الكويت: العدد 165، 2024، 11-42 .

Alomairi, Mutlaq: "ʾistrātīǧīāt al-iʿlām al-ilktrūnī fī al-kwyt tiǧāh al-ʾamn al-sībrānī", *Arab Journal for the Humanities*: 165, 2024, 11-42 .

استراتيجيات الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني

مطلق سعد العميري*

الملخص

يبتغي هذا البحث الوصول إلى معرفة الاستراتيجيات الموظفة في الإعلام الإلكتروني بالكويت تجاه الأمن السيبراني، ودراسة الفروق بينها وفقًا للمتغيرات الشخصية للعينة لتحقيق الأمن السيبراني، وقد تمثلت الحاجة البحثية الداعية لهذه الدراسة في مشكلتها التي نجمت عن كون هجمات القرصنة الإلكترونية لم تعد مقصورة على القراصنة وحدهم، بل أصبح هناك شركات متخصصة في الجرائم السيبرانية؛ ومن هنا كانت الحاجة ملحة للسيطرة على تلك الهجمات والتخلص من عواقبها والتصدي لها؛ وهذا الذي تسعى دولة الكويت لتحقيقه؛ ما يفرض دراسة الحالة الكويتية وبيان مخططاتها المضادة للقرصنة . ومن أجل تحقيق هذه الغاية جرى الاستناد إلى المنهج الوصفي وبناء الاستبانة بوصفها أداة لتحصيل البيانات، وقد تكونت عينة البحث من **150** فردًا من العاملين في الصحف الكويتية الإلكترونية ووكالة الأنباء الكويتية (كونا) والمواقع الإعلامية الحكومية الكويتية والقائمين عليها.

وقد انتهى البحث إلى عدة نتائج؛ من أبرزها:

جاءت المخططات التي يوظفها الإعلام الإلكتروني تجاه الأمن السيبراني بمستوى مرتفع؛ وهذا ينم عن ارتفاع المخططات التي يوظفها الإعلام الإلكتروني بالكويت تجاه الأمن السيبراني حيث التدريب الإعلامي المجتمعي للإبلاغ عن المواقع التي تجسد الأخبار الزائفة وكشف بؤر ومخطط المنظمات الإرهابية وتعريف الجمهور بالعقوبات والقوانين الرادعة لمرتكبي التهديدات السيبرانية، كما أن واقع استعمال العاملين في الصحافة الكويتية الإلكترونية والمواقع الإعلامية الحكومية الكويتية من مخططات تجاه الأمن السيبراني جاء مرتفعاً، وهذا يدل على ارتفاع درجة استعمال الكوادر المبحوثة للاستراتيجيات تجاه الأمن السيبراني حيث تسعى الصحف والمواقع الكويتية الإلكترونية إلى وجود الدعم الفني كأحد أساسيات الأمن السيبراني للأنظمة الإدارية وقد توفر الصحف والمواقع الكويتية الإلكترونية إدارة خاصة بالأمن السيبراني.

وخرجت الدراسة بمجموعة من المقترحات؛ أهمها: زيادة وعي العاملين بالإعلام الإلكتروني بمخاطر الاعتماد على الأجهزة الشخصية كالهواتف المحمولة لتخزين البيانات السرية المتعلقة بالعمل، وامتلاك لنظام حوكمة تقني لتوفير الأمن السيبراني للتعاملات الإلكترونية، وتشديد العقوبات على جرائم الفضاء السيبراني، ولا بد من توفير المزيد من الدعم الفني بوصفه أحد الأساسيات لتحقيق الأمن السيبراني للبيانات الإدارية.

الكلمات المفتاحية: مخططات، الإعلام، الأمن السيبراني، استراتيجيات، القرصنة الإلكترونية.

* أستاذ مساعد، وزارة الداخلية، أكاديمية سعد العبد الله للعلوم الأمنية، دولة الكويت. al-3mairi@il.com

الاستلام: 2023/3/30، **التعديل النهائي:** 2023/7/12، **إجازة النشر:** 2023/7/24.

https://doi.org/10.34120/0117-042-165-001

To cite this article/ الإشارة المرجعية للبحث

العميري، مطلق: "استراتيجيات الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني"، **المجلة العربية للعلوم الإنسانية**، جامعة الكويت: العدد 165، 2024، 11-42 .

Alomairi, Mutlaq: "'istrātīǧīāt al-i'lām al-ilktrūnī fī al-kwyt tiǧāh al-'amn al-sībrānī", *Arab Journal for the Humanities*: 165, 2024, 11-42 .

مقدمة

شهد العالم في الفترة الحالية تطورات سريعة في كافة مجالات الحياة، فقد أصبحت الحياة اليومية ترتبط باستخدام التقنيات والإنترنت، وعلى الرغم من كافة الإيجابيات الناتجة عن التقنيات المتطورة، إلا أنه ظهرت مشكلات كالجرائم السيبرانية التي تهدد الأمن الدولي والشخصي بكافة أنواعه، مما ساهم في ظهور تحديات منها الأمن السيبراني الذي يشير لحماية التطبيقات والبيانات والعمليات وحفظ المعلومات الوطنية للدولة والأفراد، والمحافظة عليها، وذلك من خلال منع الدخول غير المرخص والعبث بها، وذلك من خلال نظام فعال لحماية تلك الخدمات.

ومع زيادة الإيمان بالدور المهم الذي يحققه الإعلام الإلكتروني في تشكيل وعي المجتمع، تم وصف التطورات الحديثة التي تشهدها الوسائل المختلفة للإعلام، بأنها تعتبر طفرة كبرى ونقلة تقنية نوعية على مستوى الاتصال والإعلام وصناعة الأخبار، ويرجع ذلك للتقنيات الإعلامية المتطورة التي تم توفيرها، من خلال مشاركة الأفراد في القضايا المهمة لهم عبر نشرها والتفاعل معها ومناقشة الآخرين فيها.

وشغل الأمن السيبراني كافة دول العالم حتى أصبح جزءًا رئيسيًا من السياسات الاقتصادية والأمنية والإعلامية، وأصبح المسؤولون في الدول يهتمون بالأمن السيبراني كأولوية أساسية في سياستهم، وذلك بعدما انتشر مصطلح الأمن السيبراني بعد الهجمات المسماة "الفدية" التي استهدفت دولاً كثيرة منها الكويت، وأدت لتعطل مرافق حيوية في عديد من تلك الدول، ما جعل الأمن السيبراني أولوية حاولت المؤسسات زيادة الوعي بالأمن السيبراني وتوظيفه لمجابهة التهديدات السيبرانية المتوقعة[1].

ويعد الأمن السيبراني من أساسيات الاقتصاد الرقمي، نتيجة لزيادة الاعتماد على الأجهزة الرقمية وشبكة الإنترنت، والتقنيات الناشئة التي أصبحت جزءاً رئيسيًا من الاقتصاد في كافة دول العالم، مما يبرز ضرورة الوعي بهذه التهديدات السيبرانية وكيفية صدها بأعلى درجة من الجدية، وتفعيل منظومة الأمن السيبراني في كافة القطاعات الحيوية بالدولة، وإعداد بنية تحتية متطورة لكافة المؤسسات لحمايتها[2].

ويمكن تقسيم التهديدات السيبرانية لثلاثة أنواع أساسية، وهي: الهجمات على التوافر، وعلى النزاهة، وعلى البيانات السرية. فالهجوم على التوافر يجري لمنع المستخدمين من الوصول للبيانات الخاصة بهم لكي يقوموا بدفع فدية محددة، بينما يهدف الهجوم على النزاهة لتخريب الشخص، وذلك بكشف المعلومات لتشويش أفراد المجتمع وإفقادهم ثقة التعامل مع تلك المؤسسة، أما الهجوم الذي يستهدف البيانات لسرقة بيانات الخاصة بالحسابات وبطاقات الائتمان للاستيلاء على الأموال الخاصة بالأفراد أو المؤسسات[3].

فالهجوم السيبراني يختلف من حالة لأخرى فهو يشمل على: الانتقام، والتجسس، واستعراض القوة، وإلحاق الأضرار المادية بالخصوم... غيرها، مما يجعلها من التهديدات الخطيرة التي تستهدف الدول والمؤسسات والأفراد، وذلك نظراً لطبيعتها المتطورة والمعقدة وانخفاض تكلفتها. وقد أدت هذه العوامل لدفع الدول لزيادة الاهتمام بالأمن السيبراني في ضوء زيادة اختراق البنية الإلكترونية، مما جعل الحكومات تضع الأمن السيبراني ضمن الأولويات بهدف التصدي للمتسللين والبرمجيات المدمرة، وأي تهديدات أخرى من شأنها أن تدمر الأنظمة الإلكترونية الضعيفة[4]. واستطاعت الكويت أن تحتل المرتبة السادسة عربياً في المؤشر العالمي للأمن السيبراني، إذ وبحسب ما أعلنت عنه الهيئة العامة لتقنية المعلومات، تقدمت دولة الكويت بـ 72 مرتبة في عام 2019م لتحتل المركز السابع والستين عالمياً والسادس عربياً، وهو ما يعد قفزة نوعية بعدما كان ترتيبها 139 عالمياً في عام 2017م. ويرجع ذلك لمحاولة الدولة التغلب على تهديدات الأمن السيبراني والإعداد لها بتوظيف الخبرات الشبابية والمستشارين العالميين، وفقاً لاتفاقيات تعاون عالمية مع الدول الرائدة بمجال الأمن السيبراني[5]. وسيتخذ بحثنا هذا تجربة الإعلام الإلكتروني الكويتي نطاقاً للتطبيق فيما يخص المخططات التي يجري تطبيقها في مجال الأمن السيبراني، ومعرفة العوامل المؤثرة في مخططات الإعلام الإلكتروني تجاه الأمن السيبراني بالكويت.

مشكلة الدراسة

إن الهجمات السيبرانية لم تعد نتيجة لعمل أفراد أو مجموعات من القراصنة فقط، بل أصبح مصدر تلك الهجمات شركات متخصصة في الجرائم السيبرانية تستثمر الأموال وتتعاون في ما بينها، بالإضافة للخبرة والمعرفة والمثابرة التي ساهمت في جعل قدرات تلك الجهات أفضل من قدرات المنظمات المتخصصة في مختلف الدول ، ومن أجل التغلب على تلك المشكلة، تحاول الكويت السعي لتطوير قدراتها في تعزيز الأمن السيبراني، والعمل على تطوير التعاون والحوار بهذا المجال. وتتمحور مشكلة دراستنا حول معرفة مخططات الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني بتحليل آراء العاملين بالصحف الكويتية الإلكترونية ووكالة الأنباء الكويتية (كونا) والمواقع الإعلامية الحكومية الكويتية والقائمين عليها، وسنعالج هذه الإشكالية عبر طرح مجموعة من التساؤلات نوردها في ما يلي:

أسئلة الدراسة

- ما الاستراتيجيات التي يوظفها الإعلام الإلكتروني بالكويت تجاه الأمن السيبراني؟
- ما العوامل المؤثرة في مخططات الإعلام الإلكتروني تجاه الأمن السيبراني في الكويت؟
- هل توجد فروق بين مخططات الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني تعود للمتغيرات الشخصية لدى عينة البحث؟
- ما واقع توظيف العاملين بالصحف الإلكترونية ومواقع الإعلام الحكومي في إطار المخططات الخاصة بالأمن السيبراني في الكويت؟
- ما هي المرجعيات التي استندت إليها الصحف الإلكترونية ومواقع الإعلام الحكومي في سياق الأمن السيبراني في الكويت؟

أهمية البحث

تتأسس أهمية دراستنا هذه إذا ما أخذنا بعين الاعتبار التحولات الثلاثة الآتية:

- انخفاض عدد الأبحاث في مجال الأمن السيبراني والإعلام، على الرغم من

جهود الدولة لتنمية المجتمع والأمن القومي، بخاصة في ضوء زيادة التهديدات بمجال المجتمع الرقمي والأمن السيبراني والبحث عن سبل لمجابهة التهديدات والمخاطر المتزايدة.

- تنوع أشكال الإعلام الإلكتروني في الكويت، وأهمية رصد المخططات المستخدمة لتحقيق الأمن السيبراني.
- زيادة أهمية الأمن السيبراني نتيجة لأهمية التعامل مع المعلومات بأساليب آمنة، بتحديد التهديدات الأمنية بمجال الإعلام الإلكتروني بالكويت، والتعرف على أساليب التعامل معها باستخدام أساليب دفاعية مناسبة وتطبيقها بفاعلية وكفاءة.

أهداف الدراسة

تتحدد أهداف الدراسة فيما يلي:

- الوقوف على الاستراتيجيات التي يوظفها الإعلام الإلكتروني بالكويت تجاه الأمن السيبراني.
- بحث العوامل المؤثرة في مخططات الإعلام الإلكتروني تجاه الأمن السيبراني في الكويت.
- دراسة الفروق بين المخططات في الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني التي قد تعود للمتغيرات الديموغرافية لدى العينة المنتقاة.
- رصد واقع مخططات الصحف الإلكترونية ومواقع الإعلام الحكومي تجاه الأمن السيبراني في الكويت.
- التوصل لمعرفة المرجعيات المعتمدة لدى الإعلام الكويتي في سياق الأمن السيبراني.

تحديد المفاهيم

الأمن السيبراني

يحتوي أمن البيانات على الأجهزة الحاسوبية، ومنها مخططات صيانة البيانات وأجهزة الحاسوب من التدخلات غير المصرح بها أو إتلاف[6].

إن الأمن السيبراني يتكون من سياسات أمنية وأدوات ومبادئ توجيهية وضمانات ومناهج لإدارة المخاطر واتباع الممارسات الفعالة لحماية معلومات المستخدمين، والمتمثلة في الأجهزة والخدمات والبنية التحتية والتطبيقات وأنظمة الاتصالات عند تخزينها أو نقلها في بيئة إلكترونية، فالأمن السيبراني يظهر بتحقيق النزاهة والسرية للمعلومات بالفضاء السيبراني[7]. فالأمن السيبراني مفهوم حديث لم يكن متوافرًا في الماضي، فقد ظهر وازدادت أهميته نظرًا لارتباط الأنشطة الحياتية على مدار اليوم بالإنترنت، بسبب الحاجة لتأمين المعدات والبيانات ضد الاختراقات . ويشير اجتهاد الباحثين في الوصول لمفهوم محدد للأمن السيبراني لأهميته الكبيرة؛ إذ يفترض الأمن السيبراني أن كافة العناصر الموجودة بالبيئة والنظام المحيط تحتاج للحماية باعتبارها عرضه للاستهداف والاختراق، ويتضح الأمن السيبراني من خلال محاولة تحقيق الأمن البيئي والمادي في بيئة الشبكات.

ويمكن تعريفه إجرائيًا في البحث الحالي بأنه ممارسة حماية الأنظمة من أي تهديدات رقمية عبر محاولة الدخول للمعلومات أو إتلافها بالمؤسسات المعنية.

الإعلام الإلكتروني

هو مختلف النماذج والخدمات الحديثة في حقل الإعلام التي تمنح تطور المحتوى الإعلامي، خلال العملية الإعلامية، وذلك بتوظيف التقنيات التي يجري توظيفها لدمج تقنيات الاتصالات بالشكل والمضمون[8].

ويمكن تعريف الإعلام الإلكتروني إجرائيًا بأنه الخدمات الصادرة عن وسائل الإعلام والصحف الكويتية الإلكترونية، ووكالة الأنباء (كونا) ومواقع الإعلامي الحكومية، وتشمل المواقع والتطبيقات والخدمات من خلال الأجهزة الرقمية المتنوعة.

أساسيات الأمن السيبراني

هي مجموعة عناصر تعمل كل منها لتوفير جزء محدد من الحماية، بحيث تتكامل كافة العناصر ووظائفها لتحقيق الحماية المستهدفة للمعلومات، وفي حالة حدوث خلل في أي من العناصر تتأثر الحماية بصورة سلبية ويمكن تحديدها في ما يلي:

السرية: وتعد من أهم أساسيات أمن البيانات، ويجب توافرها ببيانات الشبكات الإلكترونية وبتعاملاتها، فهي تهدف للمحافظة على البيانات وأمنها، من خلال الاستيثاق من سرية المعلومات. يمكن أن تكون السرية من أهم جوانب أمن البيانات انتشاراً فهي مرتبطة بأهمية الحفاظ على سرية البيانات المعتمدة على الإنترنت، ما يتطلب حمايتها والحذر من البرامج والهجمات الضارة التي يمكن أن تعصف بسلامة البيانات. ويعد التشفير أسلوبًا للإبقاء على المعلومات في أمن وسرية؛ وذلك عبر تغييرها لصور غير مفهومة خلال نقلها، ولا يمكن الاطلاع عليها إلا من خلال خريطة فك الترميز[9].

ولا شك في أن السرية خطوة فعالة للوصول لأمن المعلومات، فهي أمر ضروري ومهم للمحافظة على سلامة البيانات في المنظمات التي تستخدم الإنترنت والشبكات.

التوافرية: وهي القدرة على صنع البيانات ومواردها المادية بأسلوب يمكن من الوصول إليها وفقًا للحاجة إليها. والتوافر هو القدرة على الوصول للأنظمة دون تعطيل أو تأخير في سير العمليات، ويقصد بها التأكد من عدم قدرة أي فرد من منع الوصول المشروع للبيانات خلال الوقت المناسب؛ إذ تتطلب بعض الحالات تغيير المعلومات باستمرار. كما يتضح دورها في منع الأفراد من منع الآخرين من الوصول للمعلومات من خلال جعلها غير متوافرة أو تعطيل الوصول لها، وتقاس بالمدة التي تبقي البيانات قيد الاستخدام[10]. فاستخدام تقنيات البيانات يساهم بتقليل الوقت المستغرق للوصول للمعلومة، وجعلها متاحة للأطراف المعنية في الوقت المناسب، مع ضمان عدم وجود أي خطر أو تهديد يمنع هذا الوصول.

النزاهة: تشير النزاهة لدرجة مصداقية المعلومات ومواردها، ويتم استخدامها لمراجعة عمليات الرقابة والدخول على التغييرات غير المرغوبة. وتشتمل النزاهة على سلامة محتوى البيانات وتكاملها، وذلك لضمان بقاء المعلومة سليمة دون حدوث أي تعديل أو تغيير بصورة غير مقصودة أو بصورة مقصودة من خلال الهجمات، فسلامة المحتوى هو استعمال أدوات وأساليب تضمن صحة البيانات عند إدخالها أو نقلها بين الأجهزة بهدف التأكد من عدم تغييرها، وتحقيق أعلى مستوى من الصيانة لمحتوى البيانات، عبر تشفير البيانات والحماية من الفيروسات ومتابعة إجراءات النفاذ للبيانات[11]. ومن ثم يعتقد

الباحث بأن نزاهة البيانات تظهر خلال الحفاظ على المعلومات من التعديل وأن اجتماع الأساسيات الثلاث معا يحقق الغاية المأمولة؛ وهي أمان المعلومات وسريتها.

الأمن المادي: صون البيانات ضد الوصول غير المسموح لها، وذلك بالمحافظة على المسافة بين الخوادم الرئيسية ومواقع محطات العمل[12].

أنواع التهديدات السيبرانية

هناك أساليب متعددة يجري استخدامها للوصول غير المشروع للبيانات بالفضاء السيبراني، وتتحدد الهجمات السيبرانية بالنطاقات التالية:

- سرقة كلمات المرور: حيث يجري الاستيلاء على كلمات المرور للوصول للمعلومات من خلال أكثر من طريقة، منها التخمين باعتبار الفرد المستهدف يمكن أن يستخدم تاريخ ميلاده أو اسمه أو رموز معينة يمكن اكتشافها، أو من خلال الخداع والتلصص، فقد يجري خداع الفرد لجعله يعطي كلمات المرور لأفراد معينين أو... غيرها[13].
- الهجمات الطمسية: وذلك النوع من الهجمات يجري من خلال استبدال صفحة الويب التي يستخدمها الشخص المستهدف بصفحة ويب تشبهها، ويجبره من خلالها على الإدلاء بالبيانات المهمة ككلمات السر أو بطاقات الائتمان[14].
- هجمات رفض أداء الخدمة: وذلك النوع من الهجمات يجري من خلال تعطيل النظام واستغلال بعض جوانب النظام لمنع المستخدمين من الوصول للخدمات، فيقوم الشخص المخترق بتحميل النظام المستهدف مهاجمته بطلبات أكثر من الطاقة المحددة له مما يؤدي لانهياره ويصبح غير متاح لتقديم الخدمات. وعادة ما يتم استعمال الروبوت عادة في هذه الهجمات مثل الروبوت القائم على الاتصال، ويتم في حالة وجود تبادل واتصال بيانات بين الخادم والعميل، بينما الروبوت منقطع الاتصال يقوم بالهجوم دون توافر أي اتصال[15].
- هجمات البنية التحتية الحرجة: يقع الهجوم من شبكات اتصالات ومعلومات، فكلما ارتبطت البنية التحتية بالإنترنت بشكل كبير، كلما كان تأثير تلك الهجمات

قوي على النظام، لذا فإن المؤسسات تحاول تشديد الرقابة على أجهزة الكهرباء وذلك باعتبارها المشغل الرئيسي لكافة الأنظمة، بالإضافة لتوفير خطة للحفاظ عليها من الهجمات [16].

- الهجمات الخداعية: وتستغل تلك الهجمات نقاط الضعف الموجودة في بروتوكولات الإرسال والاستقبال للتسلل للنظام؛ إذ إن أسلوب عمل البروتوكولات يعد من المعلومات العامة التي يسهل معرفتها، لذا فإن هذه الهجمات تشمل إعادة توجيه الرسائل أو منعها عن طرف محدد[17].

مخططات سياسة الأمن السيبراني

يعتمد البحث الحالي على مخططات الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني، وذلك للحد من الغزو السيبراني للبيانات بمجال الإعلام الإلكتروني؛ لذا يمكن رصد عدة مخططات جرى الاستناد إليها في هذا الصدد؛ منها:

- تحديد المسؤوليات والأدوار ومسؤولية اتخاذ القرارات داخل المؤسسة وإدارة الأزمات: وذلك باختيار مؤسسات الإعلام الإلكتروني المسؤوليات. خاصة مسؤولية اتخاذ القرار عند حدوث أي هجمات سيبرانية على المعلومات، ذلك لتوضيح حدود مسؤوليات العاملين وتسهيل متابعة الأداء ومحاسبتهم عند ظهور أي تقصير يضعف من أمن الموارد المعلوماتية[18].
- إدارة البيانات ويشتمل على حوكمة المعلومات وتصنيفها بالإضافة لإدارة وأمن البيانات بالمؤسسة: فتحديد ضوابط عامة يساهم في تطوير التطبيقات والبرامج بصورة فعالة، بالإضافة صحة البيانات وعمليات الكمبيوتر في كافة الموارد، باعتبارها إجراءات عامة ليست مربوطة بإجراءات أو معاملات محاسبية[19] معينة، تهدف لحماية البيانات بكافة صورها من الاطلاع أو الإفصاح أو التغيير بدون تفويض. لذا فإن سياسة أمن البيانات تهدف لحماية البيانات خلال عمليات العزل والإعداد والنقل والإتلاف، وزيادة الرقابة على موارد المعلومات الإلكترونية، بالإضافة إلى تحقيق الأمن المطلوب للبيانات من الاستخدام والوصول غير المرخص. يقع على عاتق المؤسسة تحديد معايير شاملة تحتوي

على موارد المعلومات وتفاصيلها لتحديد آثار المعلومات وأهميتها، بالإضافة إلى بذل الجهد اللازم لإدارة البيانات، وتصنيف المعلومات الموجودة وفقًا لحساسيتها ودرجة أهميتها.

- خصوصية معلومات العملاء: تهدف الخصوصية إلى الحفاظ على بيانات العملاء مثل: العنوان، والاسم، والبريد الإلكتروني... وغيرها، وعدم الإفصاح عنها لأي جهات خارجية، بالإضافة لمراعاة خصوصية المعلومات وعدم انتهاكها من قبل العاملين الآخرين الذين لا علاقة لهم بالمعلومات، لذا فمن المهم التأكد من وجود كافة الاحتياطات لتحقيق لوازم الأمن للمحافظة على البيانات والبعد بها عن السرقة، بالإضافة لزيادة وعي العاملين لتجنبيهم الخداع الذي يمكن أن يؤدي لسرقة معلوماتهم ذات الأهمية[20].
- ضوابط المخاطر السيبرانية للسيطرة على تلك مخاطر وخطط الاستمرار ومواجهة الأزمات: تهدف لمحاولة توقع المخاطر المحتملة وتقييم درجة حدوثها، وذلك من خلال معرفة التهديدات التي يمكن حدوثها، بالإضافة لتحديد نقاط الضعف المتعلقة بموارد وأنظمة التقنية، عن طريق تحليل سيناريو للمخاطر من خلال تحديد مصادر التهديد ونوعيتها وتوقيتها والنتائج المتوقعة منها[21].
- إدارة الأطراف الخارجية للعمليات بجانب العمليات المسندة للأطراف الأخرى: تهدف لتوضيح آليات تعامل المؤسسات مع الأطراف الخارجية المختصة بالأمن السيبراني، وذلك من خلال اللجوء إليهم للمساعدة عند حدوث هجمات سيبرانية، فالتعامل مع هذه الجهات الخارجية يتطلب توافر سياسة مدروسة وواضحة تحدد طبيعة المسؤوليات والمهام المحددة لهم خارجيًا وداخليًا في المؤسسة، فالجهات التي يجري التعاقد معها تلتزم بتوفير الخدمات المتعلقة بالمؤسسة[22].
- تنظيم الأمن المادي والبيئي ومراقبة الشبكات والأنظمة والتطبيقات وتطويرها: وتهدف لحماية موارد البيانات المادية من أي تهديدات بيئية أو بشرية تؤثر بسرية وسلامة المعلومات، وتحاول الإدارة وضع الضوابط اللازمة التي تحقق سلامة كافة الأنظمة والمعدات في المؤسسة المتعلقة بأمن البيانات[23].

وترتبط ضوابط الأمن المادي بتحديد وصول العاملين غير المصرَّح لهم لأي مورد أو معلومة، بالإضافة للمحافظة على المؤسسة بصورة تحول دون الأعمال الهجومية عليها، وتأتي تلك الضوابط لمحاولة تقليل المخاطر وليس للحد منها[24].

- تدريب وزيادة وعي العاملين في المؤسسة بخصوص الأمن السيبراني للتأكد من تطبيق كافة العاملين لبنود الحماية: وهذا المخطط من مسؤوليات الموارد البشرية، وتهدف لتدريب العاملين للتعامل مع الأمن السيبراني بتطوير برامج مراقبة وأمن الأفراد، فالإضافة لتعهد العاملين بعدم الإفصاح عن أي بيانات سرية[25].
- تحديد آلية الإفصاح للأفراد المعنيين عن بنود استراتيجية الأمن السيبراني: بتوضيح البيانات المستهدف وصولها للأفراد الخارجية التي يجري التعامل معهم، وتحتوي على وضع قيود محددة للأطراف المتكفلة بحماية موارد البيانات بالمؤسسة، تمنعهم الوصول للبيانات التي لا تقع تحت إطار عملهم، بالإضافة لطبيعة البيانات التي يحتاجها العاملين والتي يتاح الإفصاح عنها[26].
- تحديد الجهات المالية ونظام التحديث والمراجعة وصلاحيات التوزيع والاطلاع والمسؤوليات والأهداف وإجراءات العمل المرتبطة بها والعقوبات في حالة عدم تنفيذ المهام: وتشتمل تلك الاستراتيجية على تحديد آلية العمل والحدود التي سيتم تطبيق الاستراتيجية عليها، بالإضافة لصلاحيات العاملين فيما يتعلق بالوصول للبيانات أو الاطلاع عليها وتوزيعها، وتحتوي على تفسير للضوابط والتعليمات والعقوبات التي ستقع على عاتق العاملين في حالة حدوث أي تقصير أو خلل[27].

الأدبيات السابقة

بمراجعة الأدبيات التي درست الأمن السيبراني نجد زيادة ملحوظة في عددها خلال الأعوام السابقة ما يبرر أهمية موضوع الأمن السيبراني وأهمية البحث في تأثير المتغيرات المتنوعة عليه، ومن تلك الدراسات:

تناولت دراسة فاطمة علي أحمد[28] الأمن السيبراني والنظافة الرقمية، وذلك لمعرفة التحديات خلال التعامل مع شبكة الانترنت وزيادة عمليات الانتهاك والاختراق يومًا بعد يوم. وتناولت الدراسة موضوع الأمن السيبراني ودوره في ردع تلك الانتهاكات. واستندت الدراسة إلى المنهج الوصفي كمنهج للبحث، وخلصت إلى أن النظافة الرقمية تعد جزءًا أساسيًّا من الأمن السيبراني، بالإضافة إلى وجود علاقة بينها وبين الذكاء الاصطناعي، وأوصت الدراسة بتكثيف الدورات التوعوية لزيادة وعي أفراد المجتمع بالنظافة الرقمية والأمن السيبراني للحد من الانتهاكات.

من جهتها بحثت دراسة أسماء علَّام[29] المخططات التي يتبعها خطاب صحافة التقنيات العربية لارتفاع نسبة الوعي تجاه الأمن السيبراني في مصر والسعودية من خلال الاستناد إلى تحليل الخطاب لكافة الأشكال الصحفية التي انصبت على الأمن السيبراني في الصحف. جرى اعتماد استمارة تحليل الخطاب بوصفها أداة لتحصيل المعلومات. وتوصلت الدراسة لاتفاق خطاب الصحافة الإلكترونية العربية على أن الأمن السيبراني مهم للدفاع عن الذات وعن الإنجازات الوطنية، باعتبار أن الهجمات السيبرانية لم تعد مجرد فعل لأفراد أو لمجموعات من القراصنة، ولكنها أصبحت نتاج فعل يقوم به متخصصون في الجرائم السيبرانية يتعاونون ويستثمرون الأموال والمعرفة، كما وظف الخطاب في الصحف الإلكترونية أسلوب تقديم الشواهد والأدلة ووضوح الأهداف لبيان استعداد لمواجهة الهجوم السيبراني.

وحاولت دراسة عبد الرحمن[30] بحث تعزيز الأمن السيبراني ودوره في المحافظة على الأمن الوطني، والتعرف على الفئات المستهدفة بتعزيز وعيها بثقافة الأمن السيبراني. واعتمدت الدراسة على المراجع كمنهجية لمراجعة الأدبيات السابقة للتعرف على أهمية البحث الاقتصادي والبيئي والاجتماعي والثقافي والدولي والمحلي. واستنتجت الدراسة اعتماد الأفراد على مواقع تعليمية لتعزيز الثقافة بالأمن السيبراني خاصة لدى الأطفال، وتوعيتهم بأهمية استعمال كلمات مرور معقدة، وتحديث التطبيقات والبرامج بصورة مستمرة، واستخدام برامج الوقاية من الفيروسات والاختراقات السيبرانية. وأوصت الدراسة برفع الوعي عبر النشرات الدورية والبرامج التدريبية، وإتاحة الفرصة للمعلمين

للحصول على دبلوم الأمن السيبراني، واستقطاب كفاءات بشرية للعمل على تطوير وسائل الوقاية.

كما تناولت دراسة مصباح الصحفي، مستوى وعي معلمات الحاسب الآلي بالأمن السيبراني في تعليم المرحلة الثانوية بجدة، واعتمدت على عينة تكونت من 352 من معلمات الحاسب الآلي. مستخدمًا الاستبانة كأداة لجمع البيانات من العينة. واستنتجت الدراسة ضعف وعي معلمات الحاسب الآلي بمفاهيم الأمن السيبراني، وضعف لديهم في مستوى الوعي بالأمن السيبراني، وعدم وجود أي فروق دالة في درجة وعي أفراد العينة ترجع للمؤهل العلمي وأعوام الخبرة [31].

وتناولت دراسة سامي بونيف[32] فاعلية المخططات لصد الهجمات السيبرانية وذلك لبحث الأخطار التي واجهتها أميركا عقب الأحداث الإرهابية. فقد أصبح الأمر لا يتعلق بمواجهة أطراف مماثلة ولكن مجابهة جماعات لا تخضع لسلطة، مما جعلها تتوجه نحو البحث عن أساليب جديدة لمواجهة الخطر القائم وزيادة الأساليب الوقائية، خاصة في المجال السيبراني الذي أصبح من مظاهر الحياة الإنسانية ومن الأدوات الرئيسية في مخططات الدول. وقام الباحث بجمع البيانات من الأدبيات ذات الصلة للتعرف على المخططات الاستباقية، وخلص في دراسته إلى وجود بعض الصعوبات التي تعرقل مخططات الردع؛ منها: عدم المرونة في ضوء العلاقات الضيقة بين الأطراف، بالإضافة لوجود فروق في التقنيات؛ ما يزيد من الهجمات التي تتجاوز قدراتهم.

منهجيَّة الدِّراسَة وإجراءاتها

تهدف دراستنا هذه إلى معرفة مخططات الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني، وسنستعرض في هذه الجزئية منهجية الدراسة وإجراءاتها بغرض تحقيق الأهداف المسطرة لها.

منهج الدِّراسَة

للوصول إلى ما يرمي إليه البحث جرى الاســتعانة بالمنهج الوصفي التحليلي الهادف إلى تناول ظاهرة بعينها بالدرس والتحقق من درجة وجود الظاهرة[33].

مجتمع الدِّراسَة وعينته

استهدفت دراستنا هذه عينة من العاملين في الصحافة الإلكترونية والمواقع الإعلامية الحكومية في دولة الكويت. وبالنظر لصعوبة حصر مجتمع هؤلاء الكوادر فقد وقع الاختيار على عينة عشوائية بسيطة عددها مائة وخمسون موظفًا بالإعلام.

سمات العينة:

الجدول (1) السمات الديموغرافية للعينة

البيانات الديموغرافية	التصنيف	العدد	النسبة
السن	دون 30 سنــة	34	%22.7
	بين 30 و 40 سنــة	68	%45.3
	تجاوز 40 سنــة	48	%32.0
المؤهل	شهادة جامعية	72	%48.0
	دبلوم	41	%27.3
	دراسات عليا	37	%24.7
الخبرة	دون 5 أعوام	23	%15.3
	بين 6 و 10 أعوام	79	%52.7
	تجاوز 10 أعوام	48	%32.0
المسمى الوظيفي	موظف	80	%53.3
	رئيس قسم	49	%32.7
	مدير	21	%14.0

نجد أنّ معظم المبحوثين بنسبة (45.3 %) بين 30 إلى 40 سنة، وكان (48%) منهم ذوو الشهادات العالية، وكانت النسبة الكبرى ممن لديهم خبرة من 6 إلى 10 أعوام، وذلك بنسبة (52.7%) حيث جاءت أعلى نسبة منهم بـ (53.3%) موظفون.

أداة الدِّراسَة

بعد مراجعة الأدبيات السابقة التي تتلاقى ولو مع أحد متغيراته بالبحث الحالي جرى تنفيذ الاستبانة لتحصيل البيانات؛ كي يتمكن الباحث من تحقيق أهداف الدراسة.

بناء أداة الدِّراسَـة

لما كان الهدف من الدراسة هو معرفة مخططات الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني، جرى إعداد الأداة، مما ورد بالأدبيات ذات العلاقة بأهداف البحث، وقد تكونت أداة الدراسة على النحو التالي:

أولًا: المتغيرات الديمغرافية: وتشمل على البيانات الأولية

ثانيًا: محاور الدراسة: ويشتمل على (3) محاور؛ وهي:

1- **المحور الأول:** المخططات التي يوظفها الإعلام الإلكتروني بالكويت تجاه الأمن السيبراني وقوامه 7 فقرات.

2- **المحور الثاني:** العوامل ذات التأثير في مخططات الإعلام الإلكتروني تجاه الأمن السيبراني في الكويت ويتكون من 9 فقرات.

3- **المحور الثالث:** واقع استعمال هؤلاء الكوادر المبحوثين للمخططات تجاه الأمن السيبراني ويتكون من 9 فقرات.

صدق الاستبانة

للتحقق من صدق الاستبانة التي اعتمدناها كأداة للدراسة جرى اتباع الخطوات التالية:

أولًا: باستخدام طريقة صدق المحكمين

وهي التي يجري من خلالها طلب رأي بعض أهل الاختصاص من أساتذة الجامعات؛ للاستبصار بخبراتهم وآرائهم، لمعرفة مدى ملائمة ووضوح العبارات، واتساقها مع محاورها مع اقتراح أية تعديلات ممكنة لتطوير الاستبانة.

وبعد مراجعة آراء السادة المحكمين حول العبارات المتفق كانت الاستبانة في صورتها الأخيرة تتكون من (25) فقرة.

ثانياً: صدق البناء للاستبانة

يكون ذلك بتحقيق الصلة بين الإجابات عن كل مفردة ودرجة محورها كلها؛ وذلك بتطبيقها على عينة أخرى استطلاعية (30) فردًا بخلاف العينة العشوائية المبحوثة، وكانت النتائج.

الجدول (2) الصلة بين الفقرة والدرجة الكليَّة

المخططات التي يوظفها الإعلام الإلكتروني بالكويت تجاه الأمن السيبراني		العوامل والمتغيرات ذات التأثير في مخططات الإعلام الإلكتروني تجاه الأمن السيبراني في الكويت		واقع استعمال الكوادر المبحوثين من مخططات تجاه الأمن السيبراني	
المفردة	معامل الارتباط	المفردة	معامل الارتباط	المفردة	معامل الارتباط
1	** 0.499	1	** 0.827	1	** 0.824
2	** 0.617	2	** 0.512	2	** 0.531
3	** 0.584	3	** 0.756	3	** 0.724
4	** 0.750	4	** 0.719	4	** 0.645
5	** 0.501	5	** 0.600	5	** 0.556
6	* 0.390	6	* 0.430	6	** 0.588
7	* 0.462	7	** 0.696	7	** 0.736
		8	** 0.647	8	** 0.750
		9	** 0.871	9	**0.660

** ذات دلالة عند 0.01

معامل الصلة بين المفردات والدرجة الكليَّة لمحورها، وجاءت جميعها معاملات ذات قيم عالية بالإضافة إلى كونها دالة إحصائيًّا دون 0.05 ما يشير إلى اتسام المفردات بدرجة عالية من صدق البناء؛ ما يجعلنا نقبل الاستبانة ونعتمد عليها.

ثالثًا: ثبات الاستبانة

تم التأكد من الثبات بواسطة معادلة (Alpha Chronbach) لقياس الثبات لمحاور الاستبانة، كما يلي:

الجدول (3) معاملات ألفا كرونباخ للمحاور

المحور	المفردات	القيمة
المحور الأول: المخططات التي يوظفها الإعلام الإلكتروني بالكويت تجاه الأمن السيبراني	7	0.813
المحور الثاني: العوامل ذات التأثير في مخططات الإعلام الإلكتروني تجاه الأمن السيبراني في الكويت	9	0.852
المحور الثالث: واقع استعمال كوادر المبحوثين لمخططات تجاه الأمن السيبراني	9	0.805
الدرجة الإجمالية للاستبانة	25	0.820

يتبين لنا إذن أن المعاملات كافة لألفا كرونباخ عالية القيمة، ونجد أن الدرجة الكلية لثبات الاستبانة جاءت مساوية (0.820)، ومما سبق يتبين لنا أن الاستبانة تتسم بالثبات؛ ما يمكننا من الاعتماد على محاور ومفردات الاستبانة للتحقق من أهداف الدراسة.

نتائِج الدِّراسَة وتفسيرها

فيما يلي عرض لنتائج الدراسة وذلك بعد أن جرى معالجتها إحصائيًّا والوصول إلى الإجابة عن أسئلتها والتحقق من صحة فروضها.

الإجابة عن أسئلة الدراسة

الأول: ما المخططات التي يوظفها الإعلام الإلكتروني بالكويت تجاه الأمن السيبراني؟

للتعرف على المخططات التي يوظفها الإعلام الإلكتروني بالكويت تجاه الأمن السيبراني من خلال إيجاد ما يأتي:

الجدول (4) المتوسِّطات الحسابيَّة والانحرافات المعياريَّة والترتيب لعبارات المحور الأول

الرقم	الفقرة	الوسط الحسابي	الانحراف	الترتيب	درجة الموافقة
1	توعية المواطنين بالاستخدام الأمثل للمنصات الرقمية	3.82	0.844	5	موافق
2	تعريف المواطنين بالأساليب التي يستخدمها المجرم السيبراني	3.73	0.861	6	موافق

الرقم	الفقرة	الوسط الحسابي	الانحراف	الترتيب	درجة الموافقة
3	تعريف الجمهور بالعقوبات والقوانين الرادعة لمرتكبي التهديدات السيبرانية	4.45	0.781	2	موافق بشدة
4	استغلال المنصات الرقمية في بث الانتماء الوطني والتوعية بمخاطر الجرائم السيبرانية	4.23	0.798	3	موافق بشدة
5	إنشاء مواقع إلكترونية لتبادل المعلومات المفيدة عن الأمن السيبراني	4.06	0.831	4	موافق
6	التدريب الإعلامي المجتمعي للإبلاغ عن المواقع التي تجسد الأخبار الزائفة وكشف بؤر ومخطط المنظمات الإرهابية	4.52	0.609	1	موافق بشدة
7	القيام بالحملات الإعلامية التوعوية للحد من الشائعات والبيانات المفبركة التي تهدد حياة الأشخاص والدولة	4.45	0.761	2	موافق بشدة
الوسط الحسابي العام		4.18	0.78	موافق	

من الجدول يتبين أن المخططات التي يوظفها الإعلام الإلكتروني بالكويت تجاه الأمن السيبراني جاءت عالية؛ إذ جاء الوسط الحسابي (4.18)، واتجاه (موافق)، وقيمة للانحراف المعياري (0.78) منخفضة القيمة تعني التجانس في اتجاهات العينة المختارة حول المخططات التي يوظفها الإعلام الإلكتروني بالكويت تجاه الأمن السيبراني، وكانت قيم الانحرافات تتراوح بين (0.861 – 0.609)، قيم منخفضة تشير إلى اتفاق آراء العينة المختارة حول تلك الفقرات.

وفي الترتيب الأول (6): (التدريب الإعلامي المجتمعي للإبلاغ عن المواقع التي تجسد الأخبار الزائفة وكشف بؤر ومخطط المنظمات الإرهابية)، بمتوسِّـــط حسـابي (4.52)، وانحراف (0.609)، واتجاه (موافق بشدة)، وفي الترتيب الأخير (2): (تعريف المواطنين بالأساليب التي يستخدمها المجرم السيبراني) بمتوسِّـــط حسابي (3.73)، وانحراف (0.861)، واتجاه (موافق).

ويستنتج الباحث أن المخططات التي يوظفها الإعلام الإلكتروني بالكويت تجاه الأمن السيبراني جاءت عالية، وهذا يدل على ارتفاع المخططات التي يوظفها الإعلام

الإلكتروني بالكويت تجاه الأمن السيبراني، حيث التدريب الإعلامي المجتمعي للإبلاغ عن المواقع التي تجسد الأخبار الزائفة وكشف بؤر ومخطط المنظمات الإرهابية وتعريف الجمهور بالعقوبات والقوانين الرادعة لمرتكبي التهديدات السيبرانية.

السؤال الثاني: ما المتغيرات والعوامل ذات التأثير في مخططات الإعلام الإلكتروني تجاه الأمن السيبراني في الكويت؟

للتعرف على مخططات الإعلام الإلكتروني تجاه الأمن السيبراني في الكويت؛ تم إيجاد ما يأتي:

الجدول(5) المتوسِّطات الحسابيَّة والانحرافات المعياريَّة والترتيب لعبارات المحور الثاني

الرقم	الفقرة	الوسط الحسابي	الانحراف	الترتيب	درجة الموافقة
1	عقد دورات تدريبية للعاملين للتقنيين لتدريبهم على تطبيق الأمن السيبراني	4.27	0.791	2	موافق بشدة
2	توفير الميزانيات لتحقيق الأمن السيبراني	3.76	0.933	6	موافق
3	امتلاك لنظام حوكمة تقني لتوفير الأمن السيبراني للتعاملات الإلكترونية	3.85	0.866	4	موافق
4	تطوير البنية التحتية السيبرانية للحد من الاختراق والتجسس والقرصنة الإلكترونية	3.70	0.930	7	موافق
5	تطوير وتحديث البرامج والتقنيات المعلوماتية والتقنية باستمرار بشكل يتيح التعرف على التقنيات الدقيقة التي تساعد على كشف الجريمة ومرتكبيها	3.85	0.855	4	موافق
6	تشديد العقوبات على جرائم الفضاء السيبرانيي	4.14	0.833	3	موافق
7	تقديم الحوافز للمتميزين والمبدعين في الأمن السيبراني	3.47	0.672	8	موافق
8	ضرورة تحديد المسؤوليات وصلاحيات الوصول لكل فرد	3.80	0.833	5	موافق
9	توعية العاملين بمخاطر استعمال الأجهزة الشخصية مثل الهاتف المحمول لتخزين معلومات سرية خاصة بالعمل	4.40	0.658	1	موافق بشدة
	الوسط الحسابي العام	3.92	0.82		موافق

المتغيرات والعوامل ذات التأثير في مخططات الإعلام الإلكتروني تجاه الأمن السيبراني في الكويت جاءت عالية؛ إذ جاء الوسط الحسابي لفقرات المحور الثاني كلها (3.92)، بالموافقة (موافق)، وبانحراف معياري منخفض القيمة عند مستوى (0.82) ما تدلُّ على تطابق اتجاهات العينة المختارة للدراسة حول المتغيرات والعوامل ذات التأثير في مخططات الإعلام الإلكتروني تجاه الأمن السيبراني في الكويت، وكانت قيم الانحرافات تتراوح بين (0.933 – 0.658)، قيم منخفضة تشير إلى اتفاق آراء العينة المحتارة حول تلك الفقرات.

وفي الترتيب الأول (9): (توعية العاملين بمخاطر استعمال الأجهزة الشخصية مثل الهاتف المحمول لتخزين معلومات سرية خاصة بالعمل)، بمتوسِّـط حسـابي (4.4)، وانحراف (0.658)، واتجاه (موافق بشدة)، وفي الترتيب الأخير (7): (إتاحة الحوافز للمتميزين والمبدعين في مجال الأمن السيبراني) بمتوسِّـط (3.47)، وانحراف (0.672)، واتجاه (موافق).

ويرى الباحث أن العوامل ذات التأثير في مخططات الإعلام الإلكتروني تجاه الأمن السيبراني في الكويت جاءت عالية، وهذا يدل على وجود عديد من العوامل والمتغيرات ذات التأثير في مخططات الإعلام الإلكتروني تجاه الأمن السيبراني في الكويت مثل العمل على التوعية بمخاطر استعمال الأجهزة الخاصة؛ كالهاتف المحمول وعقد دورات تدريبية للعاملين التقنين لتجريبهم على تطبيق الأمن السيبراني.

السؤال الثالث: ما واقع استعمال هؤلاء الكوادر المبحوثين للمخططات تجاه الأمن السيبراني؟

للتعرف على واقع استعمال العاملين في الصحف الكويتية الإلكترونية والمواقع الإعلامية الحكومية الكويتية من مخططات تجاه الأمن السيبراني؛ من خلال إيجاد المتوسِّطات الحسابيَّة والانحرافات المعياريَّة والترتيب لفقرات المحور الثالث.

الجدول (6) المتوسِّطات الحسابيَّة والانحرافات المعياريَّة والترتيب لعبارات المحور الثالث

رقم الفقـــرة	الفقرة	المتوسط	الانحراف	الرتبـة	درجة الموافقة
1	يتوفر بالصحف الكويتية الإلكترونية نظام حماية سيبراني على مستوى عالٍ	4.06	0.911	3	موافق
2	يتم عقد اجتماعات دورية لمتخصصي الأمن السيبراني بالصحف الكويتية الإلكترونية لتعريفهم بآخر المستجدات في هذا المجال	4.03	0.926	4	موافق
3	توفر الصحف والمواقع الكويتية الإلكترونية إدارة خاصة بالأمن السيبراني	4.07	0.841	2	موافق
4	تتوفر أنظمة حماية أمنية للأجهزة التقنية والحاسوبية بالصحف الكويتية الإلكترونية	3.73	0.960	8	موافق
5	تطبق الصحف والمواقع الكويتية الإلكترونية كل ما يتعلق بالإجراءات الإدارية لتحقيق الأمن السيبراني ضمن منظومة المعلومات الإدارية بالجامعة	3.97	0.904	5	موافق
6	تسعى الصحف والمواقع الكويتية الإلكترونية لتوفير الدعم الفني كأحد لوازم تنفيذ الأمن السيبراني لأنظمة المعلومات الإدارية	4.08	0.886	1	موافق
7	تتوفر خطة لإدارة مخاطر الأمن السيبراني لنظم المعلومات الإدارية بالصحف الكويتية الإلكترونية	3.61	0.847	9	موافق
8	يوجد نظام شبكي آمن لتبادل البيانات بالصحف الإلكترونية	3.84	0.823	7	موافق

رقم الفقـــرة	الفقرة	المتوسط	الانحراف	الرتبـة	درجة الموافقة
9	يتم مراقبة العاملين بالصحف الكويتية الإلكترونية للتأكد من تطبيق السياسات والإجراءات الوقائية لمنع تسريب المعلومات	3.91	0.976	6	موافق
المتوسط العام		3.92	0.90	موافق	

يتبين لنا من الجدول أن واقع استعمال هؤلاء الكوادر المبحوثين للمخططات تجاه الأمن السيبراني جاء مرتفعًا؛ إذ جاء المتوسِّط العام للمحور الثالث (3.92)، واتجاه (موافق)، وجاءت قيمة الانحراف المعياري منخفضة (0.90)، ما يعني التجانس في اتجاهات العينة المختارة حول واقع استعمال هؤلاء الكوادر المبحوثين للمخططات تجاه الأمن السيبراني، وكانت قيم الانحرافات المعيارية تتراوح بين (0.976 – 0.823)، وهي قيم منخفضة تشير إلى اتفاق آراء العينة المختارة.

وفي المرتبة الأولى (6): (تسعى الصحف والمواقع الكويتية الإلكترونية لتوفير الدعم الفني كأحد لوازم تنفيذ الأمن السيبراني لمنظومات المعلومات الإدارية)، بمتوسِّط حسابي (4.08)، وانحراف (0.886)، واتجاه (موافق)، وفي الترتيب الأخير (7): (تتوفر خطة لإدارة مخاطر الأمن السيبراني لنظم المعلومات الإدارية بالصحف الكويتية الإلكترونية) بمتوسِّـط حسـابي (3.61)، وانحراف (0.847)، واتجاه (موافق).

ومن ثم فإن واقع استعمال العاملين في الصحف الكويتية الإلكترونية والمواقع الإعلامية الحكومية الكويتية من مخططات تجاه الأمن السيبراني جاء مرتفعًا؛ وهذا يدل على ارتفاع درجة استعمال هؤلاء الكوادر المبحوثين للمخططات تجاه الأمن السيبراني حيث تسعى الصحف والمواقع الكويتية الإلكترونية إلى وجود الدعم الفني كأحد أساسيات الأمن السيبراني للأنظمة الإدارية، وقد توفر الصحف والمواقع الكويتية الإلكترونية إدارة خاصة بالأمن السيبراني.

الرابع: هل هناك فروق بين المخططات المستخدمة في الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني تعود لمتغيرات البيانات الشخصية لدى أفراد العينة؟

التحقق من طبيعة البيانات

تم الاستعانة بالاختبارات كولموجوروف سميرنوف وشابيرو (Kolmogorov–Smirnov– Shapiro–Wilk) كما يلي:

الجـــدول (7) بيانات المخططات المستخدمة في الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني

Kolmogorov–Smirnova			Shapiro–Wilk		
أداة الإحصاء	عدد درجات الحرية	مستوي الدلالة	أداة الإحصاء	عدد درجات الحرية	مستوي الدلالة
0.224	150	0.006	0.989	150	0.005

تبين أن بيانات استجابات العينة حول المخططات المستخدمة تجاه الأمن السيبراني جاءت دالة إحصائيًا؛ حيث مستوى الدلالة دون (0.05)؛ أي إن بيانات استجابات العينة حول المخططات المستخدمة تجاه الأمن السيبراني لا تنتمي للتوزيع الطبيعي المعياري؛ ومن ثم جرى الاستعانة بالاختبارات غير المعملية (Non–parametric tests) والإجابة عن السؤال من خلال اختبار كروسكال واليس (Kruskal–Wallis Test).

أولًا: العمر

الجدول (8) الفرق حول المخططات المستخدمة في الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني تعزى إلى العمر

العمر	العدد	متوسط الرتب	عدد درجات الحرية	مستوى الدلالة	أداة الإحصاء
دون 30 عامًا	34	157.72	2	0.569	1.127
بين 30 و 40 عامًا	68	143.65			
تجاوز 40 عامًا	48	139.49			
المجموع	150				

يتضح أنه لا فروق حول المخططات المستخدمة في الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني تعزى إلى العمر إذ جاءت القيمة لمستوى الدلالة (0.569) متجاوزة القيمة 0.05، وعليه لا فروق حول الاستراتيجيات المستخدمة في الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني تعزى إلى العمر.

ثانيًا: المؤهل العلمي

الجدول(9) الفروق حول الاستراتيجيات المستخدمة في الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني تعزى إلى المؤهل

المؤهل	العدد	متوسط الرتب	عدد درجات الحرية	مستوى الدلالة	أداة الإحصاء
شهادة جامعية	72	139.53	2	0.007	0.449
دبلوم	41	144.02			
دراسات عليا	37	147.21			
المجموع	150				

يتضح حضور فروق دالة إحصائيًّا حول الاستراتيجيات المستخدمة في الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني تعزى إلى المؤهل؛ إذ جاءت القيمة لمستوى الدلالة (0.007) ذات قيمة أقل من (0.05)؛ وهذا ينم عن وجود فروق حول تلك الاستراتيجيات تجاه الأمن السيبراني تعزى إلى المؤهل، وكان الفارق لمصلحة الحاصلين على دراسات عليا بمتوسط رتب قدره (147.21)؛ ما يشير إلى أهمية الارتقاء العلمي بما يساير التطوراتات التقنية.

ثالثًا: أعوام الخبرة

الجدول (10) الفروق حول المخططات المستخدمة في الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني تعزى إلى الخبـــرة

الخـــبرة	العـــدد	متوســـط الرتب	عدد درجات الحرية	مستوى الدلالة	أداة الإحصاء
دون 5 أعوام	23	128.17	2	0.00	0.608
بين 6 إلى 10 أعوام	79	137.72			
تجاوز10 أعوام	48	151.09			
المجموع	150				

يتبين حضور فروق حول الاستراتيجيات المستخدمة في الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني تعزى إلى أعوام الخبرة إذ جاءت القيمة لمستوى الدلالـــة (0.00) ذات قيمة أقل من (0.05)؛ وهذا ينم أن الفارق لمصلحة الأكثر خبرة الفئة (أكثر من 10 أعوام) بمتوسط رتب قدره (151.09)؛ وهذا يبين أن الخبرة لها اعتباره الكبير لتولي المناصب العليا في عالم التقنيات والفضاء السيبراني.

رابعًا: الوظيفة

الجدول (11) فروق المخططات المستخدمة في الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني تعزى إلى الوظيفة

المسمى الوظيفي	العـــدد	متوســـط الرتب	عدد درجات الحرية	مســـــتوى الدلالة	أداة الإحصاء
موظف	80	134.06	2	0.233	1.481
رئيس قسم	49	132.11			
مدير	21	135.82			
المجموع	150				

يتضح غياب الفروق حول الاستراتيجيات المستخدمة في الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني تعزى إلى الوظيفة؛ إذ جاءت القيمة لمستوى الدلالـــة

(0.233) تجاوزت (0.05) وهذا ينم عن غياب الفروق الدالة حول المخططات المستخدمة في الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني تعزى إلى الوظيفة.

بناء على ما توصلنا إليه من مؤشرات رقمية ظهرت من مقاربتنا المسحية تبرز لنا النتائج التالية:

- الاستراتيجيات التي يوظفها الإعلام الإلكتروني بالكويت تجاه الأمن السيبراني جاءت عالية، وهذا يدل على ارتفاع الاستراتيجيات التي يوظفها الإعلام الإلكتروني بالكويت تجاه الأمن السيبراني.
- المتغيرات والعوامل ذات التأثير في مخططات الإعلام الإلكتروني تجاه الأمن السيبراني في الكويت جاءت عالية، وهذا يدل على وجود عديد من المتغيرات والعوامل ذات التأثير في مخططات الإعلام الإلكتروني تجاه الأمن السيبراني في الكويت، مثل العمل على التوعية بمخاطر استعمال الأجهزة الشخصية كالهاتف المحمول وعقد دورات تدريبية للعاملين التقنين لتجريبهم على تطبيق الأمن السيبراني.
- واقع استعمال هؤلاء الكوادر المبحوثين للمخططات تجاه الأمن السيبراني جاء مرتفعًا، وهذا يدل على ارتفاع درجة استعمالهم لها تجاه الأمن السيبراني حيث تسعى الصحف والمواقع الكويتية الإلكترونية إلى وجود الدعم الفني كأحد أساسيات الأمن السيبراني للأنظمة الإدارية وقد توفر الصحف والمواقع الكويتية الإلكترونية إدارة خاصة بالأمن السيبراني.
- غياب فروق دالة إحصائيًّا تعزي إلى العمر حول المخططات المستخدمة في الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني؛ ما يعني أن العمر وحده لا يكفي دون خبرة وممارسة حقيقية لتلك الاستراتيجيات تجاه الأمن السيبراني.
- حضور فروقات دالة ذات دلالات إحصائية تعزي إلى المؤهل العلمي حول المخططات المستخدمة في الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني، وكان الفارق لمصلحة الحاصلين على دراسات عليا؛ وهذا حري بعمل الجهات الإعلامية على الارتقاء بالمستوى التعليمي لدى هؤلاء

الكـوادر؛ كـون ذلـك ينعكـس بالإيجـاب لمصلحـة تلك المؤسسـات.

- حضور فروقات دالة ذات دلالات إحصائية تعزي إلى أعوام الخبرة حول المخططات المستخدمة في الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني وكان الفارق لمصلحة الأكثر خبرة الفئة (أكثر من 10 أعوام)؛ وهذا يعني أن هؤلاء الكوادر من ذوي الخبرات الكبيرة والممارسة الحقيقية جديرون بتولي المناصب القيادية وتوجيه السياسات الإعلامية، والأخذ بمستجدات العلم والتقنية للإبقاء على سلامة وأمن البيانات والمعلومات.
- انعدام وجود فروقات دالة ذات دلالات إحصائية تعزي إلى الوظيفة حول المخططات المستخدمة في الإعلام الإلكتروني في الكويت تجاه الأمن السيبراني؛ ما يعني أن هؤلاء الكوادر أيًّا كان موقعهم أو دورهم في تلك المؤسسات فإنهم يؤدون واجبهم على حسب مهامهم وعلى وفق ما يتزودون به من خبرة وتأهيل.

توصيات الدِّراسَة

من الأهمية بمكان أن يضع المسؤولون ومن يهمهم الأمر نصب أعينهم التوصيات الآتية المبنية على النتائج التي توصل إليه البحث:

- أهمية نشر الوعي بين العاملين بالأضرار المترتبة على استعمال الأجهزة الخاصة؛ مثل: المحمول في تخزين معلومات سرية؛ ومن هنا تتجلى أهمية الرقابة الصارمة التي تحول دون وقوع مثل هذه الاختراقات.
- ضرورة عقد دورات تدريبية للعاملين التقنيين لتدريبهم على تطبيق الأمن السيبراني؛ وذلك إيمانًا بأن من لا يتقدم يتقادم، لا سيما في عصر الفضاء المعلوماتي المفتوح.
- ينبغي امتلاك نظام حوكمة تقني لتوفير الأمن السيبراني للتعاملات الإلكترونية؛ وهو نظام يفرض نفسه بقوة تحت مظلة تلك النقلة التقنية المشهودة في العالم بأسره.
- لا غنى عن تشديد العقوبات على جرائم الفضاء السيبراني؛ وذلك لخطورة تلك

الجرائم التي تعصف بأمن وسلامة وممتلكات الأفراد والمجتمعات.

- لا بد من توفير المزيد من الدعم الفني بوصفه أحد الأساسيات لتحقيق الأمن السيبراني للبيانات الإدارية.

الهوامش و المراجع

(1) الصحفي، مصباح أحمد: "مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة"، **مجلة البحث العلمي في التربية**، ع20، ج10، 2019، ص495.

(2) علام، أسماء أحمد: "استراتيجية خطاب صحافة التقنيات العربية تجاه الأمن السيبراني"، **المجلة المصرية لبحوث الرأي العام بجامعة القاهرة**، مج20، ع2، 2021، ص3.

(3) Oloidi, A. "Cyber security challenges in Financial institution in Nigeria: A multiple case study", Information & Security, 2019. Available from Proquest dissertations & Theses Global. Retrieved from https://search.proquest.com/docview/2207495699?accountid=178282

(4) الغامدي، عهود أحمد: "دور الأمن السيبراني في تحقيق الميزة التنافسية"، **مجلة العلوم الاقتصادية والإدارية والقانونية**: مج5، ع9، 2021، ص146.

(5) ناصر، فرح: "الكويت تقدمت 72 مرتبة في مؤشر الأمن السيبراني"، **مجلة الأنباء**: 2019، جرى استيرادها في 26 فبراير من خلال الرابط:

https//:www.alanba.com.

(6) "استراتيجية خطاب صحافة التقنيات العربية تجاه الأمن السيبراني"، ص14.

(7) السرحان، حنين عبد المهدي: **أثر تطبيق الأمن السيبراني على جودة المعلومات المحاسبية في البنوك التجارية الأردنية**، رسالة ماجستير، الأردن: جامعة آل البيت، 2020، ص9.

(8) مساعدي، سلمى، وعادي، خالدي: "الإعلام الإلكتروني أرضية للديموقراطية أم وسيلة للقمع والمراقبة مقاربة تحليلية"، **مجلة حقول معرفية للعلوم الاجتماعية والإنسانية**: مج2، ع3، 2021، ص84.

(9) العقون، نورة: **واقع الفضاء السيبراني وإشكالية الدفاع الوطني في الجزائر**، رسالة ماجستير، الجزائر: جامعة قاصدي مرباح ورقلة، 2019، ص66.

(10) أبو حسين، حنين جميل: **الإطار القانوني لخدمات الأمن السيبراني**، رسالة ماجستير، الأردن: جامعة الشرق الأوسط، 2021، ص40.

(11) المنتشري، فاطمة يوسف: "دور القيادة المدرسية في تعزيز الأمن السيبراني في المدارس الحكومية للبنات بمدينة جدة من وجهة نظر المعلمات"، **المجلة العربية للعلوم التربوية والنفسية**: ع17، 2020، ص466.

(12) أثر تطبيق سياسة الأمن السيبراني على جودة المعلومات المحاسبية في البنوك التجارية الأردنية، ص11.

(13) أحمد، فاطمة علي: "الأمن السيبراني والنظافة الرقمية"، **المجلة المصرية لعلوم المعلومات**: مج9، ع2، 2022، ص402.

(14) قرني، أماني حمدي: "دور مواقع الإعلام الرقمي في حماية الأمن السيبراني"، **المجلة المصرية لبحوث الإعلام**: ع80، 2022، ص667.

(15) البابلي، عمار ياسر: "التحديات الأمنية المعاصرة للهجمات السيبرانية"، **القيادة العامة لشرطة الشارقة**: مج30، ع118، 2021، ص36.

(16) دلالي، الجيلالي: "رهانات الأمن السيبراني الوطني في ظل التحول الرقمي: قراءة في التأصيل المعرفي واستراتيجية المواجهة التشريعية"، **مجلة كلية القانون الكويتية العالمية**: مج10، ع37، 2021، ص541.

(17) أثر تطبيق سياسة الأمن السيبراني على جودة المعلومات المحاسبية في البنوك التجارية الأردنية، ص15.

(18) السيد، نهى مجدي: "الأمن السيبراني وعلاقته بالمضمون الإعلامي في ظل رؤية مصر 2030"، **المجلة العربية لبحوث الإعلام والاتصال**: ع35، 2021، ص499.

(19) قطب، بشائر حامد: "دور الصحف السعودية في تنمية الوعي بالأمن السيبراني"، **المجلة العربية للإعلام والاتصال**: ع25، 2021، ص312.

(20) فوزي، إسلام: "الأمن السيبراني تحليل سوسيولوجي"، **المجلة الاجتماعية القومية**: مج56، ع2، 2019، ص130.

(21) "استراتيجية خطاب صحافة التقنيات العربية تجاه الأمن السيبراني"، ص32.

(22) قلاع الدروس، سمير: "الأمن السيبراني الوطني قراءة في أهم المخططات الأمنية والتقنية لمواجهة الجريمة الإلكترونية بالجزائر"، **مجلة الرواق للدراسات الاجتماعية والإنسانية**: مج8، ع2، 2022، ص261.

(23) نصار، ولاء محمد: "آليات مركز دبي للأمن الإلكتروني للتوعية بالمخططات الوطنية للأمن السيبراني للحكومات الذكية عبر منصات التواصل الاجتماعي"، **جمعية كليات الإعلام العربية**: ع6، 2021، ص53.

(24) يونيف، سامي محمد: "دور المخططات الاستباقية في مواجهة الهجمات السيبرانية"، **المجلة الجزائرية للحقوق والعلوم السياسية**: مج4، ع7، 2019، ص128.

(25) العابد، سكينة: "أمن المعلومات عبر شبكات التواصل الاجتماعي"، **المجلة العربية للمعلوماتية وأمن المعلومات**: ع1، 2020، ص211.

(26) انديجاني، دلال صالح: "ممارسات تعزيز الوعي بثقافة الأمن السيبراني وتوصياتها في المملكة العربية السعودية"، **المجلة العربية للمعلوماتية وأمن المعلومات**: ع5، 2021، ص92.

(27) أثر تطبيق سياسة الأمن السيبراني على جودة المعلومات المحاسبية في البنوك التجارية، ص18.

(28) أحمد، فاطمة علي: "الأمن السيبراني والنظافة الرقمية"، **المجلة المصرية لعلوم المعلومات**، جامعة بني سويف: مج9، ع2، 2022، ص 390– 422.

(29) "استراتيجية خطاب صحافة التقنيات العربية تجاه الأمن السيبراني".

(30) عبد الرحمن، عبد الرحمن أكرم: **تعزيز الأمن السيبراني داخل الدولة ودوره في الحفاظ على الأمن الوطني دراسة ميدانية على الأردن من 2012– 2021**، رسالة ماجستير، الأردن: جامعة آل البيت، 2021.

(31) "مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة".

(32) بونيف، سامي محمد: "دور المخططات الاستباقية في مواجهة الهجمات السيبرانية: الردع السيبراني أنموذجًا"، **المجلة الجزائية للحقوق والعلوم السياسية**: مج4، ع7، 2019، ص 121–135.

(33) العساف، صالح بن حمد: **المدخل إلى البحث في العلوم السلوكية**، ط1، الرياض: مكتبة العبيكان، 1433هـ، ص179.

المراجع بالحروف اللاتينية

References in Roman Script

(1) Al-ʾṣḥfī, mṣbāḥ aḥmd: "mstwā al-ʾūʿī bālʾamn al-ʾsībrānī ldā mʿlmāt al-ʾḥāsb al-ʾʾalī llmrḥlh al-ṯānwyh bmdīnẗ ğdh, mğlẗ al-bḥṯ al-ʿlmī fī al-trbīh, Part. 10, No.20.

(2) ʿlām, asmāʾ aḥmd: "istrātīğẗ ḥṭāb ṣḥāfẗ al-tqnīāt al-ʿrbīh tğāh al-ʾamn al-sībrānī", al-mğlh al-mṣrīh lbḥūṯ al-rʾaī al-ʿām bğāmʿẗ al-qāhrh, Vol. 20, No. 2,2021 .

(3) Ālġāmdy, ʿhwd āḥmd: dūr al-ʾʾamn al-ʾsībrānī fī tḥqīq al-mīzh al-tnāfsīh ", mğlẗ al-ʾʾlūm al-iqtṣādīh wā al-īdārīh wā al-qānūnīh, Vol. 5, No. 9, 2021.

(4) Nāṣr, frḥ: al-kwāīt tqdmt 72 mrtbh fī muʾšr ālʾmn al-ʾsībrānī, mğlẗ ālānbāʾ, 2019.

(5) Msāʿdī, sālmā, wā ʿādī, ḫāldī: al-iʿlām al-ilktrūnī arḍīh lldīmūqrāṭīh am ūsīlh llqmʿ wā al-mrāqbh mqārbh tḥlīlīh, mğlẗ ḥqwl mʿrfīh llʿlūm al-iğtmāʿīh wā al-insānīh, Vol. 2, No. 3, 2021.

(6) Ālsrḥān, ḥnīn ʿbd ālmhdy: āṯr ttbyq ālʾāmn al-ʾsībrānī ʿlā ğaūdaẗ al-mʿlūmāt al-mḥāsbīh fī al-bnūk al-tğārīh alʾaurdnīh, master dissertation, Jordan: ğāmʿẗ al- al-baīt, 2020.

(7) Al-ʿqūn, nūrh: wāqʿ ālfḍāʾ al-ʾsībrānī wa ʾ iškālīāt al-dfāʿ al-waṭnī fi ālğzāʾr, master dissertation, Algeria: ğāmʿẗ qāṣdy mrbāḥ ūrqlh, 2019.

(8) Abū ḥusīn, ḥnīn ğmīl: al-īṭār ālqānwny lḫdmāt ālʾamn al-ʾsībrānī, master dissertation, Jordan: ğāmʿẗ ālšrq ālāwsṭ, 2021.

(9) Al-mntšrī, fāṭmh īūsf: dūr al-qīādh al-mdrsīh fī tʿzīz alʾamn al-sībrānī fī al-mdārs al-ḥkūmīh llbnāt bmdīnaẗ ğdh mn ūğhẗ nẓr al-mʿlmāt, al-mğlh alʿrbīh llʿlūm al-trbwyh wā ālnfsīh, No. 17, 2020.

(10) Āḥmd, fāṭmh ʿly: ālāmn al-sībrānī wā ālnẓāfh ālrqmyh ,ālmğlh ālmṣryh lʿlwm ālmʿlwmāt, Vol. 9, No.2, 2022.

(11) Qrnī, amānī ḥmdī: dūr mwāqʿ al-iʿlām ālrqmy fi ḥmāyẗ ālāmn al-sībrānī, ālmğlh al-mṣrīh lbḥwṯ al-iʿlām, No. 80, 2022.

(12) Al-bāblī, ʿmār īāsr: al-tḥdīāt al-ʾamnīh al-mʿāṣrh llhğmāt al-sībrānīh ,ālqyādh ālʿāmh lšrṭẗ ālšārqah ,Vol.30, No. 118, 2021.

(13) Dlālī, al-ğīlālī: rhānāt ālāmn al-sībrānī ālwṭny fi ẓl ālṭhwl ālrqmy: qrāʾh fi al-tʾaṣīl ālmʿrfy wā istrātīğīāt ālmwāğhh ālṭšryʿyh, mğlẗ klyẗ ālqānwn ālkwytyh ālʿālmyh, Vol. 10, No. 37.

(14) Al-sīd, nuhā mğdī: ālāmn al-sībrānī wā ʿlāqth bālmḍmwn al-iʿlāmī fi ẓl ruʾīẗ mṣr ,2030 ālmğlh ālʿrbyh lbḥwṯ al-iʿlām wā al-itṣāl, No. 35.

(15) Qṭb, bšāʾir ḥāmid: dūr al-ṣḥf al-sʿūdīh fī tnmīẗ al-waʿī bālʾamn al-sībrānī, ālmğlh ālʿrbyh llʿulūm wā al-itṣāl, No. 25, 2021.

(16) Fwzy, īslām: ālāmn al-sībrānī tḥlīl sūsīūlūğī, ālmğlh al-iğtmāʿīh ālqwmyh ,Vol. 56, No. 2, 2019.

(17) Qlāʿ al-drūs, samīr: ālāmn al-sībrānī qrāʾh fī ahm al-mḥṭaṭāt alʾamnīh wā al-tqnīh lmwāğhẗ al-ğrīmh al-ilktrūnīh bālğzāʾir", mğlẗ al-rwāq lldrāsāt al-āğtmāʿīh wā al-insānīh, Vol.8, No. 2. 2022.

(18) Naṣār, walāʾ mḥmd: al-īāt mrkz dubī llāmn al-ilktrūnī lltūʿīh bālmḥṭṭāt al-ūṭnīh llʾamn al-sībrānī

llḥkūmāt al-ḏkīh ʿbr mnṣāt al-twāṣl al-āğtmāʿī", ğmʿīẗ kulīāt al-iʿlām al-ʿrbīh ,No. 6, 2021.

(19) Al-ʿābd skīnh: āmn ālmʿlwmāt ʿbr šbkāt āltwāṣl ālāğtmāʿy, ālmğlh ālʿrbyh llmʿlwmātyh wā āmn ālmʿlwmāt, No. 1, 2020.

(20) Āndyğāny, dlāl ṣālḥ: mumārsāt tʿzīz al-ūaʿī bṯqāfẗ al-ʾamn al-sībrānī wā tūṣīāthā fī al-mmlkh al-ʿrbīh al-sʿūdīh, ālmğlh ālʿrbyh llmʿlwmātyh wā āmn ālmʿlwmāt, No. 5. 2021.

(21) Āḥmd, fāṭmh ʿly: ālāmn al-sībrānī wā ālnẓāfh ālrqmyh ,ālmğlh ālmṣryh lʿlwm ālmʿlwmāt bğāmʿẗ bny swyf, Vol. 9, No 2. 2022.

(22) ʿbd al-rḥmn, ʿbd al-rḥmn akrm: tʿzyz ālāmn al-sībrānī dāḫl āldwlh wā dwrh fi ālḥfāẓ ʿla ālāmn ālwṭny drāsh mydānyh ʿla ālārdn mn 2012- 2021, Master dissertation, Jordan: ğāmʿẗ āl al-baīt, 2021.

(23) Bwnyf, sāmy mḥmd: dwr al-mḫṭaṭāt ālāstbāqyh fi mwāğhẗ ālhğmāt ālsybrānyh: ālrdʿ al-sībrānī ānmwḏğān, ālmğlh al-ğzāʾirīh llḥqwq wā ālʿlwm ālsyāsyh, Vol. 4, No. 7. 2019.

(24) Ālʿsāf, ṣālḥ ibn ḥmd: al-mdḫl ilā al-bḫṯ fī al-ʿlūm al-slūkīh,1 st ed., Riyadh: mktbẗ ālʿbykan, 1433h.

(25) Ālğāsr, šʿāʿ ʿbd ālrḥmn: al-iʿlām al-ğdīd wa ālwʿy ālsyāsy, ālmğlh ālʿrbyh lʿlwm ālānsānyh, Vol. 38, No. 151, 2020.