Journal of Al-Farahidi's Arts, No: 64: 368-394
Doi: https://doi.org/10.25130/jfa.18.64.1.15

P-ISSN : 2074-9554 | E-ISSN: 2663-811
Journal of Al-Farahidi's Arts
available online at : fja.tu.edu.iq/index.php/fja

Mohamed Elamin Ahmed Abdel
E-Mail: Muh.alameen91@gmail.com

The Role of Specialized Agencies in Promoting Cybersecurity Awareness: An Analytical Study of the Media Office of the Iraqi Ministry of Interior

Keywords:
Cybersecurity, Cyber awareness, Media Office, Iraqi Ministry of Interior, Content analysis

Article history:

Received	9/3/2025
Received in revised form	21/4/2025
Accepted	11/5/2025
Available online	9/3/2026

E-mail Jaa@ tu.edu.iq

A B S T R A C T

In the current era, countries are increasingly focusing on combating cybersecurity threats that impact both individuals and institutions. Addressing these threats requires enhancing cybersecurity awareness across all segments of society. Specialized agencies, such as the "Media Office of the Iraqi Ministry of Interior," play a crucial role in raising awareness and educating citizens about cybersecurity risks and protection methods.This study aims to assess the effectiveness of the Media Office in increasing cybersecurity awareness among Iraqi citizens, with a focus on analyzing the content of publications on the office's official website. The study employed content analysis methodology to evaluate the effectiveness of the Media Office's strategies and the citizens' response to these publications.The results revealed that the Media Office heavily relies on official and credible sources, and the adopted strategies have proven effective in raising cybersecurity awareness. Additionally, there was significant interaction from citizens with the published content. The study confirmed a clear relationship between the Media Office's strategies and increased cybersecurity awareness.The study recommended measures to further enhance the Media Office's role, including improving current strategies, expanding the scope of media campaigns, increasing event documentation, providing training programs, and conducting periodic studies to measure impact and refine strategies based on the findings.

دور الأجهزة المختصة في تنمية الوعي بالأمن السيبراني المكتب الإعلامي الخاص بوزارة الداخلية العراقية(دراسة تحليلية)

محمد الامين احمد عبد/ ديون الوقف السني

المستخلص:

في العصر الحالي، تولي الدول اهتماماً كبيراً لمواجهة تهديدات الفضاء السيبراني التي تؤثر على الأفراد والمؤسسات بشكل متساوي. لمواجهة هذه التهديدات، يتطلب الأمر رفع مستوى الوعي بالأمن السيبراني عبر كافة شرائح المجتمع. تلعب الجهات المتخصصة، كالمكتب الإعلامي الخاص بوزارة الداخلية العراقية"، دوراً رئيسياً في نشر الوعي وتثقيف المواطنين بشأن مخاطر الأمن السيبراني وطرق الحماية. سعت الدراسة إلى تقييم مدى فعالية المكتب الإعلامي في تعزيز الوعي بالأمن السيبراني بين المواطنين العراقيين، مع التركيز على تحليل محتوى المنشورات على الموقع الرسمي للمكتب. استخدمت الدراسة منهجية تحليل المضمون لتقدير كفاءة الاستراتيجيات التي يعتمدها المكتب الإعلامي واستجابة المواطنين لتلك المنشورات. أظهرت النتائج أن المكتب الإعلامي يعتمد على مصادر رسمية وموثوقة بشكل رئيسي، وأن الاستراتيجيات المتبعة قد أثبتت فعاليتها في تعزيز الوعي بالأمن السيبراني. كما كشفت الدراسة عن تفاعل كبير من قبل المواطنين مع المنشورات التي يتم نشرها. أكدت النتائج وجود علاقة واضحة بين استراتيجيات المكتب الإعلامي وزيادة الوعي بالأمن السيبراني. وقدمت الدراسة توصيات تهدف إلى تعزيز دور المكتب الإعلامي بشكل أكبر، تشمل تحسين الاستراتيجيات الحالية، توسيع نطاق الحملات الإعلامية.

الكلمات المفتاحية : الأمن السيبراني، تنمية الوعي، المكتب الإعلامي لوزارة الداخلية، العراق

المقدمة

اهتمت الدول في عصرنا الحالي بمحاربة تهديدات الفضاء السيبراني كونها تستهدف الأفراد والمؤسسات على حد سواء ويتطلب التصدي لهذه التهديدات زيادة الوعي بالأمن السيبراني بين كافة فئات المجتمع حيث تلعب الأجهزة المختصة ومنها "المكتب الإعلامي الخاص بوزارة الداخلية العراقية" دوراً هاماً في نشر الوعي بالمخاطر الخاصة بالأمن السيبراني وطرق الحماية منه.

تستهدف هذه الورقة البحثية إلى تقييم دور المكتب الإعلامي في نشر الوعي بالأمن السيبراني بين المواطنين العراقيين، مع التركيز على تحليل مضمون المنشورات على الموقع الرسمي للمكتب الإعلامي.

إشكالية البحث

لقد احتل الاهتمام بالأمن السيبراني المراكز الأولى كونه يؤثر على المعلومات التي تربتط بالأمن القومي، وهنا تبرز الحاجة إلى فهم مدى فعالية استراتيجيات نشر الوعي حول الأمن السيبراني من خلال تحليل محتوى منشورات المكتب الإعلامي الخاص بوزارة الداخلية العراقية.

السؤال الرئيسي :

ما هو دور المكتب الإعلامي الخاص بوزارة الداخلية العراقية في نشر الوعي بالأمن السيبراني؟

الأسئلة الفرعية:

1. ما مدى فعالية استراتيجيات المكتب الإعلامي في تنمية الوعي بالأمن السيبراني بين المواطنين؟
2. ما مدى تفاعل المواطنين مع مضمون المنشورات الخاصة بالأمن السيبراني والصادرة من قبل"المكتب الإعلامي"الخاص بوزارة "الداخلية العراقية"؟

أهمية البحث

- إلقاء الضوء على الأهمية للدور المكتب الإعلامي بوزارة الداخلية العراقية في نشر الوعي بالأمن السيبراني.
- اكتشاف نوعية المنشورات والمعلومات المقدمة من قبل المكتب الإعلامي عن الأمن السيبراني.
- تقديم توصيات لتحسين استراتيجيات نشر الوعي بالأمن السيبراني.

أهداف البحث

1. تقييم فعالية استراتيجيات المكتب الإعلامي في زيادة الوعي بالأمن السيبراني بين المواطنين.
2. تحليل مضمون المنشورات من قبل المكتب الإعلامي الخاص بوزاة الداخلة العراقية حول الأمن السيبراني.
3. تقديم توصيات لتحسين جودة وفعالية المحتوى المنشور للمساهمة في رفع قدرة المكتب الإعلامي لتعزيز الوعي بالأمن السيبراني.

فرضيات البحث

الفرضية الرئيسية:

"يفترض وجود علاقة ذات دلالة إحصائية بين دور المكتب الإعلامي الخاص بوزارة الداخلية العراقية وبين تنمية الوعي بالأمن السيبراني".

الفرضيات الفرعية:

1. يفترض وجود "علاقة ذات دلالة إحصائية" لاستراتيجيات المكتب الإعلامي وبين الوعي بالأمن السيبراني بين المواطنين.
2. يفترض وجود علاقة ذات دلالة إحصائية بين مضمون المنشورات الصادرة من قبل المكتب الإعلامي وبين قدرته على نشر الوعي بالأمن السيبراني.

منهجية البحث

ستتبنى هذه الدراسة على المنهج الوصفي التحليلي مع التركيز على مضمون المنشورات وتحليل البيانات بهدف وصف وفهم دور المكتب الإعلامي في تعزيز الوعي بالأمن السيبراني.

أداة البحث:

اعتمدت الدراسة على طريقتين لجمع البيانات:

أولاً: تحليل مضمون المنشورات على الموقع الرسمي للمكتب الإعلامي الخاص بوزارة الداخلية العراقية والمتعلقة بالأمن السيبراني.

ثانياً: استبانة مصممة تبعاً للمحاور البحثية، وسوف يتم توزيعها إلكترونيًا على عينة 384 من طلاب الكليات (العلمية والإنسانية)، تتضمن الاستبانة أسئلة تعتمد على مقياس ليكرت الخماسي، مما يتيح للمشاركين تقييم كل بند بناءً على مدى موافقتهم.

تحليل البيانات:

يتم استخدام برنامج SPSS لتحليل البيانات، بالإضافة إلى الاعتماد على عدد من البرامج الإحصائية الأخرى، سيتم تحليل إجابات المشاركين وفقاً للمحاور البحثية، وتحليل مضمون المنشورات لفهم مدى تأثيرها على تنمية الوعي بالأمن السيبراني.

المبحث الأول: الإطار النظري

المطلب الأول: الأمن السيبراني (تعريفه ، أهميته، استراتيجياته)

الأمن السيبراني

يتكون مصطلح "الأمن السيبراني" من كلمتين: "الأمن" و"السيبراني". "الأمن" يعني الأمان وعدم الخوف، حيث يشير إلى حالة من الاطمئنان النفسي والسكينة وزوال الخوف. على سبيل المثال، في القرآن الكريم قال الله تعالى: ﴿وَإِذْ قَالَ إِبْرَاهِيمُ رَبِّ اجْعَلْ هَذَا بَلَداً آمِناً وَارْزُقْ أَهْلَهُ مِنَ الثَّمَرَاتِ﴾.

من ناحية تقنية، يعرف الاتحاد الدولي للاتصالات "الأمن السيبراني" على أنه عدة إجراءات مثل السياسات الأمنية، والإجراءات، والمبادئ التوجيهية، وأساليب إدارة المخاطر، والتدريبات

والممارسات والتقنيات المستخدمة لحماية "البيئة السيبرانية"، والمنشآت، والمستخدمين(خليل، 2012، ص. 38).

التعريف الاصطلاحي للسيبرانية

تعددت تعريفات "السيبرانية" ولكنها تتفق على أنها تتعلق بحماية الأنظمة والشبكات والبرامج من الهجمات الرقمية. هذه الهجمات قد تستهدف مواقع إلكترونية عبر وسائل إلكترونية أخرى. وتشمل هذه التعريفات الممارسات الاحتياطية الاستباقية قبل حدوث أي خلل، والإجراءات العلاجية بعد حدوث الخلل(الطيار، 2020، ص. 264).

لقد أولى اهتماماً كبيراً بمفهوم الأمن السيبراني مؤخراً بسبب التطور التقني الحديث واستخدامها على نطاق واسع، حيث إن المعهد الوطني للمعايير والتكنولوجيا (NIST) عرف الأمن السيبراني على أنه حماية الأصول المعلوماتية من التهديدات التي تتعرض لها المعلومات أثناء معالجتها وتخزينها ونقلها عبر أنظمة المعلومات المتداخلة بين الشبكات(National Institute of Standards and Technology, 2018).

أما الوكالة الفرنسية لأمن أنظمة المعلومات(ANSSI) ، فتصف الأمن السيبراني على أنه فضاء تواصل يشمل الربط البيئي العالمي للمعدات المعالجة للبيانات الرقمية، ولا يقتصر على شبكة الإنترنت فقط، بل يشمل أيضاً شبكات عالمية وخاصة"(Gps/ AcARs/swift/psth)" (صفاء، & مهدي، 2020، ص.49).

وفي كتاب "Cyber Security Analytics: Technology and Automation" لـــ Martti Lentoو Pekka Nettaanmaki ، يتم تعريف الأمن السيبراني بأنه مجموعة من الإجراءات المتخذة للدفاع ضد الهجمات السيبرانية وعواقبها، وتنفيذ التدابير المضادة المطلوبة (الشمري، إسماعيل، 2020، ص.277)، وتكوين رؤى حول كيفية تحسين وحوكمة أمن معلومات المنشأة وجهود إدارة المخاطر(Ramirez et al., 2022).

الأمن السيبراني، والذي يُعرف أيضًا بأمن الحاسوب أو أمن المعلومات، ويشار إليه باللغة الإنجليزية بـــ Cybersecurity، هو أحد فروع علم التكنولوجيا الذي يهدف إلى حماية المعلومات من الوصول غير المصرح به، أو التعديل، أو التدمير، أو الابتزازيهدف هذا المجال إلى حماية الدول والأفراد من التهديدات التي قد تؤدي إلى تعطيل العمليات التجارية أو

الحصول على المال بطرق غير مشروعة((وزارة الاتصالات وتكنولوجيا المعلومات، 2021، ص.18).

ترتبط بالأمن السيبراني العديد من المصطلحات مثل "الردع السيبراني" (Cyber Deterrence) (هيئة الإعلام، 2021)، الذي يعرف على أنه حظر أعمالٍ ضارة ضد أصولٍ وطنية بالفضاء الرقمي. و"الهجمات السيبرانية" (Cyber Attacks) (العنزي، 2021)، التي تعني أي فعل يضعف من قدرات ووظائف الأنظمة الإلكترونية(Evelyne, 2020, p.231). و يُعرف الأمن السيبراني إجرائياً بحماية الأفراد وبياناتهم وحساباتهم من الهجمات الإلكترونية للحفاظ على سلامة ونزاهة المعلومات المخزنة داخل الأنظمة الإلكترونية.

الأمن السيبراني وأهميته:

يرتبط الأمن السيبراني بشكل وثيق بالجريمة الإلكترونية كونها تُمارس في البيئة الإلكترونية أو الافتراضية من قِبل أفراد أو منظمات تتمتع بذكاء ومعرفة تقنية متطورة. تسبب هذه الجرائم خسائر كبيرة للمجتمع. في عالمنا المترابط عبر الإنترنت، يبرز الأمن السيبراني كعنصر أساسي في الحياة اليومية، ويؤثر على المستويات السياسية والاقتصادية والاجتماعية. أصبح الأمن السيبراني الآن محور الحياة المعاصرة، الذي يعتمد عليه كل من الدول والأفراد في جميع تعاملاتهم.

بالإضافة إلى ذلك، يُنظر إلى الأمن السيبراني كرافد جديد للأمن القومي وجزء من الأمن الجماعي. تتزايد العلاقة بين الأمن والتكنولوجيا، ومع تعرض المصالح الاستراتيجية لمخاطر إلكترونية، يمكن أن تتحول الأنظمة الإلكترونية إلى وسيلة وأداة للصراع الدولي، مما يساهم في تغذية التوترات الدولية(الفرحان، 2021، ص.2246).

استراتيجيات الأمن السيبراني:

يعد الأمن السيبراني الآن جزءًا بالغِ الأهمية في "الثورة الصناعية الرابعة" (Industry 4.0) وفي جميع شركات التصنيع والتصميم، ذكر الباحثون Raicu, G.& Raicu,A. (2022) في دراستهم استراتيجيات جديدة للأمن السيبراني في الثورة الصناعية الرابعة، حيث يجب مراعاة الثغرات الحالية وعمليات الاستغلال المحتملة، وناقلات الهجوم، والهجوم، والتسوية، ومؤشرات الأداء، كما يعد الخطر السيبراني في إدارة دورة حياة المنتج محوراً بالغ الأهمية،

إذ يكشف عن مشكلات التوثيق، والاتصالات غير المؤمنة، وقضايا النشر الافتراضي، وقابلية التعرض للهجمات الفيزيائية.

وكان من الضروري اتخاذ تدابير مناسبة للمعالجة، يأتي من بينها التعليم في مجال الأمن السيبراني، لذا فإنه من الضروري تنفيذ سياسات وخطط تقليل المخاطر المناسبة في إدارة دورة حياة المنتج لمنع "الهجمات السيبرانية"(Raicu & Raicu, 2022).

استراتيجيات الأمن السيبراني تتضمن العديد من الإجراءات والممارسات لضمان حماية الأنظمة والشبكات من التهديدات السيبرانية، نذكر منها:

- ✓إحدى هذه الاستراتيجيات هي التوعية والتدريب، حيث يجب أن يكون لدى الموظفين معرفة وفهم عميقين حول ممارسات الأمن السيبراني. تتضمن تلك التدريبات المنتظمة على كيفية التعرف على التهديدات لتجنبها. وفقا لتقرير صادر عن معهدSANS ، فإن تدريب الموظفين باستمرار هو أحد العوامل لمنع تلك الهجمات(SANS Institute, 2021).
- ✓ينبغي على الشركات أيضًا تنفيذ تقييمات دورية للمخاطر لتحديد نقاط الضعف في الأنظمة الأمنية وتحديثها بشكل منتظم وقد أكدت شركة Gartner على أهمية التقييم الدوري للمخاطر كجزء من استراتيجية الأمن السيبراني الفعالة (Gartner, 2020).
- ✓استخدام تقنيات التشفير يعتبر جزءًا أساسيًا من "حماية المعلومات" الحساسة أثناء نقلها أو تخزينها حيث ينصح المعهد الوطني للمعايير والتكنولوجيا (NIST) باستخدام التشفير لحماية البيانات الحساسة National Institute of Standards and Technology, (2021).
- ✓تساعد جدران الحماية وأنظمة الكشف عن التسلل في منع الهجمات غير المصرح بها على الشبكات وقد أشار تقرير من مؤسسة CISCO إلى فعالية جدران الحماية والأنظمة الخاصةبكشف التسلل في تأمين الشبكات(Cisco, 2020).
- ✓يجب التأكد من تحديث جميع البرامج والنظم بانتظام لسد الثغرات الأمنية المعروفة. يوصي مركز أمان الإنترنت (CIS) بتحديثات البرامج الدورية كجزء من أفضل الممارسات في الأمن السيبراني (Center for Internet Security, 2021).

المطلب الثاني: المكتب الإعلامي الخاص بوزارة الداخلية العراقية

يلعب المكتب الإعلامي الخاص بوزارة الداخلية العراقية دوراً حيوياً كحلقة وصل بين الوزارة والمجتمع، بما في ذلك الجهات الإعلامية والمواطنين. يُعنى المكتب بتغطية الأنشطة والفعاليات المتعلقة بالوزارة، وإدارة صفحات التواصل الاجتماعي لضمان تواصل فعّال ومستمر. يقوم المكتب أيضاً بتقديم التسهيلات اللازمة لعقد المؤتمرات والاجتماعات، بالإضافة إلى متابعة ما يُعرض في وسائل الإعلام المختلفة وتقديمه للجهات المعنية. كما يضطلع المكتب بتنظيم مواعيد مقابلات المسؤولين مع المواطنين ومنتسبي الوزارة، مما يسهم في تعزيز الشفافية والتواصل المباشر مع المجتمع (وزارة الداخلية العراقية، د.ت).

إن الموقع الرسمي يتضمن عدة أقسام منها: قسم الأخبار، وقسم نشاطات العلاقات و الإعلام ويشمل قسم محاربة الشائعات، وقسم التوجيه المعنوي حيث كانت له عدة مهام منها إلقاء المحاضرات في " قيادة قوات حفظ القانون"، بالإضافة إلى التوجيه المعنوي وقد شرع أخيراً إقامة حملات توعوية تثقيفية في " مدينة كربلاء المقدسة"، وقد عمل قسم نشاطات العلاقات والإعلام بالتزامن مع أيام عاشوراء على الاستمرار ببث رسالتها التحصينية والتوعوية بين جموع المعزين، وكان من ضمن منهج الوزارة هو العمل على دعم أصحاب المحتوى الإيجابي وقد ذكر الموقع أن طبيباً عراقياً قد دخل موسوعة غينيس بتحقيقه أعلى مشاهدات طبية " ، يحتوى الموقع أيضاً على قسم أخبار الشرطة المجتمعية وكانت آخر الأخبار التي نشرها الموقع عن تحرير فتاة من التعنيف الأسري في محافظة الأنبار، والاستمرار بتنفيذ الحملات التطوعية والخدمية في المدارس، وأخبار أخرى عن توصيات الوزارة وجهودها لمتابعة الجمهور وتلقي البلاغات وغيرها"(وزارة الداخلية العراقية، د.ت).

المبحث الثاني: الأدبيات السابقة

(استراتيجيات نشر الوعي بالأمن السيبراني وأهمية التعاون بين الأجهزة الحكومية لتعزيزه)

المطلب الأول: استراتيجيات نشر الوعي بالأمن السيبراني

تعد جرائم الأمن السيبرانية امتداداً طبيعياً للثورة الرقمنة، وقد ازدادت بشكل ملحوظ على مدى الفترة الماضية وتطورت من قضايا ثانوية إلى رئيسية وظاهرة "عالمية" حتى إن ذلك كان يؤثر على أعداد كبيرة من الأشخاص نظراً لتعرضهم للقرصنة أو السرقة والأذى بسبب تلك الجريمة حيث إنها تعد من أخطر التحديات التي تواجه المجتمع العالمي في العصر

الرقمي،وتُظهر الدراسات أنها تتزايد باستمرار، مما يفرض تحديات كبيرة على الأفراد والمؤسسات والحكومات. وفقاً لتقرير صادر عن معهد الدراسات الأمنية(Kshetri, 2013) فإن الجريمة السيبرانية يمكن أن تتسبب في خسائر مالية هائلة وتؤثر سلباً على الاقتصاد العالمي.

وتتطلب مكافحتها استراتيجيات متعددة الجوانب، تشمل تعزيز البنى التحتية للأمن السيبراني، والعمل على تطوير تشريعات مناسبة قانونية ، وتوعية الأفراد لحماية بياناتهم الشخصية. يشير تقرير من مركز الدراسات الاستراتيجية والدولية (Lewis, 2018) إلى أن التعاون الدولي وتبادل البيانات بين الدول يمكن أن يلعب دوراً بغاية محاربة الجرائم السيبرانية. من خلال تعزيز التعاون بين القطاعين العام والخاص وتطوير القدرات التقنية والبشرية، يمكن تحقيق تقدم ملموس في حماية المجتمع من تهديدات الجريمة السيبرانية، بالإضافة لصعوبة كشف مرتكبيها سوى بأساليب تقنية عالية ودقيقة (العنزي، 2021، ص.112).

شهدت ثورة المعلومات والمعرفة تطورًا هائلًا منذ بداية القرن التاسع عشر، مما أدى لحدث تغييرات في : القطاعات الأمنية والزراعية والخدماتية والصناعية وغيرها. أصبحت المعلومات والمعرفة الآن أساسًا للكثير من السلع والخدمات الحديثة، حيث يتطلب إنتاج السلع الرقمية أو المعلوماتية خبرة كبيرة. كما أن المعلومات تتسم بالتبدل والتغير المستمر، مما يجعلها بمثابة شريان الحياة للمؤسسات المعتمدة على قواعد ثابتة ترتكز على تكنولوجيا المعلومات(الجلفاوي، 2021، ص. 77).

في ظل التطورات التكنولوجية المستمرة، وتنوع أدوات القوة، وتطور طبيعة الحروب عبر أجيالها المختلفة، تزداد أهمية تحقيق الردع السيبراني، والذي بات معيارًا لمدى قدرة الدول على حماية نفسها من محاولات الاختراق وتأمين بياناتها ومعلوماتها، وحماية أمنها القومي. ذلك خاصةً في ظل استخدام بعض الدول والفاعلين من غير الدول، كالمنظمات الدولية والجماعات الإرهابية، للفضاء الإلكتروني لتحقيق أهدافهم في الصراعات المختلفة. تطور مفهوم الحروب السيبرانية، وتعززت القدرات التي تهدد الأمن وتعوق التنمية، حيث تضاعف الخطر الإلكتروني مع تقدم الوسائل التكنولوجية (السيد، 2021، ص.86)

يقع على عاتق الإعلام مسؤولية كبيرة في مواجهة تهديدات الأمن الفكري(غازي، 2022، ص.14)، الذي يعني سلامة فكر الإنسان من الانحراف لتحقيق الاستقرار بالمجتمعات، وهو

ما يتضمن رفع مستويات التوعية بمجال الفضاء الإلكتروني كونه أداة لتحقيق ميزة نسبية في (الصراعات الدوليةِ الحديثة)، ليؤثر سلبًا على مستوى الأمن المعلوماتي العالمي.نتج عن ذلك تحول في مفهوم القوة واستبدال القوى العسكرية التقليدية، التي تشمل الأدوات العسكرية والقوة الصلبة، بمفهوم القوة الإلكترونية. هذه القوة الإلكترونية لا تخضع لقوانين دولية واضحة، مما يجعلها تختلف تمامًا عن القوة التقليدية التي يحكمها القانون الدولي.

لهذا السبب، ساد الاعتقاد بأن وسائل الإعلام تمتلك القدرة على تغيير اتجاهات الأفراد والسيطرة عليهم، حيث أن وسائل الإعلام قد حلت محل العنف والقهر في السيطرة على الجماهير واستلاب عقولهم، من خلال اللعب على نفسيتهم وإقناعهم بواقع جديد عبر طرح قضايا منطقية تؤثر على المتلقين وتجعلهم يؤيدون الطرح الذي تتبناه تلك الجهة على حساب الجهة الأخرى، تهدف أية عملية اتصالية إلى إقناع المتلقي والتأثير فيه معرفياً ونفسياً وسلوكياً من خلال تزويده بالمعلومات والبيانات، سواء كانت صحيحة ضمن سياقاتها الطبيعية أو معلومات ناقصة أو حتى كاذبة ومفبركة، ويتم ذلك بأساليب وبرامج متنوعة عبر مواقع التواصل الاجتماعي(الراجحي، 2018).

إن انتشار تقنيات الاتصالات الحديثة والإعلام قد فرض واقعاً سيبرانياً جديداً أصبح يُعرف بالفضاء السيبراني أو الافتراضي، الذي أثر على حياة الأفراد والمجتمعات وأدى إلى ظهور العديد من الجرائم الإلكترونية أو ما يعرف بجرائم المعلومات، تزامناً مع التطورات المتلاحقة للتقنية والتكنولوجيا(السيد، 2021).

إذ تعتمد استراتيجيات تلك الحرب النفسية للمعلومات على تزويد المتلقي بمجموعةٍ متناقضةٍ من المعلومات في آنٍ واحدٍ، لضعنا في حالة من الحيرة والشك، ويؤدي إلى تشظي الرأي العام الأولي المعارض وإعادة تشكيله ليتفق مع الهدف المطلوب كما يمكن للمعلومات والإشاعات التي تروجها الجهات المستخدمة أن تؤدي لتشكيل رأي عام يتبلور في الاتجاه الذي تسعى لتحقيقه(الداعمي، 2019، ص.15).

تتطلب السيطرة على الرأي العام حالياً، التحكم بوسائل الإعلام الاجتماعي الحديثة والتكنولوجيا للوصول إلى أوسع شريحة من الجمهور المهتم بالقضية المطروحة. نظرًا لقدرة وسائل الإعلام، التقليدية والحديثة، على الوصول إلى أعداد كبيرة من الناس والتأثير عليهم بسهولة، أصبحت وسائل الإعلام الرقمية منصة شائعة الاستخدام وفقًا للنوايا الاجتماعية

والأيديولوجية. وقد أدى هذا إلى استخدامات غير مشروعة وضعت المجتمعات والدول في مواقف حرجة. ظهرت أشكال من تلك الجرائم: مثل التسلل والاختراق للمواقع، وتدمير البيانات الحساسة أو سرقتها واستغلالها، وسرقة الأموال، وانتهاك الأمن والخصوصية(سلام، & وكهينة، 2020، ص.485).

يلعب الإعلام دورًا جوهريًا وأساسياً في مختلف جوانب الحياة الإنسانية والثقافية والاجتماعية والأمنية والسياسية. يعتبر الإعلام وسيلة للنمو والتنمية والاستقرار في المجتمعات، ويؤدي دورًا رئيسيًا في نشر وتفعيل الوعي الأمني، ودعم عمل الجهات الأمنية في مواجهة الاختراقات التي تهدد استقرار المجتمعات وأمنها (جابوربي، 2020، ص. 487). تسعى العديد من الجهات المؤثرة دائمًا لتوجيه الرأي العام لخدمة أغراضها الشخصية، وكسب تأييد الجمهور لوجهة نظرها. لذلك، فإن السيطرة على وسائل الإعلام الاجتماعي والتكنولوجيا صارت أمرًا أساسياً للوصول إلى الفئة المستهدفة من الرأي العام.

يُعرف هذا النمط الإعلامي بعدة مسميات تُستخدم بالتبادل مع الإعلام السيبراني، مثل الإعلام الجديد، الإعلام الإلكتروني، والإعلام الرقمي. جميع هذه المسميات تشير إلى نفس المفهوم، وهو الإعلام عبر الوسائط المختلفة المتاحة على شبكة الإنترنت والفضاء الافتراضي واعتبرت هذه الأدوات الحديثة وسائل أساسية لنقل الأخبار والمعلومات بشكل مستمر وأفكارٍ تجاوزت حدود المجتمعات (أسماء، 2020، ص. 54).

يتحمل الإعلام مسؤولية كبيرة في التصدي لمواجهة تهديدات الأمن الفكري، إذ تزايدت القدرات التي تهدد الأمن مع تصاعد المخاطر الإلكترونية بشكل متزامن مع التقدم الكبير في المجال(غازي، 2022، ص. 14). يلعب الأمن الفكري دورًا أساسيًا في تمكين الشباب من مواجهة الانحرافات، والحد من ثقافة العنف والتطرف والجريمة، وذلك من خلال توعية الأفراد والمؤسسات عبر الإعلام لتعزيز الأمن الفكري والتغلب على المعوقات التي تعترضه(القحطاني، 2019، ص.496).

المطلب الثاني: التعاون بين الأجهزة الحكومية لتعزيز الأمن السيبراني:

في السنوات الأخيرة، شهد حجم البيانات زيادة ملحوظة نتيجة الاعتماد على إنترنت الأشياء لبناء الأنظمة المترابطة، مثل الأنظمة العسكرية الذكية، وزيادة التطبيقات المرتبطة بوسائل التواصل الاجتماعي كالنصوص والصور والصوتيات والفيديو. تلعب البيانات الضخمة دوراً

مهماً في المجال العسكري، إذ تعزز القدرة على اتخاذ قرارات استراتيجية أكثر دقة وتحسين جوانب الأمن والدفاع (سفاح، 2023).

تُستخدم البيانات الضخمة بطرق متعددة، منها:

تحليل المخاطر والاستخبارات: وهي تساهم في جمع وتفسير البيانات من مصادر متنوعة، بما في ذلك البيانات الجغرافية أو الاجتماعية أو الاقتصادية أو العسكرية. يساعد ذلك في إدراك التهديدات الأمنية وفحص "القضايا الجيوسياسية"، ويدعم صناع القرار في تطوير استراتيجياتهم العسكرية.

التنبؤ بالحدث:من خلال الاعتماد على: تقنيات منها البيانات الضخمة وتعلم الآلة لإنشاء نماذج تنبؤية تساعد في توقع الأحداث مستقبلاً، كالتحركات العسكرية المحتملة أو "تغيراتٍ جيوسياسية".

وهي تتيح تحليل لمحتوى المرئي سواءً (الصور ومقاطع الفيديو) المأخوذة من مصادر متنوعة، مثل الأقمار الصناعية والطائرات بدون طيار، لاستخلاص المعلومات الأساسية.

التدريب والمحاكاة: من خلال المساهمة في تطوير بيئات تدريبية افتراضية ومحاكاة لتدريب القوات العسكرية على سيناريوهات مختلفة.

ويعد استثمار المسؤولين في المجال العسكري ومراكز الدراسات في البيانات الضخمة أمراً ضرورياً لاستخراج الدلالات المهمة في شأن الأمن القومي للمواطنين والعسكريين، فعلى سبيل المثال، نجد إدارة الجيش الأمريكي قد أظهرت اهتماماً بتحديد العوامل التي تدفع الجنود إلى الانتحار وتحديد المخاطر المرتبطة بها في حين وقد وجد صناع القرار أن " البيانات الضخمة" لعبت الدور المحوري في تحديد الأنماط السلوكية الخاصة بالجنود. لذا، قامت إدارة الجيش بجمع كمية كبيرة من البيانات المتعلقة بالجنود بهدف تحديد العناصر الأكثر عرضة للانتحار (سفاح، 2023).

الفيروسات وحرب المعلومات

تؤدي فيروسات الحاسوب دوراً محورياً في إطار حرب المعلومات والحروب الإلكترونية. تُعتبر تلك الفيروسات والبرمجيات الخبيثة أدوات "استراتيجية" لتوظف في الهجمات السيبرانية لتحقيق أهداف محددة. مع زيادة التهديدات المتوقعة من هذه الفيروسات واستخدامها لأغراض عسكرية، بدأت الدول في اتخاذ إجراءات لمواجهتها.

تمتلك الدول المتقدمة موضوعات ذات درجة عالية من السرية، وقد فرضت قيوداً على نشر الأبحاث الفنية التي قد تكشف عن أسرار الحاسبات الحديثة ونظم التشغيل المستخدمة في المجالات العسكرية والمدنية،حيث كان أحد الأمثلة الحديثة على هذا النوع من الأسلحة هو الفيروس"Stuxnet" ، الذي أعلنت إيران في 25 سبتمبر 2010 أن وحداتها الصناعية تعرضت لهجمات إلكترونية بسببه،ووفقاً للعديد من التقارير يُعدStuxnet" أحد أكثر الأدوات تعقيداً المستخدمة حتى الآن، حيث يستهدف هذا الفيروس أنظمة التحكم الصناعية التي تُستخدم على نطاق واسع في مراقبة الوحدات الآلية(McMillan, 2010)،كما يتميز "Stuxnet" بحجمه الكبير وتشفيره المعقد، ويعتمد على تقنيات ذكية جديدة ولا يحتاج إلى تدخل بشري، حيث يكفي أن توجد بطاقة ذاكرة مصابة به ليبدأ في العمل.

نظرًا لتعقيده وتطوره، يُعتقد أن "Stuxnet" من صنع دولة، ويستهدف منشآت حيوية. بناءً على هذا الاستنتاج، افترضت العديد من المصادر أن مفاعل بوشهر الإيراني قد يكون الهدف الأساسي لهذا الفيروس(Reuters, 2010).

الجيش الإلكتروني

تشير الجيوش الإلكترونية إلى مجموعات متخصصة في مجال الحرب الإلكترونية والأمن السيبراني، والتي تسهم في حماية الأصول الرقمية بالإضافة للبنى التحتية وكذلك (البيانات الحساسة) من الهجمات الإلكترونية والتجسس أو الهجمات السيبرانية.

الجيوش الإلكترونية وأنواعها:

- الجيش السيبراني :(Cyber Army) فهو ينفذ عمليات الدفاع السيبراني والرد على الهجمات الإلكترونية، وقد يكون جزءاً من "القوات المسلحة العامة" أو كيانات مستقلة.
- وحدة الأمن السيبراني :(Cyber Security Unit) تعمل هذه الوحدات ضمن الشرطة أو جهات إنفاذ القانون، مستهدفةً مكافحة الجرائم الإلكترونية والابتزاز ومراقبة الأنشطة السيبرانية الضارة.
- الجيش الإلكتروني الهجومي :(Offensive Cyber Army) يستخدم قدراته لتنفيذ هجمات إلكترونية ضد الأهداف المعادية التي تؤثر على السياسة والأمن والاقتصاد.

- وحدة استخبارات الجيوش الإلكترونية :(Cyber Intelligence Unit) تهتم بجمع وتحليلها للمعلومات السيبرانية والاستخبارات الإلكترونية لتحديد التهديدات المحتملة والثغرات في أنظمة الأمان.
- الجيوش الإلكترونية الخاصة :(Special Cyber Forces) هي وحدات خُصصت لتنفيذ للمهام السيبرانية الحساسة والعمليات السرية.

ووفقاً لمعهد راند، وهو مؤسسة بحثية أمريكية مستقلة، هناك خمس دول تُعد الأقوى في مجال الجيش الإلكتروني ، بالإضافة للهجمات السيبرانية ، مرتبة من الأقوى إلى الأضعف بناءً على مستويات البنى التحتية، والقدرات ومواقع الرصد والميزانية المخصصة لتلك الأنماط من الحروب الإلكترونية، و تتصدر الولايات المتحدة القائمة، تليها الصين، ثم روسيا، وإسرائيل في المركز الرابع، وبريطانيا في المركز الخامس. بالإضافة إلى ذلك، هناك دول بارزة أخرى مثل إيران وكوريا الشمالية(RAND Corporation, n.d.).

- **نقاط القوة في العراق**

تتضمن نقاط القوة الرئيسية في العراق، التي يمكن اعتبارها أسسًا إيجابية لتطوير إطار عمل فعال للحماية الهيئات من الهجمات السيبرانية والحرب المعلوماتية، ما يلي:

"**إصدار وثيقة سياسات ومعايير حماية أمن المعلومات:** تسعى تلك الوثيقة إلى تحديد الأطر والسياسات والمعايير اللازمة، وتوضيح الأدوار والمسؤوليات داخل المؤسسات، مما يعزز قدرتها على الحماية الذاتية من الهجمات السيبرانية.

""**موافقة المجلس الوزاري للأمن الوطني على تشكيل الفريق الوطني للاستجابة للحوادث والتهديدات السيبرانية**": يختص ذلك الفريق المشترك في مجال الأمن السيبراني والاستجابة للحوادث السيبرانية، ويعمل أيضًا على حماية البنية التحتية للإنترنت ونشر الوعي حول حماية الخصوصية والحماية الذاتية للأفراد والمنظمات على الإنترنت.

"**تأمين وحماية الشبكات ومراكز البيانات الوطنية والمواقع الرسمية**": يتولى الفريق الوطني مسؤولية تأمين وحماية الشبكات ومراكز البيانات الوطنية والمواقع الرسمية المتعلقة بالقضاء السيبراني في العراق، كما يعمل على تنسيق الجهود ودعم المؤسسات في "القطاعي الخاص أو العام" لحماية نفسها وخدماتها في الفضاء السيبراني(كريم، 2023).

المبحث الثالث: الإطار التطبيقي

المطلب الأول:

- تحليل المضمون للمنشورات الصادرة من قبل المكتب الإعلامي الخاص بوزارة الداخلية العراقية.
- سوف تتضمن استمارة تحليل المضمون الفئات التالية:
- وسوف نتبع عدة أسئلة في تحليل المضمون الإعلامي تتمثل في: "كيف قيل، من القائل، ماذا وأين قيل؟"

فئة المصدر سواء كان الفئة شخص أو مجموعة، فئة الاتجاهات: هل محايدة أو مؤيدة أو معارضة، فئة الاستمالة (الأسلوب الإقناعي) مثل الأدلة والبراهين أو التأثير ، فئة الصور: (مصاحبة الخبر بصورة، أو رسم أو محتوى آخر)، القوى الفاعلة: الشخصية المتحدثة هل هي شخصية رسمية أو من العامة.

الموقع	"المصادر"	التكرارات	النسبة %
المصدر (أين؟)	مصدر داخلي	10	%52
	مصدر خارجي	9	%48
القوى الفاعلة (من ؟)	المجموع	19	%100
	شخصية رسمية	18	%75
	عامة	6	%25
	المجموع	24	%100
الاستمالة (الأسلوب الإقناعي) (كيف؟)	منفعية	6	%38
	عقلية /ذهنية	19	%73
	عاطفية / تحذيرية	1	%3
المجموع		26	%100
الصور (كيف؟)	لحظية /تفاعلية	36	%97
	رمزية	1	%3
	لا يوجد صورة	0	
المجموع		37	%100

كان المصدر الداخلي قد حظي بنسبة أعلى وهي 52%، أما فئة القوة الفاعلة فكانت الشخصيات الرسمية متمثلة في مكتب وزير الداخلية هي النسبة الأعلى عن الشخصيات العامة وكانت بنسبة 75%، أما نوع الاستمالة فكانت ذهنية وعقلية بمعنى أنها وثقت بالبراهين ، أما المنفعية فكانت بنسبة 38%، والتحذيرية بنسبة 3%، ثم كانت فئة الصور التفاعلية اللحظية هي الأعلى نسبة وهي97% مما يعني توثيق الحدث لحظة بلحظة ولم يكن هناك أي خبر غير موثق بالصور ثم حظيت الصور الرمزية على ما نسبته 3%.

معظم الأخبار الخاصة بالوعي عن الأمن السيبراني كانت قد حظيت بتأييد المتابعين ولم يكن هناك نسبة للتعارض أو السلبية بل إن متابعين الموقع الرسمي كانوا يؤدون الجهود المبذولة من قبل وزارة الداخلية بل قاموا أيضاً بمشاركة الأخبار على صفحاتهم الشخصية.

المطلب الثاني: تحليل البيانات ،وعرض النتائج، ومناقشتها

الإطار التطبيقي

منهجية البحث:

اعتمدت الدراسة منهجاً وصفياً تحليلياً، من خلال التعرف على متغيرات الدراسة وجمع البيانات ،وتحليلها، وتفسيرها بطريقة دقيقة ومنهجية بهدف إعطاء تفسير ونتائج تحقق أهداف الدراسة

مجتمع وعينة الدراسة:

يتكون مجتمع الدراسة الحالية من طلاب الكليات العلمية والإنسانية العراقية واستخدمت الدراسة أسلوب العينات للحصول على بيانات الدراسة وتم نشر الرابط الخاص بالاستبيان على كافة مواقع التواصل الاجتماعي الخاصة بأفراد مجتمع الدراسة وقد بلغ عدد أفراد عينة الدراسة 384 فرد وهم الذين قاموا بالإجابة على أسئلة استمارة الاستبيان الالكتروني

الأساليب الإحصائية:

استخدمت الدراسة برنامجSPSS لتحليل بيانات الدراسة من خلال الأساليب الاحصائية التالية (معامل الفاكرونباخ– معامل ارتباط بيرسون – النسب والتكرارات – الوسط الحسابي والانحراف المعياري)

أداة الدراسة

تكونت استمارة الاستبيان من قسمين يتضمن القسم الأول البيانات الشخصية لأفراد عينة الدراسة (الجنس، العمر، المستوى الدراسي) ويشتمل القسم الثاني علي العبارات المتعلقة بمحور دور المكتب الإعلامي الخاص بوزارة الداخلية العراقية ويتضمن بعدين (استراتيجيات المكتب الإعلامي، المنشورات الصادرة من المكتب الإعلامي) ويشتمل على 10 عبارات ومحور الوعي بالأمن السيبراني ويشتمل على 10 عبارات وتم استخدام مقياس ليكرت ذو الخمس درجات في الإجابة على عبارات الدراسة

جدول (1) مستويات الاستجابة على عبارات أداة الدراسة

المستوي	الدرجة
منخفض جدا	1.79-1
منخفض	2.59-1.8
متوسط	3.39-2.60
مرتفع	4.19-3.40
مرتفع جدا	5.00 – 4.20

صدق أداة الدراسة

تم حساب صدق عبارات استمارة الاستبيان من خلال القيام بحساب قيمة معامل الارتباط بيرسون بين درجة كل عبارة والدرجة الكلية للمحور التي تنتمي إليه العبارة وذلك لتحديد مستوي الاتساق الداخلي لأداة الدراسة وتبين أن جميع معاملات الارتباط لجميع عبارات استمارة الاستبيان كانت ذات دلالة إحصائية عند مستويات معنوية (0.01) وهذا يعني أن الأداة تتمتع بمستوي صدق مرتفع وهي صالحة لأغراض الدراسة.

ثبات أداة الدراسة

تم حساب معامل ألفا كرونباخ لعبارات محاور الاستبيان وكانت النتائج كما يلي:

جدول (2) معامل الثبات لمحاور استمارة الاستبيان

المحاور	معامل الفا كورنباخ	عدد العبارات
دور المكتب الإعلامي الخاص بوزارة الداخلية العراقية	0.856	10
الوعي بالأمن السيبراني	0.848	10
إجمالي استمارة الاستبيان	0.879	20

يتبين أن قيمة معامل الثبات Alphaوهي أكبر من 0.7 لجميع محاور استمارة الاستبيان مما يؤكد على صلاحية وارتباط عبارات محاور استمارة الاستبيان وارتفاع مستوي ثبات أداة الدراسة مما يسمح باستخدام الأداة لغرض الدراسة.

خصائص عينة الدراسة

جدول (3) توزيع عينة الدراسة وفقا للخصائص للشخصية

الخصائص	الفئات	العدد	النسبة %
الجنس	ذكر	328	85.4
	أنثي	56	14.6
العمر	أقل من 19 سنه	232	60.4
	من 19 سنة إلى 21 سنة	104	27.1
	22 سنة فأكثر	48	12.5
المستوى الدراسي	الفرقة الاولى	44	22.9
	الفرقة الثانية	72	37.5
	الفرقة الثالثة	32	16.7
	الفرقة الرابعة	44	22.9

تحليل (محاور الدراسة):

المحور الأول: دور المكتب الإعلامي الخاص بوزارة الداخلية العراقية

1- استراتيجيات المكتب الإعلامي

جدول (4) الوسط الحسابي والانحراف المعياري والترتيب ومستوي الموافقة على عبارات استراتيجيات المكتب الإعلامي

العـــــبارة	المتوسط الحسابي	الانحراف المعياري	الترتيب	مستوي الموافقة
يعمل المكتب الإعلامي على زيادة وعي أفراد المجتمع بأهمية الأمن السيبراني	4.188	0.930	1	مرتفع
يقوم المكتب الإعلامي بتنظيم حملات توعية للمواطنين لتعريفهم مخاطر (تكنولوجيا المعلومات الحديثة)	4.063	0.803	5	مرتفع
يعمل المكتب الإعلامي بالعمل على زيادة وعي الأفراد بعدم الإفصاح عن أي بيانات شخصية لهم عبر المواقع التي يتعاملون معها	4.125	0.859	3	مرتفع
يهتم المكتب الإعلامي بتوعية الأفراد بأهمية استخدام كلمات سرية صعبة ومعقدة لتوفير الحماية الكافية	4.167	0.689	2	مرتفع
يهتم المكتب الإعلامي بتوعية الأفراد بعدم التعامل مع الرسائل الالكترونية مجهولة المصدر	4.063	0.721	4	مرتفع
المتوسط	4.121	0.800	مرتفع	

تم ترتيب عبارات استراتيجيات المكتب الإعلامي من قيمة الوسط الحسابي من وجهة نظر عينة الدراسة تبين أن عبارة (يعمل المكتب الإعلامي على زيادة وعي أفراد المجتمع بأهمية الأمن السيبراني) هي أكثر العبارات أهمية بقيمة 4.188 وانحراف معياري 0.930 وبدرجة موافقة مرتفعة بينما كانت العبارة (يقوم المكتب الإعلامي بتنظيم حملات توعية للمواطنين لتعريفهم مخاطر تكنولوجيا المعلومات الحديثة) هي أقل العبارات أهمية بقيمة 4.063 وانحراف معياري 0.803 وبدرجة موافقة مرتفعة وعند دراسة عبارات استراتيجيات المكتب الإعلامي تبين أن جميع العبارات في مستوي الموافقة المرتفع مما يوضح ارتفاع مستوى الاستراتيجيات التي يقوم المكتب الإعلامي الخاص بوزارة الداخلية العراقية بتطبيقها حيث بلغت قيمة الوسط الحسابي 4.121 بانحراف معياري 0.800

2-المنشورات الصادرة من المكتب الإعلامي

جدول (5) الوسط الحسابي والانحراف المعياري والترتيب ومستوي الموافقة على عبارات المنشورات الصادرة من المكتب الإعلامي

العـــــبارة	المتوسط الحسابي	الانحراف المعياري	الترتيب	مستوي الموافقة
المنشورات الصادرة من المكتب الإعلامي تهتم بتعريف الأفراد أحدث المعلومات المتعلقة بكيفية حماية اجهزتهم والتعامل مع التكنولوجيا الحديثة	4.021	0.779	4	مرتفع
المنشورات الصادرة من المكتب الإعلامي تقوم بتوضيح كيفية استخدام أنظمة حماية متقدمة لمواجهة الجرائم الالكترونية	4.104	0.772	3	مرتفع
المنشورات الصادرة من المكتب الإعلامي توضح الدورات والبرامج التدريبية التي يمكن للأفراد الحصول عليها في كيفية التعامل مع مخاطر تكنولوجيا المعلومات الحديثة	3.896	0.921	5	مرتفع
المنشورات الصادرة من المكتب الإعلامي توضح الطرق المستخدمة للحصول على بيانات الكروت الائتمانية للعملاء والمواطنين	4.271	0.639	1	مرتفع جدا
المنشورات الصادرة من المكتب الإعلامي توضح كل المعلومات اللازمة عن قرصنة التطبيقات السحابية	4.250	0.597	2	مرتفع جدا
المتوسط	4.108	0.742	مرتفع	

تم ترتيب عبارات المنشورات الصادرة من المكتب الإعلامي من قيمة الوسط الحسابي من وجهة نظر عينة الدراسة تبين أن عبارة (المنشورات الصادرة من المكتب الإعلامي توضح الطرق المستخدمة للحصول على بيانات الكروت الائتمانية للعملاء والمواطنين) هي أكثر العبارات أهمية بقيمة 4.271 وانحراف معياري 0.639 وبدرجة موافقة مرتفعة جدا بينما كانت العبارة (المنشورات الصادرة من المكتب الإعلامي توضح الدورات والبرامج التدريبية التي يمكن للأفراد الحصول عليها في كيفية التعامل مع مخاطر تكنولوجيا المعلومات الحديثة) هي أقل العبارات أهمية بقيمة 3.896 وانحراف معياري 0.921 وبدرجة موافقة مرتفعة وعند دراسة عبارات المنشورات الصادرة من المكتب الإعلامي تبين أن عبارتين في مستوى الموافقة المرتفع جدا وثلاث عبارات في مستوي الموافقة المرتفع مما يوضح ارتفاع مستوى

المنشورات الصادرة من المكتب الإعلامي الخاص بوزارة الداخلية العراقية حيث بلغت قيمة الوسط الحسابي 4.108 بانحراف معياري 0.742

مما سبق يتبين ارتفاع مستوى دور المكتب الإعلامي الخاص بوزارة الداخلية العراقية حيث بلغت قيمة الوسط الحسابي 4.115 بانحراف معياري 0.771

المحور الثاني: الوعي بالأمن السيبراني

جدول (6) الوسط الحسابي والانحراف المعياري والترتيب ومستوى الموافقة على عبارات الوعي بالأمن السيبراني

العبـــارة	المتوسط الحسابي	الانحراف المعياري	الترتيب	مستوى الموافقة
يقوم الأفراد بحماية أنفسهم وأجهزتهم من خلال عدم استخدام أي رابط او رسالة مجهولة	4.271	0.701	8	مرتفع جدا
يقوم الأفراد بالاطلاع على أحدث المعلومات المتعلقة بكيفية حماية اجهزتهم والتعامل مع التكنولوجيا الحديثة	4.313	0.714	6	مرتفع جدا
يقوم الأفراد باستخدام أنظمة حماية متقدمة لمواجهة الجرائم الالكترونية	4.229	0.772	9	مرتفع جدا
يهتم الأفراد بالحصول على الدورات والبرامج التدريبية في كيفية التعامل مع مخاطر تكنولوجيا المعلومات الحديثة	4.375	0.565	3	مرتفع جدا
يهتم الأفراد بالتحديث المستمر والدوري لكلمات السر والشفرات المستخدمة في التعاملات التكنولوجية	4.333	0.719	4	مرتفع جدا
يقوم الأفراد باستخدام الأجهزة المتطورة التي توفر الحماية الكافية وتقلل من احتمالية التعرض للمخاطر	4.417	0.642	2	مرتفع جدا
الأفراد لديهم وعي بوجود برامج التحسس للحصول على بياناتهم وحساباتهم البنكية	4.188	0.756	10	مرتفع
يهتم الأفراد باستخدام كلمات سرية صعبة ومعقدة لتوفير الحماية الكافية	4.292	0.646	7	مرتفع جدا
يهتم الأفراد بعدم التعامل مع الرسائل الالكترونية مجهولة المصدر	4.417	0.608	1	مرتفع جدا
يقوم الأفراد بعدم الإفصاح عن أي بيانات شخصية لهم عبر المواقع التي يتعاملون معها	4.313	0.619	5	مرتفع جدا

تم ترتيب عبارات الوعي بالأمن السيبراني من حيث درجة الأهمية النسبية (قيمة الوسط الحسابي الأكبر) من وجهة نظر عينة الدراسة تبين أن عبارة (يهتم الأفراد بعدم التعامل مع الرسائل الالكترونية مجهولة المصدر) هي أكثر العبارات أهمية بقيمة 4.417 وانحراف

معياري 0.608 وبدرجة موافقة مرتفعة جدا بينما كانت العبارة (الأفراد لديهم وعي بوجود برامج التحسس للحصول على بيانتهم وحساباتهم البنكية) هي أقل العبارات أهمية بقيمة 4.188 وانحراف معياري 0.756 وبدرجة موافقة مرتفعة وعند دراسة عبارات محور الوعي بالأمن السيبراني تبين أن تسع عبارات في مستوى الموافقة المرتفع جدا وعبارة واحدة في مستوي الموافقة المرتفع مما يوضح وجود مستوى مرتفع جدا للوعي بالأمن السيبراني لدى طلاب الكليات العلمية والإنسانية بالعراق حيث بلغت قيمة المتوسط الحسابي4.315 بانحراف معياري 0.674

اختبار فروض الدراسة

جدول (7) العلاقات الإرتباطية بين دور المكتب الإعلامي الخاص بوزارة الداخلية العراقية والوعي بالأمن السيبراني

المتغيرات	الوعي بالأمن السيبراني	
دور المكتب الإعلامي الخاص بوزارة الداخلية العراقية	قيمة معامل الارتباط بيرسون	0.914
	الدلالة الإحصائية	0.000
استراتيجيات المكتب الإعلامي	قيمة معامل الارتباط بيرسون	0.897
	الدلالة الإحصائية	0.000
المنشورات الصادرة من المكتب الإعلامي	قيمة معامل الارتباط بيرسون	0.779
	الدلالة الإحصائية	0.000

تبين علاقة لها دلالة إحصائية بين دور المكتب الإعلامي الخاص بوزارة الداخلية العراقية والوعي بالأمن السيبراني وبلغت قيمة معامل الارتباط 0.914 وهو ما يبين صحة الفرضية الرئيسية للدراسة وكذلك علاقة لها دلالة إحصائية بين لاستراتيجيات التي يقوم المكتب الإعلامي الخاص بوزارة الداخلية العراقية بتطبيقها والوعي بالأمن السيبراني وبلغت قيمة معامل الارتباط 0.897 وهو ما يبين صحة الفرضية الفرعية الأولي للدراسة وأيضا علاقة لها دلالة إحصائية بين المنشورات الصادرة من المكتب الإعلامي الخاص بوزارة الداخلية العراقية والوعي بالأمن السيبراني وبلغت قيمة معامل الارتباط 0.779 وهو ما يبين صحة الفرضية الفرعية الثانية للدراسة.

استنتاجات الدراسة

- ✓ مما سبق يتبين ارتفاع مستوى دور المكتب الإعلامي الخاص بوزارة الداخلية العراقية حيث بلغت قيمة الوسط الحسابي 4.115 بانحراف معياري 0.771 وكذلك ارتفاع مستوى الاستراتيجيات التي يقوم المكتب الإعلامي الخاص بوزارة الداخلية العراقية بتطبيقها وارتفاع مستوى المنشورات الصادرة من المكتب الإعلامي الخاص بوزارة الداخلية العراقية
- ✓ وجود مستوى مرتفع جدا للوعي بالأمن السيبراني لدى طلاب الكليات العلمية والإنسانية بالعراق حيث بلغت قيمة الوسط الحسابي 4.315 بانحراف معياري 0.674
- ✓ تبين علاقة لها دلالة إحصائية بين دور المكتب الإعلامي الخاص بوزارة الداخلية العراقية والوعي بالأمن السيبراني وهو ما يبين صحة الفرضية الرئيسية للدراسة وكذلك علاقة لها دلالة إحصائيةبين لاستراتيجيات التي يقوم المكتب الإعلامي الخاص بوزارة الداخلية العراقية بتطبيقها والوعي بالأمن السيبراني وهو ما يبين صحة الفرضية الفرعية الاولي للدراسة وأيضا علاقة لها دلالة إحصائية بين المنشورات الصادرة من المكتب الإعلامي الخاص بوزارة الداخلية العراقية والوعي بالأمن السيبراني وهو ما يبين صحة الفرضية الفرعية الثانية للدراسة

الخاتمة:

الاستنتاجات:

تمحورت هذه الدراسة حول دور المكتب الإعلامي الخاص بوزارة الداخلية العراقية في نشر الوعي بالأمن السيبراني بين المواطنين العراقيين، وقد تمت الإجابة على السؤال البحثي الرئيسي والأسئلة الفرعية من خلال تحليل المضمون الإعلامي على الموقع الرسمي لوزارة الداخلية العراقية، وقد توصلت الدراسة إلى ما يلي:

1.**دور المكتب الإعلامي:**يلعب المكتب الإعلامي الخاص بوزارة الداخلية العراقية دوراً بارزاً في نشر الوعي بالأمن السيبراني، معتمداً بشكل كبير على مصادر رسمية وموثوقة.

2.**فعالية الاستراتيجيات:**استراتيجيات المكتب الإعلامي فعّالة جداً في تنمية الوعي بالأمن السيبراني بين المواطنين.

3. **تفاعل المواطنين مع المنشورات:**يوجد تفاعل كبير من قبل المواطنين مع المنشورات الخاصة بالأمن السيبراني والصادرة من المكتب الإعلامي.

4. **تحليل المضمون الإعلامي:**تحليل المضمون الإعلامي على الموقع الرسمي أظهر أن المكتب يعتمد بشكل رئيسي على الشخصيات الرسمية (مثل مكتب وزير الداخلية) وأن هذه الشخصيات كانت الأكثر حضوراً في المحتوى.

نوعية الاستمالة المستخدمة في المنشورات كانت ذهنية وعقلية، موثقة بالبراهين.

الصور التفاعلية اللحظية كانت الأكثر استخداماً، مما يدل على توثيق الأحداث لحظة بلحظة.

4. **العلاقات الإحصائية :**علاقة لها دلالة إحصائية بين دور المكتب الإعلامي والوعي بالأمن السيبراني، مما يؤكد صحة الفرضية الرئيسية للدراسة ، أثبتت الدراسة علاقة لها دلالة إحصائية بين استراتيجيات المكتب الإعلامي والوعي بالأمن السيبراني، مما يؤكد صحة الفرضية الفرعية الأول، وقد تم إثبات صحة الفرضية الثانية وهي علاقة لها دلالة إحصائية بين مضمون المنشورات الصادرة من المكتب الإعلامي والوعي بالأمن السيبراني.

التوصيات:

توصي الدراسة بالعمل على ما يلي:

1. تعزيز الاستراتيجيات الحالية للمكتب الإعلامي الخاص بوزارة الداخلية العراقية لزيادة فعالية نشر الوعي بالأمن السيبراني بين المواطنين.
2. توسيع نطاق الحملات الإعلامية لتشمل مختلف وسائل الإعلام ومنصات التواصل الاجتماعي لضمان وصول الرسائل إلى شريحة أكبر من المجتمع.
3. زيادة توثيق الأحداث والأنشطة المتعلقة بالأمن السيبراني باستخدام والفيديوهات التفاعلية لتعزيز مصداقية المنشورات وجذب انتباه المواطنين.
4. تقديم برامج تدريبية وتوعوية للمواطنين حول أفضل الممارسات في مجال الأمن السيبراني والتحديث المستمر في هذا المجال.
5. إجراء دراسات دورية لقياس تأثير الحملات الإعلامية واستراتيجيات التوعية، والعمل على تحسينها بناءً على النتائج والتغذية الراجعة من المواطنين.

المراجع العربية

1. الاستراتيجية الوطنية للأمن السيبراني. (2021). وزارة الاتصالات وتكنولوجيا المعلومات، الأردن.
2. أسماء، عاصم. (2020). الإعلام الجديد: الإشكاليات وأنماط التغير. المركز العربي للبحوث والدراسات.
3. إسماعيل، زيد محمد علي، & الشمري، صاح مهدي هادي. (2020). الأمن السيبراني كمرتكز جديد في الاستراتيجية العراقية. مجلة قضايا سياسية، 12(62)، 277–300.
4. الأمن السيبراني. (2021). هيئة الإعلام، قسم الدراسات والاتصال والعلاقات العامة، الكويت.
5. جابوربي، إسماعيل. (2020). دور الأمن السيبراني في مواجهة التهديدات الإلكترونية: دراسة حالة الجزائر. مجلة تحولات، 3، 487–505.
6. الجلفاوي، خالد مخلف. (2021). التحول الرقمي للمؤسسات الوطنية وتحديات الأمن السيبراني من وجهة نظر ضباط الشرطة الأكاديميين بالكويت. المجلة العربية للآداب والدراسات الإنسانية، 5(19)، 77–105.
7. الجلفاوي، خالد مخلف. (2021). التحول الرقمي للمؤسسات الوطنية وتحديات الأمن السيبراني من وجهة نظر ضباط الشرطة الأكاديميين بالكويت. المجلة العربية للآداب والدراسات الإنسانية، 5(19).
8. خليل، هشام محمد. (2012). الجوانب الإجرامية للجوانب المعلوماتية. مجلة الأمن والقانون، شرطة دبي، (2)، 38–55.
9. الداعمي، غالب كاظم. (2019). صناعة الرأي العام من عصر الطباعة إلى فضاء الإنترنت: تقاليد موروثة وسلطة مطلقة. دار أمجد للنشر والتوزيع.
10. الراجحي، محمد. (2018). صناعة الأخبار الكاذبة ولولب الحصار المعلوماتي للرأي العام. مركز الجزيرة للدراسات. http://studies.aljazeera.net
11. سفاح، كريم أنصر. (2023). الحروب الإلكترونية وأثرها على الأمن القومي. مركز النهرين للدراسات الاستراتيجية. https://www.alnahrain.iq/post/1031

12. سلام، لامية، & وكهينة، طالة. (2020). الجريمة الإلكترونية بعد جديد لمفهوم الإجرام عبر منصات التواصل الاجتماعي. مجلة الرواق للدراسات الاجتماعية والإنسانية، 6(2)، 485–505.

13. السيد، نهى مجدي محمد. (2021). الأمن السيبراني وعلاقته بالمضمون الإعلامي في ظل رؤية مصر 2030. المجلة العلمية لبحوث الإعلام والاتصال، 35، 86–110.

14. السيد، نهى مجدي محمد. (2021). الأمن السيبراني وعلاقته بالمضمون الإعلامي في ظل رؤية مصر 2030. المجلة العربية لبحوث الإعلام والاتصال، 25، 484–510.

15. الصفاء، تغريد، & مهدي، لبنى خميس. (2020). أثر السيبرانية في تطوير القوة. مجلة حمورابي للدراسات، 33–34، 149–170.

16. الطيار، حسين بن سليمان بن راشد. (2020). الأمن السيبراني في منظور مقاصد الشارع: دراسة تأصيلية. مجلة جامعة الطائف للعلوم الإنسانية، 6(21)، 264–290.

17. العنزي، زينب طرفي. (2022). الجريمة الإلكترونية في ميزان الفقه والقانون العراقي. مجلة الدراسات الإسلامية والبحوث الأكاديمية، 99، 112–130.

18. العنزي، ماجد بن خلاف حمود. (2021). الإرهاب السيبراني وانعكاساته على الأمن الوطني. جامعة نايف العربية للعلوم الأمنية. https://www.repository.nauss.edu.sa

19. غازي، خالد محمد. (2022). صناعة الكذب: كيف نفهم الإعلام البديل. وكالة الصحافة العربية.

20. الفرحان، علاء الدين. (2021). من الردعة إلى الردع السيبراني: دراسة لمدى تحقيق مبدأ الردع في القضاء السيبراني. مجلة الفكر، 16(1)، 2246–2265.

21. القحطاني، عواطف بنت يحيى. (2019). متطلبات تعزيز الأمن الفكري لدى الطالبة الجامعية من منظور طريقة العمل مع الجماعات. المجلة العربية للدراسات الأمنية، 35(2)، 496–520.

22. كريم، أنصر سفاح. (2023). الحروب الإلكترونية وأثرها على الأمن القومي. مركز النهرين للدراسات الاستراتيجية. https://www.alnahrain.iq/post/1031

23. وزارة الداخلية العراقية. (د.ت). المنصة الإلكترونية للإبلاغ عن المحتوى المخالف. https://moi.gov.iq/?page=4611

24. وزارة الداخلية العراقية. (د.ت). الموقع الرسمي لوزارة الداخلية العراقية. https://www.moi.gov.iq/?topic

المراجع الإنجليزية

1. Center for Internet Security. (2021). Software updates. https://www.cisecurity.org
2. Cisco. (2020). Firewalls and intrusion detection systems. https://www.cisco.com
3. Evelyne, J. (2020). Regulating cybersecurity: What civil liability in case of cyber-attacks.
4. Gartner. (2020). Cyber risk assessment. https://www.gartner.com
5. Kshetri, N. (2013). Cybercrime and cybersecurity in the global South. Palgrave Macmillan. https://doi.org/10.1057/9781137021946
6. Lewis, J. (2018). Economic impact of cybercrime: No slowing down. Center for Strategic and International Studies.
7. McMillan, R. (2010, September 21). Was Stuxnet built to attack Iran's nuclear program? PCWorld.
8. National Institute of Standards and Technology. (2018). Glossary of key information security terms. http://csrc.nist.gov/publications
9. National Institute of Standards and Technology. (2021). Data encryption. https://www.nist.gov
10. Raicu, G., & Raicu, A. (2022). Cybersecurity strategies in Industry 4.0. International Journal of Modern Manufacturing Technologies, 14(3). https://doi.org/10.54684/ijmmt.2022.14.3.233
11. Ramirez, M., Ariza, L., & Miranda, M. (2022). The disclosure of information on cybersecurity in listed companies in Latin America: Proposal for a cybersecurity discourse index. Sustainability, 14(3).
12. SANS Institute. (2021). Cybersecurity training. https://www.sans.org/cyberaces
13. Reuters. (2010, September 24). Factbox: What is Stuxnet? https://www.reuters.com