العدد 51 - أكتوبر / ديسمبر 2025

كليّة الإعلام
المجلة العربيّة لبحوث الإعلام والاتصال

العدد 51 - أكتوبر / ديسمبر 2025

أطر معالجة قضايا الأمن السيبراني في الصحافة الرقمية وأثرها على إدراك النخب الإعلامية للتهديدات الرقمية: دراسة تطبيقية

د. هاني نادي عبد المقصود

أستاذ الصحافة المساعد بقسم الإعلام التربوي بكلية التربية النوعية - جامعة المنيا

الملخص:

هدف البحث إلى دراسة أطر معالجة قضايا الأمن السيبراني في الصحف الرقمية وعلاقتها بإدراك النخب الإعلامية للتهديدات الرقمية، بالاستناد إلى نظرية الأطر الإعلامية ونظرية الاتصال بالمخاطر لفهم كيفية بناء الرسائل الإعلامية الخاصة بالأمن السيبراني ودورها في تشكيل الوعي بالتهديدات الرقمية، استخدم البحث منهج المسح بشقيه التحليلي والميداني، من خلال تحليل محتوى بوابة الأهرام وموقع اليوم السابع، وتطبيق استبيان على عينة مكونة من 422 مفردة من النخب الأكاديمية والمهنية في المجال الإعلامي، وأظهرت النتائج أن إطار التهديد والخطر كان الأكثر شيوعاً بنسبة 26.07% ، تلاه إطار الحلول والوقاية بنسبة 20.14% ، ثم إطار المسؤولية بنسبة 17.77% ، في حين تراجعت الأطر ذات الطابع الإنساني والأخلاقي والاقتصادي، كما تبين ارتفاع مستوى إدراك النخب الإعلامية لأبعاد التهديدات الرقمية، خصوصاً في مجالات الأمن السيبراني والخصوصية والتأثيرات النفسية والاجتماعية، مما يعكس وعياً حقيقياً بخطورة الظواهر الرقمية المعاصرة، مع وجود علاقة ارتباط موجبة قوية ودالة إحصائياً بين درجة تبني النخب الإعلامية لأطر معالجة قضايا الأمن السيبراني وإدراكهم للتهديدات الرقمية.

الكلمات المفتاحية: الأطر، الصحف الرقمية، الأمن السيبراني، النخبة، التهديدات الرقمية.

المقدمة:

تعتبر القضايا المتعلقة بالأمن السيبراني من بين القضايا العالمية المعاصرة، التي تجذب انتباه الجمهور العام وتركيز الحكومات، فضلاً عن المؤسسات العلمية والتكنولوجية على حد سواء، ونظرًا لسرعة التحول الرقمي وزيادة الاعتماد على الإنترنت والذكاء الاصطناعي، لم يعد أمن الفضاء السيبراني مجرد قضية تقنية بل أصبح قضية اجتماعية واقتصادية وسياسية، ولذلك فإن للصحافة الرقمية وخاصة في مجال العلوم والتكنولوجيا دوراً محورياً في تبسيط القضايا العلمية مثل قضايا الأمن السيبراني وتقديمها للجمهور بطريقة وأسلوب يسهلان فهمها على المستويين الموضوعي والتوعوي، كما أن تأطير هذه القضايا لا يتم بأي حال في فراغ اجتماعي بل يتم تأطيره ضمن معايير صحفية معينة تحدد نطاق عرض القضية وتوزيعها، فضلاً عن جوانب التي يتم إبرازها وأخرى يتم تهميشها أو تقليل أهميتها.

وتشير الدراسات السابقة إلى أن الإعلام لا ينقل الأحداث كما هي، بل يعيد صياغتها وفق إطار يعبر عن السياسة الإعلامية للوسيلة أو السياق السياسي والاجتماعي التي تتم فيه هذه الأحداث بما يؤثر في اتجاهات الجمهور، وفي نفس السياق توصلت دراسة بعنوان التهديد السيبراني والإرهاب الإلكتروني في الصحف الأمريكية إلى أن التغطية الإعلامية تسلط الضوء على إطار التهديد والخوف، مما زاد من مشاعر القلق للقراء وربطهم بين التكنولوجيا والتهديدات الأمنية (Bastug et al., 2023)، مما يدل على أن فريق الصحافة لا يكتفي فقط بإشعار الجمهور بالمواضيع الخطيرة بل يشكل وعي جماعي حول الخطورة.

كما أن التغطية الإعلامية للأمن السيبراني قد تتأثر بالانتماءات السياسية والإيديولوجية للمؤسسات الإعلامية، ففي دراسة تحليلية للتغطية الإعلامية لتسريبات الوثائق السرية، تبين أن وسائل الإعلام ذات التوجهات السياسية المختلفة قدّمت نفس الحدث بطرق متباينة، حيث اعتمدت بعض الوسائل إطار الدفاع عن الحريات الفردية، بينما تبنّت أخرى إطار التهديد للأمن القومي، وهو ما أدى إلى تباين في إدراك الجمهور للقضية (Silva et al., 2022). هذا يؤكد أن الأطر الإعلامية لا تنعكس فقط على مستوى الوعي الفردي، بل قد تمتد لتؤثر في المواقف السياسية وصناعة القرار.

كما يطرح الباحثين نماذج تفسيرية لفهم العلاقة بين الأطر الإعلامية المستخدمة للتغطية والإدراك، مثل النموذج التأثيري والذي يرى أن الرسائل الإعلامية يمكن أن تُسهم في إعادة تشكيل الوعي العام وتحفيز الأفراد على تبني سلوكيات أكثر أمانًا، مثل تحديث أنظمة الحماية أو استخدام كلمات مرور قوية (Romero-Masters, 2021). ويشير هذا النموذج إلى كيفية تحول لخطاب الإعلامي من مجرد وسيلة لنقل المعلومات إلى أداة للتغيير في الاتجاهات والسلوكيات.

وبالرغم من أهمية استخدام الأطر في التغطية فإن بعض الدراسات حذرت من الإفراط في استخدام إطار التهديد لما له من أثر سلبي محتمل، حيث يعتاد الأفراد على الخطاب المليء بالتهديدات فيتراجع تأثيره بمرور الوقت، ومن هنا تبرز الحاجة إلى الموازنة بين إبراز المخاطر وتقديم الحلول، بما يتيح للمتلقي إدراك حجم التحدي دون أن يشعر بالعجز أو الاستسلام.

وفي هذا الإطار يكتسب موضوع البحث أهمية خاصة لكونه يبحث ثلاثة محاور أساسية: هي الأمن السيبراني كقضية تهدد البنية التحتية الرقمية للدول والأفراد، والصحافة الرقمية كوسيط معرفي مسؤول عن تبسيط القضايا للجمهور، وأطر المعالجة الصحفية كأداة تأثير تسهم في تشكيل الإدراك وتوجيهه نحو الخوف والتهديدات الرقمية أو نشر الطمأنينة أو حتى التعبئة مع أو ضد القضايا المقدمة.

وبناءً على العرض السابق فإن البحث الحالي يهدف إلى تحليل الأطر التي تستخدمها الصحافة الرقمية في تناول قضايا الأمن السيبراني، والكشف عن أثر هذه الأطر على إدراك الجمهور لمستوى التهديدات الرقمية.

الإطار المعرفي:

الصحافة الرقمية:

يقصد بالصحافة الرقمية «Digital Journalism» ممارسة العمل الصحفي عبر المنصات الإلكترونية المختلفة كالمواقع الإخبارية والتطبيقات وشبكات التواصل الاجتماعي، بالاعتماد على الوسائط المتعددة وسرعة التحديث والتفاعل مع الجمهور، مما يمنحها تأثيرًا أعمق مقارنة بالوسائط التقليدية (Negreira-Rey et al., 2023)، ويعكس التحول الرقمي في غرف الأخبار تكيف المؤسسات الإعلامية مع التطورات التقنية كالذكاء الاصطناعي والتحليل الآلي للمحتوى، مما أعاد تشكيل أدوار الصحفيين وعلاقاتهم بالتكنولوجيا والجمهور(Media, 2024)، وتتعدد أبعاد التحول الرقمي في الصحافة ويمكن عرضها كالآتي:

- البعد التقني: ويهتم بتوظيف الذكاء الاصطناعي وتحليل البيانات وتطوير أساليب عرض مبتكرة.
- البعد المهاري: ويهتم بتمكين الصحفيين من مهارات رقمية متعددة الوسائط.
- البعد الأخلاقي: ويشمل مواجهة تحديات المصداقية والخصوصية ومكافحة التضليل (Bojic et al., 2024).
- البعد الاجتماعي: ويتضمن تعزيز مشاركة الجمهور في إنتاج وتقييم الأخبار.
- البعد القانوني والتنظيمي: ويشمل حماية الملكية الفكرية وضمان حرية النشر في الفضاء الرقمي.

وتسهم الصحافة الرقمية في رفع وعي الجمهور بالقضايا العامة، بفضل سرعتها وتفاعليتها وسهولة الوصول إليها، وهو ما جعلها أصبحت مصدرًا رئيسًا للمعلومات لدى فئات واسعة من المجتمع، ومن أبرز القضايا التي تتناولها في هذا الإطار قضايا الأمن السيبراني، حيث أصبحت الهجمات الإلكترونية وسرقة البيانات من أخطر التهديدات للأفراد والمؤسسات، مما يجعل دور الصحافة محوريًا في نشر الوعي والتثقيف السيبراني (Bojic et al., 2024).

كما تعمل الصحافة الرقمية على تبسيط المفاهيم التقنية، والتحذير من التهديدات الرقمية، وكشف الانتهاكات المتعلقة بخصوصية المستخدمين وتسريب بياناتهم، بما يعزز الشفافية والمساءلة، كما تُسهم في بناء الثقة بين المواطنين والمؤسسات عبر تسليط الضوء على جهود حماية البنية التحتية الرقمية وتعزيز مفهوم المواطنة الرقمية الواعية (Westlund et al., 2025).

الأمن السيبراني والتهديدات الرقمية:

يُقصد بالأمن السيبراني «Cyber Security» منظومة متكاملة من الإجراءات والسياسات التي تهدف إلى حماية الأنظمة والشبكات والبيانات من الاستخدام غير المشروع أو الاختراق، بينما تشير التهديدات الرقمية «Digital Threats» إلى الأنشطة الضارة التي تستهدف هذه الأنظمة بهدف السرقة أو التعطيل أو الإضرار بالبنية التحتية الرقمية (Dave et al., 2023)، وفي هذا الإطار أصبحت قضايا الأمن السيبراني والتهديدات الرقمية في ظل التحول الرقمي المتسارع من أبرز القضايا المعاصرة التي تمس الأفراد والمؤسسات والدول، إذ بات الاعتماد على الأنظمة الذكية والإنترنت جزءًا أساسيًا من الحياة اليومية، مما جعل حماية الفضاء الرقمي أولوية وطنية ومجتمعية (Preprints.org, 2024؛ Bojic et al., 2024)، ويمكن مناقشة قضايا الأمن السيبراني من ثلاثة أبعاد رئيسة:

- البعد التقني: ويتعلق بحماية الأنظمة باستخدام التشفير وجدران الحماية وأنظمة الكشف المبكر عن الاختراقات (Westlund et al., 2025).

- البعد التنظيمي والإداري: ويشمل وضع السياسات والتشريعات الوطنية التي تنظم أمن المعلومات، وتحدّد مسؤوليات الجهات المختلفة في حماية البنية التحتية الرقمية.

- البعد التوعوي والمجتمعي: وهو الأهم في نجاح منظومة الأمن السيبراني، إذ يعتمد على وعي الأفراد والمستخدمين بمخاطر الفضاء الإلكتروني وكيفية التعامل الآمن معه (Preprints.org, 2024).

أما التهديدات الرقمية فتتنوع تبعًا لطبيعتها وأهدافها، وتشمل:

- البرمجيات الخبيثة Malware وبرامج الفدية Ransomware التي تُشفّر بيانات المستخدمين وتطلب فدية مالية مقابل استعادتها (Falade, 2023).

- الهندسة الاجتماعية والتصيّد الإلكتروني Social Engineering, Phishing التي تستغل الثقة أو الجهل الأمني لدى المستخدمين للحصول على بياناتهم (Falade, 2023).

- التهديدات المدعومة بالذكاء الاصطناعي (AI-Powered Threats) والتي تستغل تقنيات التزييف العميق (Deepfakes) في التضليل أو الابتزاز الرقمي (Falade, 2023).

- الهجمات على البنية التحتية الحيوية مثل أنظمة الطاقة والمياه والمواصلات، والتي تمثل تهديدًا مباشرًا للأمن الوطني والاقتصادي (Dave et al., 2023؛Schmitt, 2023).

أهمية مواجهة التهديدات الرقمية:

تُعد مواجهة التهديدات الرقمية ضرورة إستراتيجية لضمان استقرار البيئة الرقمية وحماية مصالح الأفراد والدول، فنجاح أي جهود توعوية يعتمد على مدى قدرتها على الوقاية من الهجمات والتعامل الفعّال مع الحوادث الأمنية، وتبرز أهمية المواجهة في عدة جوانب رئيسة:

- حماية الخصوصية والبيانات الشخصية: حيث يؤدي تسريب البيانات إلى أضرار بالغة تمس الأفراد والمؤسسات على حد سواء.

- ضمان استمرارية الخدمات الحيوية: مثل الصحة والطاقة والنقل، التي قد تتعطل تمامًا جراء الهجمات الإلكترونية (Schmitt, 2023).

- تعزيز الثقة في البيئة الرقمية: فكلما ارتفع مستوى الأمان، زادت ثقة المستخدمين في التعامل عبر المنصات الرقمية، مما يدعم التحول الرقمي المستدام.

- حماية الأمن الوطني: إذ قد تستهدف الهجمات الإلكترونية أنظمة حكومية حساسة، مما يجعل الأمن السيبراني جزءًا لا يتجزأ من الأمن القومي للدول (Dave et al., 2023).

- رفع الوعي الرقمي لدى الجمهور: حيث تمثل التوعية حجر الأساس في مواجهة التهديدات الرقمية، فمعظم الهجمات الإلكترونية تبدأ من سلوكيات المستخدمين غير الآمنة مثل الضغط على الروابط المشبوهة أو مشاركة البيانات الشخصية دون تحقق (Falade, 2023)، لذلك يعد الاستثمار في التعليم الرقمي والتثقيف السيبراني خطوة أساسية لبناء مجتمع قادر على حماية نفسه من الاستغلال الإلكتروني.

- حماية الجمهور من المخاطر الإلكترونية: حيث أصبحت الحماية من التهديدات الرقمية مثل التنمر الإلكتروني والاستدراج والمحتوى الضار من أولويات الأمن السيبراني المجتمعي مع تزايد استخدام جميع الفئات العمرية للإنترنت (Dave et al., 2023)، فالمواجهة الفعالة لهذه التهديدات تتطلب تعاونًا بين الأسرة والمدرسة ووسائل الإعلام الرقمية لضمان بيئة إنترنت آمنة ومتوازنة.

- تعزيز الثقة في الإعلام الرقمي والمصادر الموثوقة: حيث أصبح الأمن الرقمي أداةً لحماية المحتوى الصحفي الموثوق، فالجمهور يحتاج إلى ضمان أن الأخبار التي يتلقاها عبر المنصات الرقمية لم يتم التلاعب بها أو تزويرها تقنيًا (Falade, 2023)، وهي التي تُستخدم لتضليل الرأي العام.

- تعزيز المشاركة المجتمعية في الأمن السيبراني: حيث لم تعد حماية الفضاء الرقمي مسؤولية الحكومات فقط، بل أصبحت قضية مجتمعية تشاركية، فمشاركة المواطنين في الإبلاغ عن التهديدات، وتبنّي سلوكيات رقمية مسؤولة، تخلق جدارًا من الوعي الجماعي يقلل من فرص الهجمات الإلكترونية (Dave et al., 2023).

ويؤكد الخبراء أن بناء منظومة قوية لمواجهة التهديدات الرقمية يتطلب تضافر الجهود التقنية والقانونية والإعلامية، إضافة إلى رفع الوعي العام بمخاطر الاستخدام غير الآمن للتكنولوجيا، وتلعب الصحافة الرقمية دورًا جوهريًا في هذه المنظومة من خلال نشر ثقافة الوعي الأمني لدى الجمهور، وتبسيط المفاهيم التقنية المعقدة بلغة مفهومة، وتسليط الضوء على قضايا تسريب البيانات وانتهاكات الخصوصية. فهي لا تكتفي بدور الإخبار، بل تمتد إلى التثقيف والمساءلة وبناء الثقة بين المؤسسات والجمهور، مما يجعلها شريكًا أساسيًا في منظومة الأمن السيبراني والمواطنة الرقمية المسؤولة (Preprints.org, 2024؛ Westlund et al., 2025).

الإطار النظري للبحث:

نظرية الإتصال بالمخاطر Risk Communication Theory:

الاتصال بالمخاطر هو عملية تواصل تهدف إلى تبادل المعلومات والآراء حول المخاطر بين خبراء وصناع القرار وأفراد الجمهور بغرض تمكين الفهم المشترك وتحسين استجابات الأفراد والمؤسسات لتلك المخاطر (Lopez, R., & Cho, H,2022)، ووفقاً لهذا المفهوم لا يعني الاتصال مجرد نقل المعلومات بل يشمل تفسير الرسالة واعتبارات الثقة والقيم وردود الفعل النفسية وسياق التلقي (Balog-Way & McComas, 2020)، ويُميز الباحثون بين الاتصال بالمخاطر (قبل وقوع الأزمات) والاتصال في الأزمات؛ فالتركيز في النوع الأول هو التوعية والوقاية، بينما في النوع الثاني يكون على إدارة الأضرار والشفافية والتواصل في زمن الحدث (Munro et al., 2024).

الأهداف الأساسية لنظرية الاتصال بالمخاطر: أظهرت البحوث أن الاتصال بالمخاطر يشكّل عاملًا تأصيليًا لفهم الجمهور للمخاطر، ودوره الوسيط بين الرسالة والسلوك الوقائي (Heydari et al., 2021)، **و**يمكن تقسيم الأهداف الأساسية للنظرية إلى:

- التوعية والتعليم: ويقصد به نشر المعرفة حول طبيعة المخاطر، احتمالاتها، وطرق الوقاية أو التخفيف.

- التأثير السلوكي: ويشمل تحفيز الأفراد على اتخاذ إجراءات وقائية أو تعديل سلوكهم لتقليل التعرض للمخاطر.

- الإعداد والاستجابة للطوارئ: وتشمل المساعدة في استعداد الجمهور أو المؤسسات للأزمات، أو في إدارة الأضرار في زمن الأزمة.

- إدارة المشاعر النفسية والعاطفية: وتتضمن الحد من القلق، الخوف أو الذعر، وتعزيز الشعور بالطمأنينة أو القدرة على السيطرة.

- البُعد المؤسسي والتنظيمي: ويشمل جعل الاتصال بالمخاطر جزءًا من استراتيجيات المنظمات، تعزيز الشفافية والمساءلة وبناء الثقة مع الجمهور.

- الشرعية والثقة: ويقصد به تعزيز المصداقية والثقة بالمُرسِل (الجهة التي تقدّم الرسالة) كجزء أساسي لفعالية الاتصال.

فروض النظرية:

- تحسين جودة الاتصال (وضوح الرسالة، موثوقية المصدر، التوقيت) يؤدي إلى رفع وعي الجمهور وإدراكهم للمخاطر.

- أن الرسائل التي تتضمن توصيات واضحة وقابلة للتنفيذ تزيد من احتمال التزام الأفراد بها.

- تؤثر خلفيات الجمهور المعرفية والقيم الثقافية والثقة في المصدر والخبرات السابقة على كيف تُفسَّر الرسالة وتُستقبل.

ويعتبر الاتصال بالمخاطر مرتبط ارتباطًا وثيقًا بالأمن السيبراني، وذلك للأسباب التالية(Schaltegger et al., 2025) :

- أهمية الاتصال بالمخاطر السيبرانية.

- التهديدات السيبرانية معقدة وغير مرئية وفهمها للجمهور العام صعب، ما يخلق فجوة معرفية.

- طبيعة التهديدات تتغير بسرعة (تحديث ثغرات، ظهور هجمات جديدة)، مما يزيد من عدم اليقين في الرسائل الأمنية.

- غالبًا ما يرتبط سلوك البشر بالاختراقات: خطأ بسيط، إغفال، تصفح غير آمن، فتح رسائل مزيفة. لذا فالتواصل الفعّال يمكن أن يقلل من هذه المخاطر البشرية.

الدراسات السابقة:

قام الباحث بالاطلاع على الدراسات السابقة والمرتبطة بموضوع البحث من خلال البحث في المكتبات ومواقع المجلات العلمية وبعد الحصول على الدراسات الأكثر ارتباطا بالموضوع تم تنظيمها وتصنيفها إلى محورين يمكن عرضهما كالآتي:

أولاً: دراسات تناولت أطر معالجة قضايا الأمن السيبراني في الصحافة الرقمية:

في ظل تنامي التهديدات الرقمية التي تواجه المؤسسات والجمهور على حد سواء، تزايد الاهتمام الأكاديمي بدراسة معالجة قضايا الأمن السيبراني في الصحافة الرقمية، بوصفها ضرورة لحماية البيانات والمصادر وضمان موثوقية المحتوى، وفي هذا الإطار هدفت دراسة (Schäfer et.al, 2025) بعنوان كيف يُناقَش الأمن السيبراني عبر قنوات الإعلام؟ تحليلات استكشافية لمحتوى تويتر والتقارير الإخبارية، إلى التعرف على كيفية تناول موضوع الأمن السيبراني في وسائل الإعلام المختلفة، مركزةً على الخطاب العام عبر تويتر (X) والصحافة الإخبارية الألمانية، من خلال استخدام منهجًا مختلطًا جمع بين التحليل الحاسوبي لـ 242,715 تغريدة والتحليل

اليدوي لـ 574 تقريرًا إخباريًا، مع توظيف نظرية الدافع للحماية Protection Motivation Theory لتفسير الرسائل الإعلامية المتعلقة بالسلوكيات الوقائية، وتوصلت الدراسة إلى نتائج أهمها: أن موضوعات حماية البيانات وأمن المعلومات هي الأكثر تداولًا على تويتر، وأن الخبراء والمتخصصين التقنيين يمثلون الفاعلين الأكثر تأثيرًا في النقاش العام، بينما تميل وسائل الإعلام الإخبارية إلى التركيز على التهديدات والمخاطر السيبرانية أكثر من التركيز على الممارسات الوقائية أو تحميل الأفراد مسؤولية أمنهم الرقمي. كما كشفت الدراسة عن قصور في الخطاب الإعلامي التحفيزي وضعف في تعزيز الكفاءة الذاتية للمواطنين تجاه حماية بياناتهم. وخلص الباحثون إلى أن الإعلام، بشقيه الرقمي والإخباري، لا يزال يفتقر إلى نهج تواصلي فعّال يشجع الجمهور على تبنّي سلوكيات الحماية السيبرانية.

كما هدفت دراسة (Fahim K. Sufi, 2025) بعنوان: طريقة جديدة لقياس وتحليل التحيّز الإعلامي في تغطية قضايا الأمن السيبراني، إلى تطوير إطار حاسوبي قائم على الذكاء الاصطناعي يهدف إلى تحليل وقياس أنماط التحيّز في التغطية الإعلامية للأحداث المتعلقة بالأمن السيبراني، انطلقت الدراسة من فرضية أن التحيّز في تناول القضايا السيبرانية سواء من حيث التركيز الجغرافي للمصادر الإعلامية أو نوع الأحداث المغطاة أو درجة أهميتها، ويؤدي إلى تشويه وعي الجمهور وتوجيه صناع القرار بشكل غير متوازن، واعتمد الباحث على منهج تحليلي كمي مدعوم بالذكاء الاصطناعي من خلال تحليل 1.23 مليون مادة إخبارية تم تصفيتها إلى 9314 حدثًا سيبرانيًا من 144 مصدرًا إعلاميًا على مدى خمسة أرباع زمنية متتالية، وتوصلت الدراسة إلى نتائج أهمها: أن المصادر العامة مثل BBC أظهرت تنوعًا مرتفعًا في تغطية قضايا الأمن السيبراني، بينما ركزت المصادر المتخصصة مثل Cybersecurity Insider على موضوعات محددة، كما بلغت دقة نموذج الانحدار اللوجستي 81.2% في التنبؤ بأنماط التغطية، وأوصت الدراسة بضرورة توسيع هذا الإطار التحليلي ليشمل منصات التواصل الاجتماعي بهدف كشف التحيّز والمعلومات المضللة وتعزيز الشفافية الإعلامية في تناول قضايا الأمن السيبراني.

وهدفت دراسة (Park, Seo & Kwon,2024) بعنوان الأمن السيبراني في المواقع الذكية: من منظور التواصل بالمخاطر، إلى استكشاف دور الاتصال الإعلامي في تعزيز وعي الجمهور بمخاطر الأمن السيبراني ضمن بيئة المدن الذكية، واعتمد الباحثون على المنهج الكيفي من خلال تحليل مقابلات معمقة مع خبراء أمن وتقنيين ومسؤولي سياسات عامة، إضافة إلى مسح بالاستبيان استهدف سكان بعض المدن الكورية الذكية، وتوصلت الدراسة إلى نتائج أهمها: الأطر الإعلامية الموجهة للجمهور تركز بشكل أساسي على فكرة التهديد الخارجي والخطر القومي، بينما قلّ حضور أطر الحلول التكنولوجية التشاركية، كما كشفت الدراسة أن فجوة الثقة بين الجمهور وصناع القرار تعوق تبني استراتيجيات أمنية فعالة، وأن إدماج الصحافة العلمية في حملات التوعية يمكن أن يسهم في رفع إدراك المواطنين بمخاطر الهجمات الإلكترونية.

وهدفت دراسة (العسكري، 2024) بعنوان متطلبات تحقيق الأمن السيبراني والتصدي للجرائم الإلكترونية في ضوء الرقمنة الإعلامية، إلى بيان أهمية الأمن السيبراني في حماية المعلومات، والكشف عن أسباب الجرائم الإلكترونية وآليات الإعلام الرقمي في التوعية بضرورتها ومواجهتها، واعتمدت الدراسة على المنهج الوصفي التحليلي من خلال مراجعة الأدبيات والدراسات السابقة، وناقشت عدة محاور أبرزها: آليات الإعلام الرقمي في دعم الأمن السيبراني، متطلبات تحقيق الحماية من الجرائم الإلكترونية، وجهود الدولة والاستراتيجيات الوطنية لمكافحة التهديدات السيبرانية. وتوصلت الدراسة إلى نتائج أهمها: ضرورة تنويع المحتوى الإعلامي الموجه للجمهور بأساليب مبتكرة، وتعزيز التعاون بين الجهات الرسمية والإعلامية عبر اتفاقيات مشتركة لمواجهة الهجمات السيبرانية، إضافة إلى تطوير التشريعات والقوانين وفرض العقوبات الرادعة للمجرمين الإلكترونيين.

وهدفت دراسة (زيدان، 2024) بعنوان تنمية ثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية (تصور مقترح)، إلى التعرف على واقع ثقافة الأمن السيبراني لدى طلاب جامعة حلوان، والكشف عن أهم كفايات التربية الإعلامية الرقمية اللازمة لتنميتها، مع وضع تصور مقترح لتعزيز تلك الثقافة. اعتمدت الدراسة على المنهج الوصفي، واستخدمت الاستبيان كأداة لجمع البيانات من عينة مكونة من (347) طالبًا من كليات التربية، والتجارة وإدارة الأعمال، والسياحة والفنادق بجامعة حلوان، وتوصلت الدراسة إلى نتائج أهمها: وجود ضعف واضح في تركيز اللوائح الجامعية على قضايا الأمن السيبراني، إضافة إلى نقص المتخصصين والبرامج التدريبية في هذا المجال، وانخفاض مستوى وعي الطلاب بأساليب الاستخدام الآمن لشبكات الإنترنت العامة، وعدم اهتمامهم باستخدام كلمات مرور قوية أو تحديث البرامج والتطبيقات بشكل منتظم، مما يجعلهم عرضة لمخاطر الاختراق والاحتيال الإلكتروني، وأوصت الدراسة بضرورة تصميم برامج تدريبية وتوعوية متخصصة لتعزيز الثقافة الأمنية الرقمية لدى الطلاب.

وهدفت دراسة (عصام وآخرون، 2024) بعنوان تقنيات الذكاء الاصطناعي في الإعلام الرقمي وتأثيرها على آراء الطلاب نحو قضايا الأمن السيبراني داخل الحرم الجامعي، إلى التعرف على أثر دمج تقنيات الذكاء الاصطناعي في الإعلام الرقمي على وعي الطلاب الجامعيين واتجاهاتهم نحو قضايا الأمن السيبراني، واعتمد الباحثين على المنهجين الوصفي والتحليلي، باستخدام أدوات متعددة تمثلت في الاستبيانات، والمقابلات الشخصية، وتحليل المحتوى، وأجريت الدراسة على عينة عمدية من (30) طالباً وطالبة بجامعة كفر الشيخ خلال عام 2024، وتوصلت الدراسة إلى نتائج أهمها: أن الإعلام الرقمي المدعوم بالذكاء الاصطناعي كان له دور بارز في تعزيز وعي الطلاب بقضايا الأمن السيبراني والتأثير على آرائهم واتجاهاتهم، كما بيّنت الدراسة أهمية إدماج هذه التقنيات في العملية التعليمية والتوعوية داخل الجامعات.

كما هدفت دراسة (إبراهيم،2024) بعنوان: دور المواقع الصحفية المصرية والعربية في نشر الوعي السيبراني لدى الجمهور، إلى التعرف على دور المواقع الصحفية الإلكترونية المصرية والعربية في نشر الوعي بالأمن السيبراني لدى الجمهور، واعتمدت الدراسة على منهج المسح الإعلامي بشقيه التحليلي والميداني، من خلال تحليل مضمون لخمسة مواقع صحفية عربية ومصرية هي: الشرق القطري، البيان الإماراتي، الأنباء الكويتي، اليوم السابع المصري، والأهرام الإلكتروني، خلال عامي 2021–2022، بإجمالي (1487) مادة صحفية، كما أجرت الباحثة استبيانًا ميدانيًا على عينة من (400) مفردة من الجمهور العام، وتوصلت الدراسة إلى نتائج أهمها: أن المواقع العربية والمصرية ركزت بصورة رئيسية على قضايا الجرائم التي تمس الأفراد والمؤسسات، بينما قلّ اهتمامها بالقضايا المتعلقة بأمن الدول، كما وُجدت فروق دالة بين المواقع الخليجية والمصرية في نوعية الجرائم التي تناولتها، إذ تصدّرت البرامج الفيروسية الضارة التغطيات في المواقع الخليجية، بينما برز الجهاد الإلكتروني في موقع الشرق القطري، كما أن هذه المواقع تؤدي دورًا إخباريًا وتوعويًا فعالًا، لكنها لم تُوجّه الرأي العام بشكل واضح نحو تبنّي مواقف محددة، ما يعكس حرية نسبية في معالجة قضايا الأمن السيبراني.

وهدفت دراسة (Majebi, N. L., & Drakeford, O. M. 2021) بعنوان سلامة الأطفال في العصر الرقمي: الدروس التاريخية من تنظيم وسائل الإعلام وتطبيقها على سياسات الأمن السيبراني الحديثة، إلى تحليل الأطر التاريخية لتنظيم الإعلام وكيف يمكن الاستفادة منها في تطوير سياسات الأمن السيبراني الحديثة المتعلقة بحماية الأطفال على الإنترنت، من خلال مقارنة بين التشريعات القديمة مثل قانون تلفزيون الأطفال لعام 1990 ، ومدونة إنتاج الأفلام، وتوجيهات لجنة الاتصالات الفيدرالية FCC ، والسياسات الرقمية المعاصرة مثل قانون حماية خصوصية الأطفال على الإنترنت COPPA واللائحة العامة لحماية البيانات GDPR الخاصة بالقُصّر، وتوصلت الدراسة إلى نتائج أهمها: أن البيئة الرقمية الحديثة تتسم بالطابع اللامركزي والعالمي، ما يجعل تطبيق القوانين التقليدية تحديًا كبيرًا، كما أكدت أن الإشراف غير المتسق من شركات التواصل الاجتماعي يضعف فعالية جهود الحماية، وأوصت الدراسة بضرورة تعزيز أدوات الرقابة الأبوية المعتمدة على الذكاء الاصطناعي، والتي تتيح التصفية التكيفية للمحتوى والمراقبة في الوقت الفعلي. كما دعت إلى تنفيذ برامج محو الأمية الرقمية للأطفال بالتعاون بين المدارس والأسر والقطاعين العام والخاص، بما يعزز التفكير النقدي والوعي بالمخاطر الإلكترونية.

- دراسات تناولت التوعية نحو التهديدات الرقمية:

شهدت السنوات الأخيرة اهتمامًا متزايدًا من الباحثين بدراسة قضايا الأمن السيبراني في الصحافة الرقمية، في ظل تصاعد التهديدات التي تستهدف البيانات والمصادر الإعلامية وموثوقية المحتوى، حيث هدفت دراسة (هلال، 2025) بعنوان: تصور مقترح لمواجهة تهديدات الأتمتة في التعليم الثانوى العام بمصر، إلى تحليل الفرص والتحديات والمخاوف والمخاطر والتهديدات التي قد تنجم عن تطبيق الأتمتة في التعليم العام، حيث تم مناقشة مفهوم الأتمتة وتهديداتها المختلفة وعلاقتها بالمفاهيم المتقاربة منها، من: الذكاء الاصطناعي والرقمنة والتحول الرقمي،

وتم تحليل واقع الوضع الحالي لجهود أتمتة التعليم الثانوى العام في مصر، وتقديم تصور مقترح لمواجهة تلك التهديدات مثل: تعزيز التنشئة الاجتماعية ومكافحة ظواهر التحيز والتمييز الخوارزمي ومكافحة الانتحال في الامتحانات المؤتمتة، وتوافر آليات المسؤولية الفعالة، وحماية خصوصية الأفراد وتعزيز الأمن السيبراني.

وهدفت دراسة (البدوي، 2024) بعنوان الحرب الرقمية والأمن السيبراني: خطر التهديدات يقابله تعزيز الدفاعات، إلى الكشف عن مظاهر الحرب السيبرانية وأثرها المتنامي على الحكومات والمنظمات والأفراد، مع التركيز على الدور الحاسم للأمن السيبراني في التخفيف من آثار هذه التهديدات، واعتمدت الدراسة على منهج تحليلي وصفي من خلال مراجعة الأدبيات ودراسات الحالة، حيث تم جمع بيانات من مصادر موثوقة حول الأنواع المختلفة للحرب السيبرانية، وتكتيكات الهجمات الإلكترونية مثل سلسلة القتل السيبراني والتهديدات المستمرة المتقدمة APTs، إضافة إلى الاستجابات الحكومية والدولية، ودور القطاع الخاص والمنظمات غير الربحية، وتوصلت الدراسة إلى نتائج أهمها: أن الحرب الرقمية تمثل تهديداً متزايداً للأمن العالمي، وأن فعالية الدفاعات تعتمد على التكامل بين السياسات الحكومية، التدابير القانونية، والتعاون بين القطاعات. وأوصت الدراسة بضرورة تبني استراتيجيات وقائية قائمة على المرونة وتبادل المعلومات لتعزيز قدرة الدول والمؤسسات على مواجهة التهديدات الرقمية.

كما أجرى (كلنتن، 2024) دراسة بعنوان التحديات والمخاطر بفقدان الثقة الإعلامية في ظل الإعلام الرقمي بسبب انتهاك الخصوصية والهجمات السيبرانية في المملكة العربية السعودية، وهدفت الدراسة إلى الكشف عن المخاطر التي يسببها فقدان الثقة الإعلامية نتيجة انتهاكات الخصوصية والهجمات السيبرانية في البيئة الرقمية. اعتمدت الدراسة على المنهج الوصفي الميداني من خلال استبيان إلكتروني طبقت على عينة مكونة من (69) مشاركاً، منهم (30) من المختصين في التقنية الرقمية و(39) من الأفراد العاديين ممن لديهم تجارب فعلية مع انتهاك الخصوصية، وتوصلت الدراسة إلى نتائج أهمها: أن الانتهاكات السيبرانية والإرهاب الرقمي يسهمان بشكل كبير في تآكل الثقة بالأنظمة الرقمية، كما كشفت أن سياسات الخصوصية في معظم مواقع التواصل الاجتماعي غير واضحة للمستخدمين، مما يؤدي إلى استغلال بياناتهم الشخصية. وأوصت الدراسة بضرورة وضع استراتيجيات وطنية لتعزيز أمن المعلومات، ورفع الوعي الرقمي، وتطوير السياسات والتشريعات الخاصة بحماية الخصوصية لمواجهة التهديدات السيبرانية.

وهدفت دراسة (جبار، 2024) بعنوان دور الإعلام الرقمي في توعية الجمهور العراقي بمخاطر وجرائم الأمن السيبراني، إلى التعرف على دور الإعلام الرقمي في زيادة الوعي الأمني السيبراني لدى الجمهور العراقي، وتسليط الضوء على كيفية مساهمته في التعريف بالمخاطر والجرائم السيبرانية، استخدم الباحث المنهج المسحي على عينة مكونة من (400) مفردة من مستخدمي الوسائل الرقمية ومنصات التواصل الاجتماعي في العراق، خلال الفترة من 1/1 إلى 1/2 من عام 2024 ، وتوصلت الدراسة إلى نتائج أهمها: أن وسائل الإعلام الرقمية، وخاصة

شبكات التواصل الاجتماعي، تمثل المصدر الرئيس للجمهور العراقي لمعرفة أخبار وجرائم الأمن السيبراني، وكان أبرزها تهكير المواقع الإلكترونية، كما بيّنت الدراسة أن الإعلام الرقمي يلعب دوراً إيجابياً في التوعية بمخاطر الجرائم الإلكترونية، وتقديم معلومات وقائية حولها، إضافة إلى أن ثقة المبحوثين بالمعلومات المنشورة عبر الإعلام الرقمي كانت مرتفعة، ما يعكس أهميته في تعزيز الأمن السيبراني المجتمعي.

وأجرى (Valerii Muzykant, 2023) دراسة بعنوان التهديدات الرقمية وتحديات الجيل الرقمي في التعليم الإعلامي: حالة إندونيسيا، وهدفت إلى تفسير التهديدات والتحديات التي تواجه مستخدمي الإنترنت في إندونيسيا، خصوصاً بعد تفشي جائحة كوفيد-19 وما تبعها من هجرة رقمية واسعة النطاق، واعتمدت الدراسة المنهج الوصفي التحليلي من خلال مراجعة الأدبيات وتحليل الظواهر الرقمية المعاصرة التي تؤثر على المجتمع الإندونيسي، وتوصلت الدراسة إلى نتائج أهمها: أن التطور التكنولوجي المتسارع أدى إلى ما يُسمى بـ «العجز الرقمي»، حيث تتعرض القدرات الإدراكية للأفراد إلى تحديات بسبب فرط الاتصال الرقمي وما ينتج عنه من ضعف الانتباه والإدمان على الأنشطة الرقمية، إضافة إلى تفشي الممارسات الضارة مثل التلاعب بالمعلومات، التنمر الرقمي، والاحتيال عبر الإنترنت. وأوصت الدراسة بضرورة دمج الكفاءات الرقمية والإعلامية ضمن المناهج الدراسية في مراحل التعليم المبكرة لتعزيز الوعي وحماية الأفراد من المخاطر الرقمية وضمان امتلاكهم كفاءة رقمية متكاملة.

وأجرت (البحيري،2023) دراسة بعنوان دور الإعلام الرقمي في تعزيز الأمن السيبراني ومقاومة التهديدات والجرائم السيبرانية، هدفت إلى التعرف على إسهام الإعلام الرقمي في دعم الأمن السيبراني، إضافة إلى دوره في مواجهة الجرائم والتهديدات السيبرانية. استخدمت الباحثة المنهج المسحي التطبيقي على عينة عمدية مكونة من (64) إعلامياً من مؤسسات مصرية مختلفة (الصحافة، الإذاعة، والتلفزيون). وتم جمع البيانات من خلال استمارة استبيان، وتوصلت الدراسة إلى نتائج أهمها: أن الإعلام الرقمي يقوم بدور كبير في تعزيز الأمن السيبراني بدرجة مرتفعة، كما يساهم بشكل فاعل في مقاومة التهديدات والجرائم السيبرانية بدرجة مرتفعة أيضاً، وأوصت الدراسة بضرورة وضع استراتيجية متكاملة لمكافحة التهديدات الرقمية، إلى جانب تأهيل كوادر متخصصة في الأمن السيبراني وتدريب المستخدمين على أساسيات حماية البيانات.

كما هدفت دراسة (Chen, 2022) بعنوان التواصل بالمخاطر في الفضاء السيبراني: السرد الإعلامي والفهم العام، إلى فهم العلاقة بين الأطر الإعلامية في الصحافة العلمية والإدراك العام لمخاطر الأمن السيبراني، واستخدمت المنهج الوصفي التحليلي من خلال مراجعة محتوى صحف عالمية مثل نيويورك تايمز والجارديان، إلى جانب استطلاع رأي شمل 800 مشارك من الولايات المتحدة والمملكة المتحدة، وتوصلت النتائج إلى: أن الأطر السائدة في التغطية الإعلامية كانت الأمن القومي وتهديد الخصوصية، بينما كان إطار التوعية الوقائية أقل حضورًا، كما تبين أن إدراك الجمهور يتأثر بشكل كبير بالتركيز الإعلامي على التهديدات، مما يخلق حالة من الخوف والقلق دون تقديم حلول عملية.

وهدفت دراسة (Chen,2020) بعنوان: الاتصال بالمخاطر في البيئة الرقمية، إلى مراجعة الأدبيات الخاصة بتطبيقات الاتصال بالمخاطر في قضايا الأمن السيبراني، واعتمدت على تحليل نوعي ومراجعة موسعة للأبحاث السابقة، وأظهرت أن هناك فجوة واضحة بين النماذج الذهنية للخبراء والجمهور. كما أوضحت أن وسائل الإعلام غالبًا ما تستخدم لغة تقنية معقدة لا تصل بسهولة إلى القراء العاديين، مما يقلل من فاعلية التغطية الإعلامية في رفع وعي الجمهور، وخلصت إلى ضرورة تبني الصحافة العلمية لأطر مبسطة تدمج بين التفسير العلمي والبعد الاجتماعي.

التعليق على الدراسات السابقة:

في ضوء مراجعة الدراسات السابقة التي تناولت أطر معالجة قضايا الأمن السيبراني في الصحافة الرقمية، يتبين تنوعها من حيث الموضوعات والمناهج والأدوات البحثية والعينات، بما يعكس اتساع الاهتمام العلمي بهذه القضية المعقدة التي تتقاطع فيها أبعاد تقنية وإعلامية وثقافية وتشريعية. فعلى مستوى الموضوعات، ركزت بعض الدراسات على تحليل الخطاب الإعلامي تجاه الأمن السيبراني، مثل دراسة (Schäfer,2025) التي حللت محتوى تويتر والتقارير الإخبارية الألمانية، مبرزةً هيمنة موضوعات التهديد والمخاطر على حساب السلوكيات الوقائية. في المقابل، اهتمت دراسات أخرى بتطوير أطر كمية لقياس التحيز في التغطية الإعلامية كما في دراسة(Fahim Sufi, 2025 ، التي طورت نموذجًا حسابيًا مدعومًا بالذكاء الاصطناعي لتحليل أكثر من مليون مادة إخبارية. بينما تناولت دراسات مثل (Park, Seo & Kwon,2024)موضوع الأمن السيبراني من منظور الاتصال بالمخاطر في المدن الذكية، وهو اتجاه جديد يربط بين التواصل الإعلامي والتخطيط الحضري الذكي. أما الدراسات العربية مثل (العسكري،2024) و(إبراهيم،2024) و(زيدان،2024)، فقد ركزت على الأبعاد التوعوية والمؤسسية والتعليمية لقضايا الأمن السيبراني في الإعلام الرقمي، مع التركيز على تطوير الثقافة الرقمية في الجامعات والمجتمع. كذلك تناولت دراسات أخرى العلاقة بين الإعلام والذكاء الاصطناعي مثل دراسة (عصام وآخرين،2024) التي استكشفت أثر الإعلام الرقمي المدعوم بالذكاء الاصطناعي على وعي الطلاب بقضايا الأمن السيبراني.

أما من حيث نوع الدراسات والمناهج المستخدمة، فقد تميزت الدراسات الأجنبية باتباعها للمناهج المختلطة والتحليلية الكمية المدعومة بالذكاء الاصطناعي أو التحليل الإحصائي واسع النطاق، كما في دراستي Schäfer وSufi ، اللتين استخدمتا تحليلًا ضخمًا للبيانات الرقمية ومنصات التواصل الاجتماعي. في حين اعتمدت دراسات أخرى مثل (Park et.al,2024) المنهج الكيفي بالاعتماد على المقابلات المتعمقة والمسوح الميدانية، وهو ما أتاح فهماً أكثر عمقًا لطبيعة إدراك المخاطر واتجاهات الجمهور. أما الدراسات العربية فقد اعتمدت في الغالب على المنهج الوصفي التحليلي، إما عبر مراجعة الأدبيات كما في دراسة (العسكري،2024)، أو عبر تحليل محتوى المواقع الإخبارية كما في دراسة (إبراهيم،2024)، أو عبر تطبيق استبيانات ميدانية لقياس الوعي والثقافة الأمنية لدى الجمهور والطلاب كما في دراسة (زيدان،2024). كما أن هناك عدداً من الدراسات دمج بين أكثر من منهج وأداة لجمع بيانات كمية وكيفية، مما عزز موثوقية النتائج.

وفيما يتعلق بـ العينات والأدوات البحثية، نجد أن الدراسات الأجنبية اعتمدت على عينات كبيرة الحجم ومتنوعة، حيث قامت دراسة (Sufi, 2025) بتحليل أكثر من 1.23 مليون مادة إخبارية، بينما حللت دراسة (Schäfer, 2025) مئات الآلاف من التغريدات والتقارير الإخبارية. أما الدراسة الكورية (Park et. al. 2024) فجمعت بين مقابلات الخبراء واستطلاعات ميدانية لسكان المدن الذكية. على الجانب العربي، اقتصرت العينات غالبًا على طلاب الجامعات أو الصحفيين أو الجمهور العام، كما في دراسة)زيدان،2024) طبقت على عدد 347 طالبًا، ودراسة (إبراهيم، 2024) طبقت على400 مفردة من الجمهور، ودراسة (عصام وآخرين،2024) والتي طبقت على 30 طالبًا، أما الأدوات فقد تنوعت بين الاستبيانات، والمقابلات، وتحليل المضمون، والمراجعات الأدبية، والنماذج الحسابية المعتمدة على الذكاء الاصطناعي. هذا التنوع المنهجي يعكس اختلاف السياقات البحثية، لكنه في الوقت ذاته يُظهر الحاجة إلى توسيع حجم العينات العربية.

أما على صعيد النتائج، فقد اتفقت معظم الدراسات على أن الخطاب الإعلامي حول الأمن السيبراني يميل إلى التركيز على التهديدات والمخاطر أكثر من الحلول الوقائية، وهو ما يؤكده كل من (Schäfer, 2025) و(Chen, 2022)، كما أظهرت النتائج تفاوتاً واضحاً في درجة الوعي والاهتمام بقضايا الأمن السيبراني بين الجمهور في الدول المتقدمة والدول النامية؛ ففي حين ركزت الدراسات الغربية على التحليل البنيوي للمحتوى والسياسات الاتصالية، ركزت الدراسات العربية على دور الإعلام في التوعية والتثقيف، مثل دراسات (العسكري،2024) و(زيدان،2024) و(إبراهيم،2024)، التي خلصت جميعها إلى وجود قصور في توظيف الإعلام الرقمي لتثقيف الجمهور وتعزيز سلوكيات الأمان السيبراني. كما كشفت دراسات مثل (Majebi & Drakeford, 2021) عن فجوة تشريعية وتنظيمية في حماية الأطفال عبر الإنترنت، وأوصت بدمج أدوات الذكاء الاصطناعي في الرقابة الأبوية، وهي رؤية تتقاطع مع توصيات دراسات عربية دعت إلى تطوير تشريعات وطنية للأمن الرقمي.

وبوجه عام، يمكن القول إن هذه الدراسات – رغم تباينها في الاتجاهات والمنهجيات – أسهمت في بناء معرفة تراكمية حول العلاقة بين الإعلام والأمن السيبراني، وأظهرت الحاجة إلى مقاربات تكاملية تجمع بين التحليل الإعلامي والتكنولوجي والاجتماعي. ومع ذلك، يلاحظ أن معظم الأبحاث العربية لا تزال تركز على الجانب الوصفي أكثر من الجانب التحليلي التطبيقي، في حين أن الدراسات الغربية تميل إلى بناء نماذج قياس وتنبؤ كمية أكثر دقة.

الفجوة البحثية بناءًا على نتائج الدراسات السابقة:

تتجلى الفجوة البحثية في غياب الدراسات التكاملية التي تربط بين تحليل المضمون وقياس الأثر السلوكي، فقد نجحت الدراسات السابقة في تشخيص الواقع ووصف الظاهرة، إلا أنها توقفت عند هذا الحد، ومازالت هناك حاجة ملحة لبحث ينتقل من سؤال «ماذا يوجد في المحتوى؟ ما مستوى وعي الجمهور؟ إلى سؤال أكثر عمقاً وهو: ما مدى فعالية الأطر الإعلامية التوعوية المختلفة في تغيير اتجاهات المستخدمين وسلوكياتهم تجاه قضايا الأمن السيبراني؟ وهو ما تم دراسته في البحث الحالي.

مشكلة البحث:

يشهد العالم اليوم تزايدًا ملحوظًا في الاعتماد على الفضاء الرقمي في شتى مجالات الحياة، بدءًا من التعاملات المصرفية والتعليم والعمل عن بُعد، وصولًا إلى إدارة البنى التحتية الحيوية للدول، هذا الاعتماد الهائل جعل قضايا الأمن السيبراني في صدارة الاهتمامات العالمية، نظرًا لما يترتب على أي اختراق أو هجوم إلكتروني من تهديد مباشر للأمن القومي، الاقتصاد، والخصوصية الفردية، وفي ظل هذه التحديات، تبرز الصحافة الرقمية كوسيط رئيسي لتبسيط القضايا خاصة التقنية وإيصالها للجمهور بلغة مفهومة، ما يجعلها عنصرًا فاعلًا في تشكيل وعي المجتمع تجاه المخاطر والحلول.

غير أن دور الصحافة لا يتوقف عند حدود نقل المعلومات، بل يمتد إلى صياغة إدراك الجمهور من خلال أطر المعالجة الصحفية، وهي الطريقة التي يتم بها اختيار زوايا التناول وتحديد أولويات الخبر، هذا التباين في الأطر يطرح تساؤلاً حول مدى مساهمة الصحافة الرقمية فعلًا في بناء وعي نقدي ومتوازن تجاه قضايا الأمن السيبراني، أم أنها تعيد إنتاج الخطابات السائدة التي قد تبالغ في تصوير التهديدات أو تختزل الحلول؟ إن الإجابة عن هذا السؤال تكتسب أهميتها من كونها تكشف طبيعة العلاقة بين الإعلام والجمهور، وتحدد مدى قدرة الصحافة العلمية على أداء دورها التوعوي بعيدًا عن التضخيم أو التهوين.

وبناءً على ما سبق، تتحدد مشكلة الدراسة في السعي إلى فهم كيفية معالجة الصحافة الرقمية لقضايا الأمن السيبراني من خلال الأطر الإعلامية المختلفة، وتحليل أثر هذه الأطر على إدراك الجمهور للمخاطر والحلول المرتبطة بها. ومن هنا ينبثق سؤال البحث الرئيسي: ما أطر المعالجة الصحفية لقضايا الأمن السيبراني في الصحافة الرقمية؟ وما أثرها على إدراك الجمهور للتهديدات الرقمية؟

أهمية البحث:

أولًا: الأهمية النظرية

- قد يسهم البحث في توسيع نطاق تطبيق نظرية الأطر (Framing Theory) من خلال ربطها بقضايا الأمن السيبراني في الصحافة الرقمية، وهو مجال لم يحظَ بعد بالقدر الكافي من البحث – على حد علم الباحث- مقارنة بتغطية القضايا السياسية أو الاجتماعية.

- يقدم البحث إطارًا معرفياً لفهم العلاقة بين التناول الإعلامي للقضايا السيبرانية والاتجاه نحو التهديدات الرقمية، مما يعزز من التداخل بين علوم الإعلام والاتصال ودراسات الأمن السيبراني.

- يوضح البحث كيف تؤثر أطر التغطية على إدراك الأفراد للتهديدات والحلول، الأمر الذي يساهم في تشكيل الوعي الجمعي للجمهور وليس مجرد ناقل للمعلومة.

- يأتي هذ البحث لتغطي فجوة بحثية في الأدبيات التي تربط بين الصحافة الرقمية كوسيط معرفي وبين قضايا الأمن السيبراني والتهديدات الرقمية، مما يجعلها مرجعًا يمكن البناء عليه في بحوث مستقبلية.

ثانيًا: الأهمية التطبيقية

- يوفر البحث توصيات عملية للصحفيين في الصحف الرقمية حول كيفية صياغة أطر أكثر توازنًا عند معالجة قضايا الأمن السيبراني، بما يحقق التوازن بين التحذير من المخاطر وتقديم حلول واقعية.

- تساعد نتائج البحث صناع القرار على إدراك كيفية تأثير التغطيات الإعلامية في تشكيل الرأي العام حول السياسات السيبرانية، مما يمكنهم من تطوير استراتيجيات تواصل أكثر فعالية.

- يمكن من خلال نتائج البحث توجيه الحملات التوعوية نحو خطاب إعلامي يرفع مستوى الوعي الرقمي لدى الأفراد ويحفزهم على تبني سلوكيات آمنة بدلًا من الانسياق وراء خطاب التخويف أو اللامبالاة.

أهداف البحث:

يهدف البحث إلى تحليل أطر المعالجة الصحفية لقضايا الأمن السيبراني في الصحافة العلمية، والكشف عن أثر هذه الأطر على إدراك الجمهور للمخاطر والحلول المرتبطة بها.

أولًا: الأهداف التحليلية

- رصد الأطر الصحفية المستخدمة في تناول قضايا الأمن السيبراني في الصحف الرقمية عينة البحث.

- تصنيف الأطر الإعلامية وفقًا لتكرارها وأهميتها في التغطيات الإعلامية.

- التعرف على أهم قضايا الأمن السيبراني التي تعالجها الصحف العلمية الرقمية عينة البحث.

- رصد أهداف معالجة قضايا الأمن السيبراني في الصحف العلمية الرقمية عينة البحث.

ثانيًا: الأهداف الميدانية:

- تحديد مستوى تعرض العينة للصحافة الرقمية عينة البحث.

- رصد أهم القضايا التي تتابعها العينة في الصحف الرقمية عينة البحث.

- تحديد مستوى ثقة الجمهور في معالجة قضايا الأمن السيبراني في الصحف الرقمية عينة البحث.

- قياس أثر الأطر الصحفية على إدراك العينة لمستوى التهديدات السيبرانية وحجمها.

- تحديد مدى إدراك الجمهور للتهديدات الرقمية.

متغيرات البحث:

- **المتغير المستقل:** أطر المعالجة الصحفية لقضايا الأمن السيبراني في الصحافة الرقمية.
- **المتغير التابع:** إدراك النخب الإعلامية للتهديدات الرقمية.
- **المتغيرات الوسيطة:** المتغيرات الديموجرافية (النوع - نوع النخبة).

فروض الدراسة:

الفرض الأول: توجد علاقة ذات دلالة إحصائية بين تبني النخب للأطر في معالجة قضايا الأمن السيبراني في الصحافة الرقمية وإدراكهم للتهديدات الرقمية.

الفرض الثاني: توجد فروق ذات دلالة إحصائية بين النخب الإعلامية عينة الدراسة فيما يتعلق بحجم اهتماماتهم بقضايا الأمن السيبراني حسب المتغيرات الديموجرافية (النوع ونوع النخب).

الفرض الثالث: توجد فروق ذات دلالة إحصائية بين النخب الإعلامية عينة الدراسة فيما يتعلق بمستوى إدراكهم للتهديدات الرقمية حسب المتغيرات الديموجرافية النوع ونوع النخب).

الفرض الرابع: توجد علاقة ذات دلالة إحصائية بين معدل ثقة النخب في معالجة الصحف لقضايا الأمن السيبراني ومستوى ادراكهم للتهديدات الرقمية.

نوع ومنهج البحث:

ينتمي هذا البحث إلى البحوث الوصفية بشقيها التحليلي والميداني، باستخدام أسلوب المسح بالعينة على عينتين إحداهما تحليلية على بوابة الأهرام وموقع اليوم السابع، والأخرى عينة ميدانية على عينة من النخب الإعلامية، كما تستخدم المنهج المقارن للمقارنة بين مفردات العينة التحليلية من جهة وبين مفردات العينة الميدانية.

المجتمع والعينة:

أولاً: مجتمع وعينة الدراسة التحليلية: يشمل مجتمع الدراسة التحليلية جميع المواد الصحفية المنشورة في الصحافة الرقمية التي تتناول موضوعات الأمن السيبراني، وتشمل العينة المواد الصحفية المنشورة في بوابة الأهرام وموقع اليوم لسابع خلال الفترة من 1 أبريل 2025 حتى 30 سبتمبر 2025م.

ثانياً: مجتمع وعينة الدراسة الميدانية: يشمل مجتمع البحث الحالي النخب الإعلامية الأكاديمية والمهنية بجمهورية مصر العربية، وأجري البحث الحالي على عينة متاحة قوامها 422 مفردة موزعة إلى (198 أساتذة الإعلام بالجامعات المصرية وإلى 224 من الممارسين في الصحف المصرية) خلال الفترة من 1 إلى 30 أكتوبر 2025م.

أدوات البحث(*):

1- استمارة تحليل المضمون: قام الباحث بإعداد وتصميم استمارة تحليل المضمون في صورتها الأولية بعد تحديد الفئات وتعريفها إجرائيا لتتفق مع أغراض التحليل وقد تم تقسيم الاستمارة وإعدادها بما يفي بالإجابة على تساؤلات الدراسة، حيث اشتملت على مجموعة من الفئات الأساسية التي تخدم أهداف الدراسة التحليلية. وتضمنت الاستمارة فئات للتحليل وهي: الفنون الصحفية المستخدمة، ووسائل الإبراز المستخدمة، والوسائط المتعددة المستخدمة، وأنواع الجرائم السيبرانية، والهدف من النشر، والأطر الإعلامية المستخدمة.

2- **استمارة الاستبيان:** استخدم الباحث الاستبيان كأداة لجمع البيانات والذي تضمن أسئلة حول استخدام الصحافة الرقمية ومقياس التهديدات الرقمية والذي تضمن 6 أبعاد، وتم تطبيقه إلكترونيا من خلال Google Drive وذلك لسهولة الوصول للعينة حيث أنها تغطي أكثر من فئة مع تنوع أماكن تواجدها، كما أن التطبيق الالكتروني يوفر الوقت والجهد، وتم عرض استمارة الاستبيان على عدد من المحكمين في مجالات الإعلام والإعلام التربوي وتكنولوجيا التعليم للتأكد من قياس الاسئلة لما وضعت لقياسه، وللتأكد من مدى ثبات الاستبيان قام الباحث بتطبيق معادلة ألفا كرونباخ Cronbach's Alpha والتي بينت أن معاملات الثبات لكل أبعاد الاستبيان بين (89% إلى 91%). وتم حساب الصدق الذاتي كمؤشر لصدق الاستبيان، وقد جاء مساويًا (0.89)، وهو ما يدل على درجة عالية من الصدق في الاستبيان.

مصطلحات البحث:

- **أطر المعالجة:** ويقصد بها القوالب التي يختارها الصحفي لتفسير الأحداث والقضايا، من خلال انتقاء زوايا معينة تبرز جانبًا وتغفل آخر، ويقصد بها في البحث الحالي الأطر الصحفية المستخدمة في معالجة قضايا الأمن السيبراني، مثل: إطار التهديد، إطار الحلول، إطار المسؤولية، إطار الحرية والخصوصية ..إلخ.

- **الصحافة الرقمية:** ويقصد بها مجموعة الممارسات الإعلامية القائمة على استخدام المنصات الإلكترونية والتقنيات التفاعلية في إنتاج ونشر وتداول المحتوى الصحفي عبر الإنترنت، بهدف عرض القضايا العامة، وخاصة قضايا الأمن السيبراني، بأساليب متعددة الوسائط تجمع بين النص والصورة والفيديو والبيانات التفاعلية.

- **الأمن السيبراني:** ويشير إلى مجموعة من السياسات والتقنيات والإجراءات المصممة لحماية الأنظمة الرقمية والشبكات والبيانات من الهجمات أو الاختراقات أو الاستخدام غير المصرح به، ويقصد به في البحث الحالي جميع القضايا والموضوعات المتعلقة بالتهديدات الرقمية وحماية البيانات والتي يتم تناولها في الصحافة العلمية.

- **الاتصال بالمخاطر:** ويقصد به عملية تواصل منظم لتبادل المعلومات والآراء حول الأخطار المحتملة بين الصحافة الرقمية والجمهور، بهدف تعزيز الوعي واتخاذ قرارات تقلل من آثار تلك المخاطر.

- **إدراك التهديدات الرقمية:** ويقصد به مستوى وعي الجمهور بخطورة التهديدات السيبرانية، وثقته بالحلول المقدمة، وتأثره العاطفي (خوف، طمأنينة، حياد) نتيجة التعرض لأطر المعالجة الصحفية.

الأساليب الإحصائية المستخدمة:

استخدم الباحث أساليب احصائية لمعالجة وتحليل البيانات للوصول إلى تفسيرها هي: التكرار والنسبة المئوية، والمتوسط والانحراف المعياري، ومعامل الارتباط بيرسون واختبار ت (t-test) وتحليل التباين أحادي الاتجاه (One Way ANOVA)، واختبار المقارنة البعدية LSD .

نتائج البحث وتفسيراتها:

أولاً: نتاج الدراسة التحليلية:

جدول (1) الفنون المستخدمة في معالجة قضايا الأمن السيبراني

الصحف / الفنون المستخدمة	بوابة الأهرام		اليوم السابع		الإجمالي	
	ك	%	ك	%	ك	%
الخبر	154	50.99	162	55.29	316	53.11
التقرير	53	17.55	44	15.02	97	16.30
القصة الخبرية	33	10.39	38	12.97	71	11.39
الحديث	21	6.95	23	7.85	44	7.39
المقال	28	9.27	16	5.46	44	7.39
التحقيق	13	4.30	10	3.41	23	3.87
الإجمالي	302	100	293	100	595	100

يتضح من الجدول: أن الخبر الصحفي جاء في المرتبة الأولى ضمن الفنون الصحفية المستخدمة في تناول الموضوعات العلمية الخاصة بقضايا الأمن السيبراني في كلٍّ من بوابة الأهرام واليوم السابع، حيث بلغت نسبته 50.99% و55.29% على التوالي، بإجمالي 53.11% من إجمالي المواد المنشورة، وذلك يظهر ميل الصحف الرقمية المصرية إلى التناول الإخباري السريع والمباشر لتلك القضايا، بما يتوافق مع طبيعة الصحافة الإلكترونية التي تركز على الآنية والتحديث المستمر للمحتوى لجذب القارئ المتعجل.

وجاء التقرير الصحفي في المرتبة الثانية بنسبة إجمالية بلغت 16.30% ، مما يشير إلى اهتمام نسبي بتقديم معالجة تحليلية أو تفسيرية لبعض الموضوعات، بينما تراجع الحديث الصحفي والمقال إلى نسب محدودة بلغت 7.39% لكلٍّ منهما تقريبًا، في حين جاء التحقيق

الصحفي في ذيل الترتيب بنسبة 3.87% فقط، وهو ما يعكس ضعف التوجه نحو التناول الاستقصائي أو المعمق في معالجة هذه القضايا.

ومن الملاحظ أن بوابة الأهرام تفوقت نسبيًا على اليوم السابع في استخدام القوالب التحليلية مثل المقال والتقرير، إذ بلغت نسبة المقالات بها 9.27% مقابل 5.46% فقط في اليوم السابع. ويمكن تفسير ذلك بطبيعة جمهور الأهرام الذي يميل إلى القارئ المتخصص أو المثقف، مقارنة بجمهور اليوم السابع الذي يتجه أكثر نحو الأخبار العامة والترفيهية.

وتتوافق هذه النتائج مع ما أشار إليه (العدوي،2024) بأن المواقع الإخبارية المصرية تعتمد على الخبر القصير والتغطية العاجلة في تناول القضايا العلمية، بينما تندر الأشكال الصحفية المعمقة. كما تتفق مع ما ذكرته (العوضي،2009) أن معظم التغطيات العلمية في الإعلام العربي تتخذ الطابع الإخباري السطحي بسبب قلة المتخصصين في الكتابة العلمية.

جدول (2) عناصر الإبراز المستخدمة مع قضايا الأمن السيبراني

الصحف / وسائل الابراز المستخدمة		بوابة الأهرام		اليوم السابع		الإجمالي	
		ك	%	ك	%	ك	%
العناوين	رئيسية	302	100	293	100	595	100
	ثانوية	122	40.40	60	20.48	182	30.59
الصور	إخبارية	201	66.56	189	64.51	390	65.55
	موضوعية	123	40.72	67	22.87	190	31.93
	شخصية	60	19.87	53	18.09	113	18.99
الرسوم	توضيحية	50	16.56	45	15.36	95	15.97
	ساخرة	13	4.30	14	4.78	27	4.54
	انفوجرافيك	22	7.28	23	7.85	45	7.56
الوسائط المتعددة	نص	302	100	293	100	595	100
	فيديو	49	16.23	46	15.70	105	17.65
	روابط	56	18.54	36	12.29	192	32.27
الإجمالي		302		293		595	

يتضح من الجدول: أن كلاً من بوابة الأهرام واليوم السابع قد اعتمدتا بشكل كبير على العناوين الرئيسية والصور الإخبارية كأبرز وسائل الإبراز في تناول الموضوعات العلمية والتكنولوجية خلال فترة الدراسة. حيث بلغت نسبة استخدام العناوين الرئيسية 100% في كلتا الصحيفتين، وهو ما يعكس أهمية العنوان كأداة لجذب القارئ الرقمي وإبراز المحتوى العلمي في ظل بيئة تنافسية تعتمد على سرعة التصفح، كما جاءت العناوين الثانوية بنسبة

40.40% في بوابة الأهرام مقابل 20.48% في اليوم السابع، ما يشير إلى اهتمام الأهرام بالشرح التوضيحي والتفصيلي في العنوان، بينما تميل اليوم السابع إلى الصياغة المكثفة والجاذبة.

وفيما يتعلق بالصور، فقد كانت الصور الإخبارية الأكثر استخدامًا بنسبة إجمالية بلغت 65.55%، تلتها الصور الموضوعية بنسبة 31.93%، ثم الصور الشخصية بنسبة 18.99%. وذلك يظهر ذلك أن معظم المواد العلمية المنشورة اعتمدت على صور واقعية مرتبطة بالحدث أو الظاهرة العلمية نفسها، بما يساهم في تعزيز مصداقية الخبر العلمي وتوضيح مضمونه بصريًا. أما الرسوم فقد جاءت التوضيحية في الصدارة بنسبة 15.97%، تلتها الانفوجرافيك بنسبة 7.56%، بينما كانت الرسوم الساخرة محدودة الاستخدام (4.54%)، وهو ما يعكس الطابع الجاد للموضوعات العلمية التي لا تناسب المعالجة الساخرة.

أما بالنسبة إلى الوسائط المتعددة، فقد أظهرت النتائج أن النصوص المكتوبة ظلت الوسيلة الأساسية بنسبة 100% في كلا الموقعين، تليها الفيديوهات بنسبة 17.65%، ثم الروابط التفاعلية بنسبة إجمالية بلغت 32.27%، وهو مؤشر على بدء توجه الصحف الرقمية المصرية نحو التفاعلية وتكامل الوسائط المتعددة، خاصة في الموضوعات التكنولوجية التي تستفيد من الشرح البصري والتفاعل مع المصادر الخارجية.

وتتفق هذه النتائج مع ما توصلت إليه دراسة (Elrefai, 2019) أن الصحافة الرقمية المصرية ما زالت تعتمد على النصوص والصور الإخبارية كوسائط رئيسية في عرض المحتوى العلمي، مع محدودية في توظيف الوسائط التفاعلية المتقدمة مثل الفيديوهات والإنفوجرافيك.

جدول (3) أنواع الجرائم السيبرانية التي تعالجها الصحف

الصحف / الجرائم السيبرانية	بوابة الأهرام		اليوم السابع		الإجمالي	
	ك	%	ك	%	ك	%
الاختراقات	48	15.89	57	19.45	105	17.65
الاحتيال الإلكتروني	42	13.91	46	15.70	88	14.79
سرقة الهوية الرقمية	30	9.93	28	9.56	85	9.75
الفيروست والبرمجيات الخبيثة	28	9.27	23	7.85	51	8.57
الابتزاز الالكتروني	34	11.26	31	10.58	56	10.92
التنمر الالكتروني	22	7.28	25	8.53	47	7.90
التجسس الالكتروني	26	8.61	20	6.82	46	7.73
جرائم الألعاب الإلكترونية	18	5.96	22	7.51	40	6.72
التزوير الالكتروني	16	5.30	17	8.50	33	5.55
الهجمات على البنية التحتية	18	5.96	14	4.78	32	5.38
الإجمالي	302	100	293	100	595	100

يتضح من نتائج الجدول: أن بوابة الأهرام واليوم السابع توليان اهتمامًا متزايدًا بتغطية قضايا الجرائم السيبرانية، وهو ما يعكس تصاعد وعي الإعلام المصري بأهمية الأمن الرقمي في ظل التحول التكنولوجي المتسارع. بلغ إجمالي المواد الصحفية التي تناولت الجرائم السيبرانية خلال الفترة من أكتوبر 2024 إلى سبتمبر 2025 نحو 595 مادة، منها 302 مادة في بوابة الأهرام و293 مادة في اليوم السابع، بما يشير إلى تقارب واضح في حجم التغطية وتوازن في الاهتمام بين المؤسستين الصحفيتين.

حيث جاءت جرائم الاختراقات في المرتبة الأولى بنسبة 17.65٪، وهي النسبة الأعلى بين جميع الفئات، مما يدل على أن القضايا المرتبطة باختراق الحسابات أو المواقع أو المؤسسات الحكومية تستحوذ على اهتمام بارز من الصحف الرقمية المصرية. وتُفسَّر هذه النتيجة بأن أخبار الاختراقات ذات طابع حدثي سريع وجاذب للقراء، إضافة إلى توافر مصادرها الرسمية من بيانات أمنية وتقارير سيبرانية. وتميل بوابة الأهرام إلى تناول هذه القضايا من منظور تحليلي وتوعوي يركز على المؤسسات الحكومية، بينما تركز اليوم السابع على الطابع الخبري المباشر ونشر التفاصيل السريعة للحوادث.

أما جرائم الاحتيال الإلكتروني فقد احتلت المرتبة الثانية بنسبة 14.79٪، وهو ما يشير إلى اهتمام متزايد بالجرائم الرقمية ذات البعد الاقتصادي، مثل الاحتيال المالي، وانتحال هوية الشركات، والتعاملات الوهمية عبر الإنترنت. ويرتبط هذا الاهتمام بتوسع المعاملات الرقمية في المجتمع المصري، خاصة مع انتشار المحافظ الإلكترونية والدفع عبر التطبيقات البنكية. كما ركزت اليوم السابع على القصص الفردية والحوادث الواقعية للنصب الإلكتروني، في حين اهتمت بوابة الأهرام بنقل تحذيرات الجهات الرسمية والبنوك حول مخاطر الاحتيال الرقمي.

واحتلت قضايا الابتزاز الإلكتروني المرتبة الثالثة بنسبة 10.92٪ من إجمالي التغطية، وهو ما يعكس إدراكًا متزايدًا بخطورة هذه الظاهرة اجتماعيًا ونفسيًا، خاصة في الحالات التي تمس الأفراد وتؤثر على سمعتهم وحياتهم الشخصية. وجاءت معالجة بوابة الأهرام لتلك القضايا في إطار توعوي قانوني، بينما قدمت اليوم السابع نماذج واقعية تمس الجمهور بشكل مباشر.

أما الجرائم الأخرى مثل الفيروسات الرقمية، والتنمر الإلكتروني، والتجسس، وتزوير البيانات، فقد شكّلت مجتمعة ما بين 30 إلى 35٪ من إجمالي التغطية. وتكشف هذه النسبة عن اهتمام متزايد بالموضوعات التقنية، لكنها في الوقت ذاته تشير إلى أن التناول لا يزال يميل إلى السطحية الإخبارية أكثر من التحليل العلمي المتعمق. ويتضح أن بوابة الأهرام أكثر تنوعًا في معالجاتها لهذه الفئات، بينما تركز اليوم السابع على الجوانب الإنسانية المرتبطة بها. في المقابل، جاءت فئات مثل جرائم الألعاب الإلكترونية والهجمات على البنية التحتية الرقمية في أدنى المراتب بنسبة لا تتجاوز 6٪، نظرًا لندرة المعلومات حولها وصعوبتها الفنية بالنسبة للصحفيين.

وبوجه عام، تُظهر النتائج غلبة الطابع الإخباري السريع على التغطية التحليلية المعمقة، وغياب الاهتمام بالصحافة الاستقصائية في مجال الأمن السيبراني، مما يشير إلى أن التناول الصحفي لا يزال يعتمد على البيانات الرسمية أكثر من الدراسات التقنية المتخصصة. كما يعكس اختلاف أنماط المعالجة بين الصحيفتين تأثير طبيعة جمهورهما المستهدف؛ إذ تميل اليوم السابع إلى الأسلوب الشعبي السريع لجذب القارئ العام، بينما تحافظ بوابة الأهرام على طابعها الرسمي والمهني.

وتتفق نتائج الدراسة الحالية مع ما توصلت إليه دراسة (العسكري، 2024) التي أكدت أن الإعلام الرقمي العربي يركّز على النشر الإخباري المباشر في تناول قضايا الأمن السيبراني مع ضعف التحليل المتخصص، وتختلف النتائج الحالية عن ما أشارت إليه بعض الدراسات الأجنبية مثل (Jones & Scott. 2022) التي لاحظت في الإعلام الغربي اتجاها متزايدًا نحو التعمق في تحليل أسباب الجرائم السيبرانية ودوافعها التقنية. وبذلك يمكن القول إن الصحافة الرقمية المصرية، رغم اهتمامها المتنامي بقضايا الأمن السيبراني، لا تزال بحاجة إلى تطوير أدواتها المهنية والتقنية لتنتقل من مرحلة النقل الإخباري إلى المعالجة التحليلية المتخصصة.

جدول (4) الهدف من عرض قضايا الأمن السيبراني التي تعالجها الصحف

الصحف / الهدف من النشر	بوابة الأهرام		اليوم السابع		الإجمالي	
	ك	%	ك	%	ك	%
عرض الموضوع فقط	1.2	33.77	111	37.88	213	35.79
نشر الوعي المجتمعي بالأمن الرقمي	64	21.91	58	19.80	122	20.50
تعزيز الثقافة الأمنية لدى الجمهور	41	13.58	35	11.94	76	12.77
دعم جهود الدولة في مكافحة الجرائم الإلكترونية	56	18.54	49	16.72	105	17.64
تصحيح المفاهيم الخاطئة ومكافحة الشائعات الرقمية	24	7.95	27	9.22	51	8.57
توجيه الرأي العام نحو الاستخدام الأخلاقي للتكنولوجيا	15	4.97	13	4.44	28	4.70
الإجمالي	302	100	293	100	595	100

يتضح من الجدول: أن تغطية قضايا الأمن السيبراني في كلٍّ من بوابة الأهرام واليوم السابع اتسمت بتنوع في الأهداف الصحفية، إلا أن الغلبة كانت للطابع الإخباري المباشر، إذ جاءت فئة عرض الموضوع فقط في المرتبة الأولى بنسبة إجمالية بلغت نحو 35.79٪ من إجمالي المواد المنشورة. ويُشير ذلك إلى أن غالبية التغطيات تركز على نقل الحدث أو الواقعة كما هي، دون تعمق في التحليل أو تقديم محتوى توعوي أو تثقيفي للجمهور. ويرتبط هذا النمط بطبيعة الصحافة الرقمية المصرية التي تميل إلى السبق الإخباري وسرعة النشر لجذب المتابعين، كما أن حجم الموارد البشرية المتخصصة في الصحافة التقنية لا يزال محدودًا في المؤسسات الإعلامية المحلية.

أما هدف نشر الوعي المجتمعي بالأمن الرقمي فجاء في المرتبة الثانية بنسبة 20.50٪، وهو مؤشر إيجابي على بداية تطور في توجه الصحافة المصرية نحو أداء دورها التوعوي، خاصة في ظل تصاعد الجرائم الإلكترونية التي تمس الأفراد مباشرة مثل الاحتيال الإلكتروني أو الابتزاز، وقد تميزت بوابة الأهرام في هذه الفئة من خلال نشر مقالات وتقارير توعوية تستند إلى مصادر رسمية، بينما مالت اليوم السابع إلى تبسيط الرسائل التحذيرية عبر لغة إعلامية قريبة من الجمهور العام.

وجاء هدف تعزيز الثقافة الأمنية لدى الجمهور في المرتبة الثالثة بنسبة 12.77٪، وهي نسبة تُظهر اهتمامًا محدودًا بالجانب المعرفي والتثقيفي المتعمق، إذ تميل المواد إلى تبسيط المعلومات التقنية دون تحليل للسياسات أو تقديم حلول عملية، ويدل ذلك على أن الصحافة المصرية ما زالت في مرحلة أولية من تطوير صحافة الأمن السيبراني المتخصصة.

وفيما يتعلق بهدف دعم جهود الدولة في مكافحة الجرائم الإلكترونية، فقد بلغت نسبته الإجمالية 17.64٪، مما يعكس الدور المؤسسي للإعلام في دعم السياسات الحكومية وتعزيز الثقة في الأجهزة الأمنية. وتبدو بوابة الأهرام أكثر ميلًا لهذا التوجه بحكم طابعها الرسمي، مقارنة باليوم السابع التي تميل إلى الطابع الشعبي السريع.

أما هدف تصحيح المفاهيم الخاطئة ومكافحة الشائعات الرقمية فحقق نسبة 8.57٪، وهي نسبة متواضعة لكنها ذات دلالة، إذ تشير إلى إدراك متزايد لمشكلة الشائعات الرقمية ومخاطر التضليل الإعلامي. بينما جاءت فئة توجيه الرأي العام نحو الاستخدام الأخلاقي للتكنولوجيا في أدنى المراتب بنسبة 4.70٪، مما يكشف ضعف الاهتمام بالجوانب الأخلاقية والقيمية لاستخدام الإنترنت، على الرغم من أهميتها في الحد من الجرائم السيبرانية وسلوكيات الخطر الرقمي.

وتُظهر المقارنة بين الصحيفتين أن بوابة الأهرام تتفوق نسبيًا في الفئات ذات الطابع التوعوي أو المؤسسي مثل نشر الوعي ودعم جهود الدولة، بينما تبرز اليوم السابع في الفئات الإخبارية المباشرة. ويعكس هذا الفارق اختلاف الخط التحريري لكلا الموقعين، إذ تلتزم الأهرام بالمعالجة الرسمية والتحليلية، في حين تركز اليوم السابع على جذب القراء بالسرعة والعناوين المثيرة.

جدول (5) الأطر التي تستخدمها الصحف في معالجة قضايا الأمن السيبراني

الصحف / الأطر المستخدمة	بوابة الأهرام		اليوم السابع		الإجمالي	
	ك	%	ك	%	ك	%
إطار التهديد / الخطر	89	29.47	96	32.76	185	31.09
إطار المسئولية	56	18.54	44	15.02	100	16.81
إطار الحلول / الوقاية	49	16.23	41	13.99	90	15.13
إطار التوعية / التثقيف / التفسير	44	14.57	47	16.03	91	15.29
إطار الأخلاق / الخصوصية	23	7.62	25	8.53	48	8.07
الإطار الاقتصادي	21	6.95	18	6.14	39	6.55
الإطار الإنساني	13	4.30	15	5.12	28	4.71
الإطار النقدي	7	2.32	7	2.39	14	2.35
الإجمالي	302	100	293	100	595	100

يتضح من الجدول: أن إطار التهديد أو الخطر تصدّر الأطر المستخدمة بنسبة إجمالية بلغت 31.09٪ من إجمالي التغطيات، ما يدل على أن الصحافة الرقمية المصرية تميل إلى معالجة قضايا الأمن السيبراني من زاوية الخوف والتحذير والتركيز على المخاطر المحتملة مثل الاختراقات والهجمات الإلكترونية وفقدان البيانات. ويعكس ذلك اهتمامًا بتأثير هذه الجرائم على الأفراد والمؤسسات أكثر من تفسير أبعادها التقنية. وقد ظهر هذا الإطار بشكل أوضح في موقع اليوم السابع الذي يميل إلى الأسلوب العاطفي والمباشر في صياغة العناوين والأخبار.

وجاء إطار المسئولية في المرتبة الثانية بنسبة 16.81٪، وهو الإطار الذي يبرز الجهات المسئولة عن معالجة الظاهرة مثل الدولة أو المستخدمين أو المؤسسات التقنية. ويبدو أن بوابة الأهرام كانت أكثر استخدامًا لهذا الإطار مقارنة باليوم السابع، نتيجة لطابعها المؤسسي واعتمادها على البيانات الرسمية والتصريحات الحكومية.

أما إطار الحلول والوقاية فقد بلغ 15.13٪، وهو مؤشر إيجابي يعكس بعض الجهود الصحفية في تقديم نصائح وإجراءات للوقاية من الجرائم السيبرانية. وقد ركزت بعض المواد المنشورة على دور المستخدمين في تأمين حساباتهم، واستخدام كلمات مرور قوية، والتعامل الآمن مع الروابط والمواقع الإلكترونية.

بينما جاء إطار التوعية والتثقيف والتفسير قريبًا من النسبة السابقة (15.29٪) مما يدل على اهتمام متزايد بالبعد التعليمي والإرشادي في التغطية، خاصة في المقالات الطويلة والتقارير المتخصصة. ويبدو أن اليوم السابع أكثر ميلًا لاستخدام هذا الإطار من خلال لغة مبسطة ومباشرة تناسب جمهورها العام.

واحتلت الأطر ذات الطابع القيمي مثل إطار الأخلاق والخصوصية نسبة 8.07٪، ما يعكس إدراكًا محدودًا لأهمية الجوانب الأخلاقية والقانونية في التعامل مع الفضاء السيبراني. وقد تناولت بعض المواد قضايا مثل حماية البيانات الشخصية، والابتزاز الإلكتروني، ونشر الصور الخاصة، لكنها لا تزال في نطاق ضيق.

وجاء الإطار الاقتصادي بنسبة 6.55٪، وهو ما يشير إلى ضعف الاهتمام بتأثير الجرائم الإلكترونية على الاقتصاد الرقمي أو خسائر الشركات الناشئة، رغم أهمية هذا الجانب في الإعلام الاقتصادي العالمي. أما الإطار الإنساني فبلغ 4.71٪، وهو ما يعكس محدودية التناول الصحفي للجوانب النفسية والاجتماعية للضحايا، في حين جاء الإطار النقدي في أدنى المراتب بنسبة 2.35٪، وهو ما يدل على ضعف ممارسة الصحافة التحليلية أو النقدية في تقييم السياسات الحكومية أو أداء المؤسسات التكنولوجية

ويمكن القول في ضوء ما سبق إن الصحافة الرقمية المصرية بدأت في الانتقال التدريجي من خطاب الخطر والتحذير إلى خطاب الوقاية والتثقيف، لكنها لا تزال بحاجة إلى تعميق المعالجة النقدية والاقتصادية والإنسانية لتصبح أكثر شمولًا واحترافية في تناول قضايا الأمن السيبراني.

واتفقت نتائج لبحث الحالي مع ما توصلت إليه دراسة (الأزرق،2020) والتي أكدت أن التغطية الصحفية المصرية لقضايا الأمن السيبراني تميل إلى التركيز على إطار التهديد والخطر باعتباره أكثر الأطر استخدامًا في معالجة القضايا الرقمية، مع إهمال نسبي للأطر التوعوية والوقائية. هذا الاتفاق يظهر بوضوح في نتائج الجدول الذي أبرز تفوق إطار التهديد/الخطر على بقية الأطر في كلٍّ من بوابة الأهرام واليوم السابع، ما يعكس توجهًا إعلاميًا يقوم على إثارة الانتباه والتحذير أكثر من نشر المعرفة التقنية أو الوقائية.

كما اتفقت نتائج البحث أيضًا مع ما توصلت إليه دراسة (عثمان، 2025) والتي خلصت إلى أن الإعلام في كلٍّ من مصر والإمارات يعتمد بدرجة كبيرة على إطار المسؤولية في عرض الجرائم السيبرانية، حيث يتم توجيه اللوم إلى المؤسسات أو الأفراد أو الدولة عند وقوع الانتهاكات الرقمية، دون التركيز الكافي على الحلول الاستباقية أو الأطر الاقتصادية المرتبطة بالجرائم الإلكترونية.

في المقابل، اختلفت نتائج البحث الحالي مع دراسة (Rodríguez-Priego et al,2020) والتي أكدت أن الأطر المعرفية والتعليمية (مثل إطار التوعية والوقاية) هي الأكثر تأثيرًا في تعديل سلوك المستخدمين تجاه التهديدات الرقمية، ودعت إلى زيادة استخدامها في الإعلام الرقمي، أما في البحث الحالي، فقد ظهر أن هذه الأطر جاءت في مراتب تالية بعد إطار التهديد والمسؤولية، مما يعكس فجوة بين الممارسات الإعلامية المصرية والتوجهات البحثية الدولية التي تشجع على التثقيف والتوجيه بدلاً من التحذير وحده.

ثانياً: نتائج الدراسة الميدانية:

جدول (6) أهم الصحف التي تتابعها العينة

مدى الاستخدام / الصحف	دائما		أحيانا		نادراً	
	ك	%	ك	%	ك	%
بوابة الأهرام	60	14.2	150	35.5	212	50.2
اليوم السابع	190	45.0	150	35.5	82	19.4
المصري اليوم	110	29.1	180	42.7	132	31.3
الأخبار	55	13.0	140	32.2	227	53.8
الوطن	80	19.0	190	45.0	152	36.0
الجمهورية	40	9.5	110	26.1	272	64.5
جملة من سئلوا	422					

يتضح من نتائج الجدول: وجود تباين واضح في مدى استخدام الصحف الإلكترونية المصرية بين أفراد العينة. فقد جاءت صحيفة اليوم السابع في المقدمة من حيث الاستخدام الدائم بنسبة 45%، مما يعكس انتشارها الكبير واعتماد الجمهور عليها كمصدر أساسي للأخبار. تلتها المصري اليوم بنسبة 26.1% ثم الوطن بنسبة 19%، وهو ما يدل على أن هذه الصحف الثلاث تحظى بمستوى عالٍ من الاهتمام والمتابعة سواء بشكل دائم أو متقطع.

أما بالنسبة للصحف القومية، فقد أظهرت النتائج أن بوابة الأهرام تُستخدم نادراً من قبل أكثر من نصف المستجيبين بنسبة 50.2%، في حين بلغت نسبة الاستخدام النادر لصحيفة الأخبار حوالي 53.8%، وارتفعت إلى 64.5% في صحيفة الجمهورية، وهي النسبة الأعلى ضمن فئة «نادراً». هذا يعكس زيادة الإقبال على الصحف الخاصة الإلكترونية مقارنة بالصحف القومية، وربما يعود ذلك إلى اهتمام متزايد من الصحف الخاصة بالتفاعل مع الجمهور.

وبشكل عام، يوضح الجدول أن الاتجاه العام للمبحوثين يميل نحو متابعة الصحف الخاصة والمستقلة مثل اليوم السابع والمصري اليوم والوطن، التي تتسم بسرعة النشر وتنوع المحتوى وجاذبية العرض. في المقابل، تراجعت معدلات الاستخدام للصحف القومية التقليدية، مما يعكس تحولاً في سلوك القراء نحو المنصات الإعلامية الرقمية الأكثر تفاعلاً ومواكبة للأحداث.

جدول (7) أهم الطرق التي تستخدمها العينة للوصول للصحف التي تتابعها

العينة / الطرق	ك	%
الدخول على موقع الصحيفة مباشرة	170	40.3
متابعة حسابات الصحيفة على الشبكات الاجتماعية	130	30.8
استخدام تطبيق الصحيفة	95	22.5
الاشتراك في النشرات البريدية الإلكترونية	27	6.4
الإجمالي	422	100

يتضح من نتائج الجدول: إلى أن أكثر طرق الوصول استخدامًا هي الدخول مباشرة إلى موقع الصحيفة الإلكتروني، حيث بلغت نسبة من يفعلون ذلك دائمًا 40.3%، وهو ما يعكس ثقة المستخدمين بالموقع الرسمي ورغبتهم في الحصول على الأخبار من مصدرها الأصلي دون وسائط. وجاءت متابعة الحسابات على وسائل التواصل الاجتماعي في المرتبة الثانية بنسبة 30.8%، مما يدل على أن شريحة كبيرة من الجمهور تفضل متابعة الأخبار عبر المنصات الاجتماعية لسهولة الوصول وسرعة التحديث.

أما استخدام تطبيقات الصحف فقد احتل المرتبة الثالثة بنسبة 22.5%، وهو ما يشير إلى أن التطبيقات أقل انتشارًا من المواقع المباشرة، ربما بسبب عدم توفرها لجميع الصحف أو محدودية استخدامها من قبل بعض الفئات. في المقابل، جاءت النشرات البريدية الإلكترونية في المرتبة الأخيرة بنسبة 6.4%، ما يدل على أنها أقل الطرق شيوعًا، وقد يعود ذلك إلى تغير أنماط استهلاك الأخبار واعتماد المستخدمين على الوسائط الفورية والتفاعلية بدلاً من البريد الإلكتروني.

جدول (8) أهم الموضوعات العلمية التي تتابعها العينة في الصحف الإلكترونية

العينة / الطرق	ك	%
الذكاء الاصطناعي وتطبيقاته	145	34.36
الأمن السيبراني	105	24.88
التحول الرقمي	80	18.96
الفضاء والأبحاث الفلكية	45	10.66
الابتكارات العلمية	32	7.58
التكنولوجيا والإقتصاد	15	3.55
الإجمالي	422	100

يتضح من نتائج الجدول: أن الموضوع الأكثر متابعة من قبل العينة هو الذكاء الاصطناعي وتطبيقاته بنسبة 34.36%، ما يعكس الاهتمام المتزايد بالتقنيات الحديثة ودورها في تشكيل مستقبل الحياة والعمل والتعليم. كما يظهر أن الأمن السيبراني يحتل المرتبة الثانية بنسبة 24.88%، وهو ما يشير إلى وعي متنامٍ بين القراء بأهمية حماية المعلومات والبيانات في ظل التحول الرقمي المتسارع.

وجاء في المرتبة الثالثة موضوع التحول الرقمي بنسبة 18.96%، مما يدل على اهتمام متزايد بعمليات الرقمنة في المؤسسات والخدمات. بينما تراجع الاهتمام نسبيًا بموضوعات الفضاء والأبحاث الفلكية (10.66%) والابتكارات العلمية (7.58%)، لتأتي التكنولوجيا والاقتصاد في المرتبة الأخيرة بنسبة 3.55%، ما يشير إلى أن الجمهور يميل إلى متابعة الموضوعات التقنية المباشرة المرتبطة بالحياة اليومية أكثر من القضايا العلمية البحتة أو الاقتصادية المعقدة.

ويتضح من النتائج أن العينة تُظهر ميولاً واضحة نحو متابعة الموضوعات التقنية المعاصرة مثل الذكاء الاصطناعي والأمن السيبراني، لما تمثله من قضايا راهنة تؤثر في الواقع العملي والمستقبلي. بينما تقل متابعة الموضوعات العلمية التقليدية أو الأكاديمية، مما يعكس تغير أولويات القراء نحو القضايا التطبيقية والتكنولوجية التي تمس حياتهم اليومية وتواكب التحول الرقمي العالمي.

جدول (9) أهم قضايا الأمن السيبراني التي تتابعها العينة في الصحف الإلكترونية

العينة / أهم القضايا	ك	%
الاحتيال الإلكتروني	90	21.33
الاختراقات	78	18.47
سرقة الهوية الرقمية	47	11.14
الابتزاز الالكتروني	45	10.66
الفيروست والبرمجيات الخبيثة	40	9.48
التجسس الالكتروني	34	8.06
التنمر الالكتروني	32	7.59
جرائم الألعاب الإلكترونية	18	4.27
التزوير الالكتروني	20	4.74
الهجمات على البنية التحتية	18	4.27
الإجمالي	422	100

يتضح من نتائج الجدول: أن الاحتيال الإلكتروني يأتي في المرتبة الأولى بين القضايا التي تحظى بمتابعة دائمة من أفراد العينة بنسبة 90%، وهو ما يعكس ارتفاع الوعي بخطورة الجرائم المالية الإلكترونية وتأثيرها المباشر على الأفراد والمؤسسات. تليه الاختراقات بنسبة 78%، ما يدل على اهتمام واسع بموضوع حماية الحسابات والأنظمة الرقمية من التسلل غير المشروع.

كما جاءت سرقة الهوية الرقمية (47%) والابتزاز الإلكتروني (45%) في مراتب متوسطة من الاهتمام، مما يشير إلى إدراك متزايد لمخاطر استغلال البيانات الشخصية عبر الإنترنت. في المقابل، أبدى المبحوثون اهتماماً أقل بقضايا مثل التنمر الإلكتروني، التزوير الإلكتروني، وجرائم الألعاب الإلكترونية، وهي موضوعات غالباً ما تمس فئات عمرية محددة أو حالات فردية أكثر من كونها قضايا عامة. أما الهجمات على البنية التحتية الرقمية (18%)، فجاءت في أدنى المراتب، ربما بسبب بعدها عن التجربة المباشرة للمستخدم العادي.

وتوضح النتائج أن اهتمام الجمهور بقضايا الأمن السيبراني يتركز على الجرائم التي تمس الأفراد مباشرة مثل الاحتيال الإلكتروني والاختراقات وسرقة الهوية، في حين يقل الاهتمام بالقضايا ذات الطابع المؤسسي أو التقني البحت مثل الهجمات على البنية التحتية. ويُظهر ذلك أن الوعي بالأمن الرقمي لدى المستخدمين يرتبط أكثر بحماية الذات والمعاملات الشخصية، ما يعكس الحاجة إلى تعزيز الثقافة الأمنية الرقمية في المجتمع بشكل أشمل.

جدول (10) مدى ثقة العينة في محتوى قضايا الأمن السيبراني المنشور في الصحف الإلكترونية

مدى الثقة / القضايا	ك	%
أثق بدرجة متوسطة	185	43.84
أثق بدرجة كبيرة	120	28.44
أثق بدرجة قليلة	65	15.40
لا أثق فيها مطلقاً	30	7.11
لا أستطيع التحديد	22	5.21
الإجمالي	422	100

يتضح من نتائج الجدول: أن الثقة المتوسطة هي الاتجاه الغالب بين أفراد العينة تجاه محتوى قضايا الأمن السيبراني المنشور في الصحف الإلكترونية، حيث بلغت نسبتها 43.84%. وهذا يعني أن معظم القراء لديهم ثقة نسبية مشروطة بالمحتوى، قد تعتمد على طبيعة المصدر أو مستوى التحقق من المعلومات المنشورة. كما أبدى 28.44% من الأفراد ثقة كبيرة، ما يدل على وجود شريحة معتبرة ترى أن الصحف الإلكترونية تقدم تغطية موثوقة نسبياً في هذا المجال.

في المقابل، عبّر 15.4% فقط عن ثقة قليلة، و7.11% عن عدم ثقة مطلقاً، مما يشير إلى أن نسبة محدودة من القراء تشك في دقة أو حيادية هذه التغطيات. أما فئة «لا أستطيع التحديد» (5.21%) فقد تمثل أولئك الذين ليست لديهم معرفة كافية لتقييم مصداقية المحتوى المتعلق بالأمن السيبراني.

يتضح من النتائج أن غالبية أفراد العينة يثقون بدرجات متفاوتة في المحتوى المنشور عن قضايا الأمن السيبراني في الصحف الإلكترونية، مع ميل واضح نحو الثقة المتوسطة. وهذا يعكس وجود مستوى مقبول من المصداقية لدى هذه المنصات، لكنه يشير أيضاً إلى الحاجة لتعزيز الدقة، والتحقق من المعلومات التقنية، والاستعانة بالخبراء المتخصصين لرفع مستوى الثقة العامة في هذا النوع من المحتوى.

جدول (11) الأطر التي تستخدمها الصحف في تغطية قضايا الأمن السيبراني

الأطر المستخدمة / الأطر	ك	%
إطار التهديد / الخطر	110	26.07
إطار الحلول / الوقاية	85	20.14
إطار المسئولية	75	17.77
إطار التوعية / التثقيف / التفسير	70	16.59
إطار الأخلاق / الخصوصية	35	8.29
الإطار الاقتصادي	20	4.74
الإطار الإنساني	15	3.55
الإطار النقدي	12	2.84
الإجمالي	422	100

يتضح من نتائج الجدول: أن الصحف الإلكترونية تميل في تناولها لقضايا الأمن السيبراني إلى استخدام مجموعة من الأطر الإعلامية التي تحدد زاوية المعالجة وطريقة عرض المعلومات. وقد أظهرت النتائج أن إطار التهديد والخطر جاء في المرتبة الأولى بنسبة 26.07%، وهو ما يعكس اعتماد الصحف بشكل واضح على إبراز الطابع التحذيري لهذه القضايا، من خلال التركيز على المخاطر التي قد يتعرض لها الأفراد أو المؤسسات نتيجة الاختراقات، أو الهجمات الإلكترونية، أو تسريب البيانات. هذا النمط من التغطية يسعى إلى لفت انتباه الجمهور وإثارة وعيه بالخطر، لكنه في الوقت نفسه قد يغلب عليه الطابع التخويفي إذا لم يُوازن بطرح بدائل أو حلول واقعية.

أما إطار الحلول والوقاية فقد جاء في المرتبة الثانية بنسبة 20.14%، وهو إطار إيجابي نسبيًا يركز على سبل الحماية والتدابير الوقائية من الجرائم الإلكترونية، مثل استخدام أنظمة الحماية والتشفير والتوعية بأساليب الأمن الرقمي. ويليه إطار المسؤولية بنسبة 17.77%، الذي يظهر في التغطيات التي تسلط الضوء على دور المؤسسات الحكومية أو الجهات الأمنية أو المستخدمين أنفسهم في مواجهة التهديدات السيبرانية، مما يعكس محاولة الصحف توزيع المسؤولية بين مختلف الأطراف المعنية بالأمن الرقمي.

كما احتل إطار التوعية والتثقيف والتفسير نسبة 16.59%، وهو ما يشير إلى جهود بعض الصحف في تقديم محتوى يهدف إلى رفع الوعي المجتمعي وفهم المفاهيم التقنية المرتبطة بالأمن السيبراني بلغة مبسطة. في المقابل، جاءت الأطر الأخرى مثل إطار الأخلاق والخصوصية (8.29%) والإطار الاقتصادي (4.74%) والإطار الإنساني (3.55%) والإطار النقدي (2.84%) بنسب منخفضة، ما يدل على ضعف الاهتمام بالجوانب الأخلاقية والاجتماعية والاقتصادية والنقدية المتعلقة بالقضايا السيبرانية، رغم أهميتها في بناء رؤية متكاملة حول الأمن الرقمي.

وبشكل عام، تعكس هذه النتائج أن التناول الصحفي لقضايا الأمن السيبراني يتركز بدرجة أكبر على جوانب الخطر والتحذير، في حين يقل الاهتمام بالأبعاد التوعوية والتحليلية والإنسانية التي تساعد القارئ على فهم أعمق لطبيعة هذه القضايا. وهذا يشير إلى حاجة الصحف إلى تنويع أطر التغطية الإعلامية بما يوازن بين التحذير من المخاطر وتقديم التفسيرات العلمية والحلول العملية التي تسهم في بناء وعي مجتمعي مستدام بالأمن السيبراني.

تتفق نتائج البحث الحالي مع ما توصلت إليه دراسة (Meissner, F., Buse, C., & Wilke, A, 2024)، التي أشارت إلى أن التغطية الإعلامية لقضايا الأمن السيبراني تميل إلى إبراز إطار التهديد والخطر بوصفه الإطار الأكثر حضوراً في تناول هذه القضايا، بينما تحظى الأطر الأخرى مثل الحلول والوقاية أو المسؤولية الاجتماعية بتمثيل أقل نسبيًا. ويؤكد هذا الاتفاق أن وسائل الإعلام، سواء في السياق العربي أو الدولي، تركّز في معالجتها للأمن السيبراني على الجانب التحذيري والمخاطر المحتملة أكثر من اهتمامها بتقديم مضامين تثقيفية أو توعوية تُسهم في رفع الوعي العام وتعزيز سلوكيات الحماية الرقمية لدى الجمهور.

جدول (12) يوضح تقييم استجابات العينة الكلية على مقياس التهديدات الرقمية

أبعاد / عبارات المقياس	محايد		معارض		موافق		المتوسط المرجح	النسبة	مستوى الادراك
	ك	%	ك	%	ك	%			
التهديدات الأمنية السيبرانية	342	81.0	53	12.5	27	6.5	2.45	81.00	مرتفع
الخصوصية وحماية البيانات	315	74.5	63	15.0	44	10.5	2.24	74.45	متوسط
التأثير الخارجي والرقمي	312	73.9	73	17.2	37	8.9	2.23	74.44	متوسط
البعد النفسي والاجتماعي	318	75.4	60	14.3	44	10.3	2.23	74.83	متوسط
البعد التنظيمي والقانوني	321	76.0	55	13.1	46	10.9	2.26	75.22	متوسط
التهديدات المتعلقة بالمعلومات والأخبار المضللة	300	71.2	69	16.4	53	12.4	2.16	72.94	منخفض
إجمالي المقياس	342	75.3	373	14.8	249	9.9	2.26	75.84	متوسط

يتضح من نتائج الجدول: يتضح من بيانات الجدول أن مستوى إدراك أفراد العينة للتهديدات الرقمية جاء متوسط بوجهٍ عام، حيث بلغ المتوسط المرجّح الكلي (2.26) بنسبة اتفاق بلغت (75.84%)، وهو ما يعكس وعيًا متناميًا لدى المشاركين بطبيعة المخاطر التي تفرضها البيئة الرقمية وأبعادها المختلفة. وتشير هذه النتيجة إلى أن أفراد العينة لديهم إدراك جيد لطبيعة التهديدات المرتبطة بالأمن السيبراني، والخصوصية، وحماية البيانات، والجوانب القانونية والنفسية والاجتماعية المرتبطة بالاستخدامات الرقمية.

وقد احتل بُعد التهديدات الأمنية السيبرانية المرتبة الأولى بمتوسط مرجّح (2.45) ونسبة اتفاق (81.00%)، وهو ما يشير إلى إدراك مرتفع جدًا لمخاطر الاختراقات، وسرقة البيانات، والهجمات الإلكترونية بمختلف أنواعها. وتُعزى هذه النتيجة إلى زيادة تداول قضايا الأمن السيبراني في وسائل الإعلام، وارتفاع معدلات الحوادث الرقمية التي أسهمت في رفع الوعي العام بمخاطر الفضاء السيبراني.

وجاءت أبعاد الخصوصية وحماية البيانات، والتأثير الخارجي والرقمي، والبعد النفسي والاجتماعي، والبعد التنظيمي والقانوني في مراتب متقاربة من حيث مستوى الإدراك، حيث تراوحت نسب الاتفاق فيها بين (74%–75%)، بما يعكس اتفاقًا عامًا على أن التهديدات الرقمية لا تقتصر على الجانب التقني فحسب، بل تمتد لتشمل أبعادًا أخلاقية وقانونية واجتماعية تمس حياة المستخدمين اليومية وسلوكهم الرقمي. وتشير هذه النتائج إلى وعي الأفراد بأهمية التشريعات المنظمة لاستخدام التقنية وحماية الحقوق الرقمية للمستخدمين.

أما بُعد التهديدات المتعلقة بالمعلومات والأخبار المضللة فقد جاء في المرتبة الأخيرة بنسبة اتفاق (72.94%) وبمتوسط مرجّح (2.16)، وهو ما يدل على أن الوعي بخطر المعلومات

الزائفة والتضليل الإعلاي لا يزال متوسطًا يميل إلى الارتفاع. وربما يُعزى ذلك إلى أن بعض الأفراد لا يدركون حجم التأثير الذي يمكن أن تحدثه الأخبار المضللة على الرأي العام، أو إلى ضعف مهارات التحقق الرقمي لدى المستخدمين العاديين مقارنةً بالإدراك العام للتهديدات التقنية المباشرة.

وعند النظر إلى نتائج الجدول بشكل عام، يتضح أن فئة «موافق» شكّلت النسبة الغالبة في معظم الأبعاد، ما يؤكد وجود اتجاه عام بين أفراد العينة نحو الإقرار بوجود تهديدات رقمية متعددة الأبعاد تمس حياتهم الرقمية والمجتمعية. كما أن انخفاض نسب «المعارضين» يعكس درجة توافق مرتفعة بين أفراد العينة حول طبيعة هذه التهديدات وضرورة مواجهتها بوعي ومسؤولية.

وبناءً على ما سبق، يمكن القول إن إدراك أفراد العينة للتهديدات الرقمية جاء متوسط، وهو ما يشير إلى أن جهود التوعية المجتمعية والإعلامية والسياسات التنظيمية قد أسهمت في بناء وعي جيد لدى المستخدمين. ومع ذلك، تبرز الحاجة إلى تعزيز الوعي بقضايا التضليل الإعلاي والمعلومات الزائفة بوصفها أحد أبرز أشكال التهديدات الرقمية في العصر الحديث، مما يستدعي تطوير برامج للتربية الإعلامية الرقمية تركز على مهارات التحقق والتمييز بين المصادر الموثوقة والمحتوى المضلل، وفيما يلي تفصيل استجابات العينة على عبارات المقياس بكل بعد:

جدول (12- أ) يوضح تقييم استجابات العينة على مقياس التهديدات الرقمية (التهديدات الأمنية السيبرانية)

أبعاد / عبارات المقياس	محايد		معارض		موافق		المتوسط المرجح	النسبة
	ك	%	ك	%	ك	%		
ضعف الوعي الأمني يزيد من احتمالية الاختراق	45	10.66	20	4.74	357	84.60	2.75	91.67
سرقة البيانات تشكل خطرًا كبيرًا على أمن المعلومات	40	9.48	25	5.92	357	84.60	2.75	91.67
المؤسسات والأفراد عرضة دائمًا للهجمات الإلكترونية	55	13.03	35	8.29	332	78.68	2.66	88.67
برامج الحماية الحالية تكفي لتجنب المخاطر الإلكترونية	100	23.70	180	42.65	142	33.65	2.10	70.00
المبالغة في الحديث عن الهجمات الرقمية غير مبررة	60	14.22	130	54.50	132	31.28	1.90	63.33
من النادر أن يتأثر المستخدمون بالاختراقات الرقمية	70	16.59	270	63.98	82	19.43	1.55	51.67
إجمالي البعد (ن= 422)							2.45	81.00

يتضح من نتائج الجدول: أن أفراد العينة لديهم إدراك مرتفع بمستوى التهديدات السيبرانية التي تواجه الأفراد والمؤسسات، حيث جاءت أعلى المتوسطات المرجحة عند عبارتي سرقة البيانات تشكل خطرًا كبيرًا على أمن المعلومات وضعف الوعي الأمني يزيد من احتمالية الاختراق، إذ حصلتا على متوسط مرجح بلغ (2.75) بنسبة اتفاق مرتفعة بلغت (91.67٪)، ما يعكس وعياً واضحاً لدى المبحوثين بخطورة سرقة البيانات وأهمية الوعي الأمني كعامل حاسم في الوقاية من الهجمات. كما أظهرت النتائج أن (78.68٪) من المشاركين يوافقون على أن المؤسسات والأفراد عرضة دائمًا للهجمات الإلكترونية، وهو ما يبرز إدراكاً عاماً بأن التهديدات الرقمية أصبحت واقعية ومتكررة.

وفي المقابل، جاءت عبارات مثل من النادر أن يتأثر المستخدمون بالاختراقات الرقمية والمبالغة في الحديث عن الهجمات الرقمية غير مبررة وبرامج الحماية الحالية تكفي لتجنب المخاطر الإلكترونية بتقديرات منخفضة ومتوسطات مرجحة تراوحت بين (1.55–2.10)، ما يشير إلى رفض غالبية العينة للتقليل من خطورة التهديدات أو المبالغة في الثقة ببرامج الحماية التقليدية. هذا يعني أن المشاركين يدركون أن الأمن السيبراني يتجاوز الحلول التقنية إلى تبني سلوكيات واعية وإجراءات مستمرة للوقاية.

وبشكل عام، يعكس المتوسط الكلي (2.45) بنسبة اتفاق إجمالية (81٪) اتجاهاً إيجابياً مرتفعاً نحو الإقرار بوجود تهديدات رقمية جدية ومستمرة. ويمكن تفسير هذه النتيجة بأن التغطيات الإعلامية والممارسات اليومية للأفراد في بيئة رقمية متزايدة التعقيد قد ساهمت في تعزيز هذا الوعي، مع بقاء الحاجة إلى مزيد من التوعية المتخصصة حول الوقاية والممارسات الآمنة على الإنترنت.

جدول (12 - ب) يوضح تقييم استجابات العينة على مقياس التهديدات الرقمية (التهديدات المتعلقة بالمعلومات والأخبار المضللة)

أبعاد / عبارات المقياس	محايد		معارض		موافق		المتوسط المرجح	النسبة
	ك	%	ك	%	ك	%		
الأخبار الكاذبة عبر الإنترنت تهدد ثقة الناس بالإعلام	70	١٦،٥٩	260	61.61	92	21.80	1.55	51.67
الشائعات الرقمية لا تؤثر كثيرًا على الجمهور	60	١٤،٢٢	38	8.29	327	77.49	2.63	87.67
الصور والفيديوهات المفبركة تغيّر طريقة فهمي للأحداث	90	٢١،٣٣	240	56.78	92	٢١،٨٠	1.66	55.33
من السهل دائمًا التمييز بين الأخبار الصحيحة والمزيفة	45	١٠،٦٦	22	5.21	355	٨٤،١٣	2.74	91.33
الحملات المنظمة للتضليل الرقمي أصبحت تهديدًا خطيرًا	80	١٨،٩٦	250	59.24	92	٢١،٨٠	1.62	54.00
تأثير الأخبار المضللة على الناس محدود جدًا	70	١٦،٥٩	260	61.61	92	٢١،٨٠	1.55	51.67
إجمالي البعد (ن= 422)							2.16	72.94

يتضح من نتائج الجدول: أن المتعلق بتقييم استجابات العينة حول مقياس التهديدات الرقمية المرتبطة بالمعلومات والأخبار المضللة إلى أن المشاركين يُظهرون وعياً متوسطاً يميل إلى الارتفاع بخطورة التضليل الإعلامي في البيئة الرقمية. فقد أظهرت البيانات أن أعلى العبارات اتفاقًا كانت «من السهل دائمًا التمييز بين الأخبار الصحيحة والمزيفة» بمتوسط مرجح (2.74) ونسبة (91.33٪)، ما يشير إلى ثقة نسبية لدى الأفراد بقدرتهم الذاتية على التمييز بين الحقيقة والتزييف، رغم أن هذا الإدراك قد لا يعكس بالضرورة كفاءة فعلية في التعامل مع التضليل الرقمي المعقّد. كما جاءت عبارة «الشائعات الرقمية لا تؤثر كثيراً على الجمهور» بمتوسط مرتفع (2.63) ونسبة (87.67٪)، ما قد يُفسَّر على أن بعض الأفراد يقللون من حجم التأثير النفسي والاجتماعي للشائعات الإلكترونية رغم انتشارها.

وفي المقابل، جاءت عبارات مثل: الأخبار الكاذبة عبر الإنترنت تهدد ثقة الناس بالإعلام وتأثير الأخبار المضللة على الناس محدود جداً والصور والفيديوهات المفبركة تغيّر طريقة فهمي للأحداث بمتوسطات منخفضة تراوحت بين (1.55–1.66)، مما يُظهر أن غالبية المشاركين يدركون أن الأخبار الزائفة تمثل تهديداً حقيقياً لثقة الجمهور ومصداقية الإعلام، حتى وإن لم يقرّوا بذلك بشكل مباشر في تقييماتهم الإيجابية. كما أن عبارة «الحملات المنظمة للتضليل الرقمي أصبحت تهديداً خطيراً» حصلت على متوسط (1.62) فقط، مما يشير إلى ضعف الإحساس بخطورة التضليل الممنهج مقارنة بالتهديدات التقنية أو الأمنية المباشرة.

وعند النظر إلى المتوسط الكلي (2.16) بنسبة اتفاق إجمالية (72.94٪)، يتضح أن العينة تمتلك وعياً متوسطاً بمخاطر التضليل الرقمي، إلا أن هذا الوعي يتسم بالتباين بين الثقة الذاتية في التمييز من جهة، والاستخفاف الجزئي بخطورة الأخبار المضللة المنظمة من جهة أخرى. وهذا يعكس الحاجة إلى تعزيز التربية الإعلامية والوعي المعلوماتي لدى الجمهور، بما يُمكّنهم من تحليل مصادر الأخبار واكتشاف التزييف العميق والمحتوى المضلل، خاصة في ظل تزايد الحملات الرقمية التي تستهدف التأثير على الرأي العام.

جدول (12-ج) يوضح تقييم استجابات العينة على مقياس التهديدات الرقمية (الخصوصية وحماية البيانات)

أبعاد / عبارات المقياس	محايد		معارض		موافق		المتوسط المرجح	النسبة
	ك	%	ك	%	ك	%		
مشاركة المعلومات الشخصية على الإنترنت تعرضني للمخاطر	45	10.66	30	7.11	347	82.23	2.72	90.67
نادرًا ما يتعرض الأفراد لابتزاز رقمي بسبب بياناتهم	70	16.59	260	61.61	92	21.80	1.55	51.67
اختراق الحسابات يسبب أضرارًا جسيمة لصاحبها	50	11.85	25	5.92	347	82.23	2.70	90.00
خدمات التخزين السحابي دائمًا آمنة وموثوقة	90	21.33	210	49.76	122	28.91	1.83	61.00
تسريب بيانات الأفراد يمثل تهديدًا حقيقيًا لهم	40	9.48	20	4.74	362	85.78	2.76	92.00
سياسات الخصوصية الحالية في التطبيقات تكفي لحماية المستخدمين	75	17.77	230	54.50	117	27.73	1.90	63.33
إجمالي البعد (ن= 422)							2.24	74.45

يتضح من نتائج الجدول: أن أفراد العينة يتمتعون بدرجة وعي مرتفعة نسبياً بمخاطر انتهاك الخصوصية وتسريب البيانات الشخصية عبر الإنترنت، وهو ما يتضح من ارتفاع المتوسطات المرجحة ونسب الموافقة على أغلب العبارات ذات الصلة. فقد جاءت أعلى الاستجابات عند عبارة تسريب بيانات الأفراد يمثل تهديدًا حقيقيًا لهم بمتوسط (2.76) ونسبة (92.00٪)، تلتها عبارة مشاركة المعلومات الشخصية على الإنترنت تعرضني للمخاطر بمتوسط (2.72) ونسبة (90.67٪)، مما يعكس إدراكاً عالياً لدى المشاركين بخطورة الكشف عن البيانات الشخصية على المنصات الرقمية، ووعيهم بأن حماية الخصوصية تمثل أحد أهم أبعاد الأمن السيبراني.

كما حصلت عبارة «اختراق الحسابات يسبب أضرارًا جسيمة لصاحبها» على متوسط مرتفع بلغ (2.70) ونسبة (90.00٪)، وهو ما يشير إلى إدراك واضح لتبعات الاختراق الرقمي على المستويين الشخصي والاجتماعي، خاصة في ظل تزايد حالات سرقة الحسابات واستغلالها في الابتزاز أو التشهير. في المقابل، جاءت عبارات مثل نادرًا ما يتعرض الأفراد لابتزاز رقمي بسبب بياناتهم وخدمات التخزين السحابي دائمًا آمنة وموثوقة وسياسات الخصوصية الحالية في التطبيقات تكفي لحماية المستخدمين بمتوسطات منخفضة تراوحت بين (1.55–1.90)، مما يعكس رفضاً واسعاً بين أفراد العينة لفكرة الاطمئنان المفرط للتقنيات أو السياسات الحالية، وإدراكاً بأن الضمانات المقدمة من الشركات التقنية ليست كافية لحماية المستخدمين بشكل كامل.

وبوجه عام، يُظهر المتوسط الكلي للمقياس (2.24) بنسبة اتفاق (74.45٪) أن لدى العينة مستوى وعياً جيداً بمخاطر الخصوصية الرقمية، وأنهم يدركون بوضوح العلاقة بين ممارسات الاستخدام الشخصي مثل مشاركة البيانات أو الاعتماد على الخدمات السحابية، وبين احتمالية التعرض للابتزاز أو تسريب المعلومات. وتشير هذه النتائج إلى أن قضايا الخصوصية تمثل محوراً رئيسياً في تصورات الجمهور حول الأمن السيبراني، ما يستلزم من المؤسسات الإعلامية تعزيز التوعية بسلوكيات الحماية الرقمية وتبني سياسات تواصل فعّالة تشرح للمستخدمين سبل الوقاية من هذه التهديدات المتنامية.

جدول (12-د) يوضح تقييم استجابات العينة على مقياس التهديدات الرقمية (التأثير الخارجي والرقمي)

أبعاد / عبارات المقياس	محايد		معارض		موافق		المتوسط المرجح	النسبة
	ك	%	ك	%	ك	%		
التدخلات الأجنبية عبر الإنترنت تؤثر على الإعلام والمجتمع	45	10.66	28	6.64	349	82.70	2.72	90.67
الحملات الرقمية الموجهة نادرًا ما تغيّر قناعات الجمهور	50	11.85	30	7.11	342	81.04	2.69	89.67
الحملات الممولة عبر وسائل التواصل تؤثر على الرأي العام	55	13.03	35	8.29	332	78.68	2.65	88.33
التلاعب بالترندات الرقمية لا يغيّر طريقة متابعتي للأحداث	70	16.59	240	56.78	112	26.54	1.90	63.33
القوى الناعمة الرقمية تُستخدم للتأثير غير المباشر على المجتمع	85	20.14	230	54.50	107	25.36	1.80	60.00
الوصول إلى المنصات الرقمية متاح دائمًا ولا يحد من حرية التعبير	65	15.40	255	60.43	102	24.17	1.64	54.67
إجمالي البعد (ن= 422)							2.23	74.44

يتضح من نتائج الجدول: أن أفراد العينة يُدركون بدرجة مرتفعة خطر التأثيرات الخارجية والحملات الرقمية الموجهة على الإعلام والمجتمع، حيث أظهرت العبارات ذات العلاقة بهذا البعد نسب اتفاق عالية ومتوسطات مرجحة مرتفعة. فقد جاءت عبارة التدخلات الأجنبية عبر الإنترنت تؤثر على الإعلام والمجتمع في المرتبة الأولى بمتوسط (2.72) ونسبة اتفاق بلغت (90.67٪)، وهو ما يعكس وعياً واسعاً بأن الفضاء الرقمي أصبح مجالاً تستخدمه بعض القوى الخارجية للتأثير على السياسات الداخلية وتشكيل الرأي العام. كما تلتها عبارة الحملات الرقمية الموجهة نادراً ما تغيّر قناعات الجمهور بمتوسط (2.69) ونسبة (89.67٪)، مما يدل على إدراك واضح بأن هذه الحملات قادرة على تغيير المواقف والاتجاهات المجتمعية وإن كان بعض الأفراد لا يعترفون بتأثرهم المباشر بها.

أما عبارة «الحملات الممولة عبر وسائل التواصل تؤثر على الرأي العام» فقد جاءت في المرتبة الثالثة بمتوسط (2.65) ونسبة (88.33٪)، ما يؤكد اقتناع المشاركين بأن الإعلانات الموجهة والمحتوى المدفوع عبر المنصات الرقمية يشكل أداة ضغط فعالة في تشكيل المواقف السياسية والاجتماعية. في المقابل، أظهرت العبارات الثلاث الأخيرة التلاعب بالترندات الرقمية لا يغيّر طريقة متابعتي للأحداث، القوى الناعمة الرقمية تُستخدم للتأثير غير المباشر على المجتمع، والوصول إلى المنصات الرقمية متاح دائمًا ولا يحد من حرية التعبير متوسطات أقل تراوحت بين (1.64–1.90)، مما يعكس وعياً محدوداً ببعض أشكال التأثير غير المباشر مثل القوة الناعمة الرقمية أو السيطرة على التوجهات الرائجة (الترندات)، وهي أدوات أكثر خفاءً وتأثيراً على المدى الطويل.

وعموماً، يُظهر المتوسط الكلي (2.23) بنسبة اتفاق إجمالية (74.44٪) أن العينة تدرك بدرجة مرتفعة نسبياً وجود تهديدات رقمية خارجية تؤثر في الإعلام والرأي العام، لكنها قد لا تميز بدقة بين أشكال هذا التأثير المباشر وغير المباشر. وتشير هذه النتائج إلى أهمية تعزيز الثقافة الرقمية والإعلامية لدى الجمهور، ولا سيما في ما يتعلق بفهم آليات الحملات الموجهة، والدعاية الرقمية، ودور الخوارزميات في توجيه المضمون الإعلامي، بما يسهم في تكوين جمهور أكثر وعياً وقدرة على مقاومة التلاعب بالمعلومات.

جدول (12- ه) يوضح تقييم استجابات العينة على مقياس التهديدات الرقمية (البعد النفسي والاجتماعي)

أبعاد / عبارات المقياس	محايد		معارض		موافق		المتوسط المرجح	النسبة
	ك	%	ك	%	ك	%		
التهديدات الرقمية تثير القلق والخوف لدى المستخدمين	45	10.66	30	7.11	347	82.23	2.72	90.67
لا أشعر بأي قلق من المراقبة أو الاختراق	60	14.22	255	60.43	107	25.36	1.65	55.00
الهجمات الإلكترونية تؤدي إلى فقدان الثقة في الآخرين	55	13.03	35	8.29	332	78.68	2.65	88.33
التهديدات الرقمية لا تؤثر على استقراري النفسي	70	16.59	240	56.87	112	26.54	1.80	60.00
الشعور بعدم الأمان الرقمي يقلل من استخدامي للتقنيات الحديثة	50	11.85	40	9.48	332	78.68	2.67	89.00
لا أرى أن التهديدات الرقمية تسبب أي ضغط اجتماعي	75	17.77	220	52.13	127	30.10	1.86	62.00
إجمالي البعد (ن=422)							2.23	74.83

يتضح من نتائج الجدول: أن أفراد العينة يُدركون بدرجة مرتفعة نسبياً الآثار النفسية والاجتماعية السلبية للتهديدات الرقمية، خصوصاً تلك المرتبطة بالقلق، وفقدان الثقة، والشعور بعدم الأمان في البيئة الافتراضية. فقد جاءت عبارة التهديدات الرقمية تثير القلق والخوف لدى المستخدمين في المرتبة الأولى بمتوسط (2.72) ونسبة اتفاق (90.67٪)، مما يعكس حالة قلق عام بين المستخدمين تجاه احتمالات الاختراق والمراقبة والتعرض للهجمات الإلكترونية. كما أظهرت النتائج أن عبارة الهجمات الإلكترونية تؤدي إلى فقدان الثقة في الآخرين جاءت في المرتبة الثانية بمتوسط (2.65) ونسبة (88.33٪)، وهو ما يشير إلى أن الخوف من الاستغلال الرقمي أو تسريب المعلومات الشخصية يقلل من مستوى الثقة الاجتماعية بين الأفراد في البيئات الإلكترونية.

كذلك أظهرت عبارة الشعور بعدم الأمان الرقمي يقلل من استخداي للتقنيات الحديثة متوسطاً مرتفعاً بلغ (2.67) ونسبة (89.00٪)، ما يدل على أن الإحساس المستمر بالمخاطر قد يحدّ من انخراط المستخدمين في استخدام التطبيقات والمنصات الحديثة، وهو ما يُمثل أثراً نفسياً مباشراً ينعكس على السلوك الرقمي للفرد. في المقابل، حصلت العبارات ذات الاتجاه المعاكس مثل لا أشعر بأي قلق من المراقبة أو الاختراق والتهديدات الرقمية لا تؤثر على استقراري النفسي ولا أرى أن التهديدات الرقمية تسبب أي ضغط اجتماعي على متوسطات منخفضة تراوحت بين (1.65–1.86)، ما يدل على رفض غالبية العينة لهذه التصورات المطمئنة، وتأكيدهم على وجود تأثير نفسي واجتماعي واضح لتلك التهديدات.

وعند النظر إلى المتوسط الكلي للمقياس (2.23) بنسبة اتفاق إجمالية (74.83٪)، يتضح أن لدى العينة وعياً عالياً نسبياً بأن التهديدات الرقمية لا تقتصر على الأبعاد التقنية فقط، بل تمتد لتشمل تأثيرات نفسية واجتماعية عميقة مثل الخوف، القلق، العزلة، وفقدان الثقة في العلاقات الرقمية. وتشير هذه النتائج إلى أهمية دمج البعد النفسي والاجتماعي في استراتيجيات التوعية بالأمن السيبراني، بما يساعد على تعزيز الشعور بالأمان الرقمي، وبناء الثقة في الاستخدام الآمن للتكنولوجيا دون تضخيم المخاوف أو التقليل من المخاطر الفعلية.

جدول 12- و) يوضح تقييم استجابات العينة على مقياس التهديدات الرقمية (البعد التنظيمي والقانوني)

أبعاد / عبارات المقياس	محايد		معارض		موافق		المتوسط المرجح	النسبة
	ك	%	ك	%	ك	%		
القوانين الحالية غير كافية لمواجهة الجرائم الإلكترونية	70	16.59	250	59.24	102	24.17	1.67	55.67
توجد حماية قانونية قوية تحمي الأفراد من التهديدات الرقمية	45	10.66	30	7.11	347	82.23	2.72	90.67
ضعف التشريعات يعرض المستخدمين لمزيد من المخاطر الرقمية	65	15.40	230	54.50	127	30.10	1.85	61.67
المؤسسات الرسمية توفر دائمًا الحماية الكافية من الهجمات الرقمية	40	9.48	25	5.92	357	84.60	2.75	91.67
غياب التشريعات الصارمة يزيد من جرائم الإنترنت.	75	17.77	220	52.13	127	30.10	1.87	62.33
ثقتي في النظام القانوني كافية لردع أي تهديد رقمي	70	16.59	250	59.24	102	24.17	1.67	55.67
إجمالي البعد (ن= 422)							2.26	75.22

يتضح من نتائج الجدول: أن أفراد العينة يُظهرون وعياً متوسطاً يميل إلى الارتفاع تجاه أهمية التشريعات والقوانين في الحد من الجرائم الإلكترونية، مع وجود تباين في درجة ثقتهم بفاعلية تلك التشريعات والمؤسسات الرسمية في الحماية الرقمية. فقد جاءت عبارة «المؤسسات الرسمية توفر دائمًا الحماية الكافية من الهجمات الرقمية» في المرتبة الأولى بمتوسط (2.75) ونسبة اتفاق (91.67٪)، ما يشير إلى إيمان شريحة كبيرة من المشاركين بقدرة المؤسسات الرسمية على التصدي للتهديدات الإلكترونية، أو على الأقل اعتقادهم بوجود دور تنظيمي فاعل للدولة في هذا المجال. كما جاءت عبارة توجد حماية قانونية قوية تحمي الأفراد من التهديدات الرقمية في المرتبة الثانية بمتوسط (2.72) ونسبة (90.67٪)، مما يعكس ثقة نسبية في الإطار القانوني العام المنظّم للأمن السيبراني.

وفي المقابل جاءت بعض العبارات مثل القوانين الحالية غير كافية لمواجهة الجرائم الإلكترونية وثقتي في النظام القانوني كافية لردع أي تهديد رقمي بمتوسط منخفض (1.67)، ما يدل على وجود شك أو تردد لدى جزء من العينة حيال كفاءة الإطار القانوني والتنفيذي، وربما إدراكهم لوجود فجوات في التطبيق أو بطء في تحديث القوانين بما يتناسب مع تطور التهديدات الرقمية، كما سجلت عبارة ضعف التشريعات يعرض المستخدمين لمزيد من المخاطر الرقمية وغياب التشريعات الصارمة يزيد من جرائم الإنترنت متوسطات معتدلة (1.85–1.87)، ما يعكس وعياً بأن ضعف التشريعات يمثل عامل خطر، لكنه ليس الوحيد في زيادة معدلات الجريمة الإلكترونية.

وبوجه عام يشير المتوسط الكلي للمقياس (2.26) بنسبة اتفاق إجمالية (75.22٪) إلى أن لدى العينة ثقة جزئية في الإطار التنظيمي والقانوني للأمن السيبراني، مقرونة بإدراك أن بعض الجوانب ما زالت تحتاج إلى تطوير، خصوصاً في مجالات تطبيق القوانين، تحديث التشريعات، ورفع كفاءة أجهزة إنفاذ القانون في التعامل مع الجرائم الرقمية المعقدة. وتبرز هذه النتائج الحاجة إلى تعزيز الشفافية القانونية والتعاون المؤسسي بين الهيئات الحكومية وشركات التقنية، مع تكثيف حملات التوعية القانونية للمستخدمين لضمان حماية فعّالة للحقوق الرقمية في المجتمع.

وتُظهر نتائج الدراسة الخاصة بمقياس التهديدات الرقمية عبر أبعاده أن أفراد العينة يتمتعون بمستوى وعي مرتفع نسبيًا تجاه المخاطر الرقمية بمختلف صورها، سواء التقنية أو الاجتماعية أو القانونية، فقد أظهر البعد الأمني السيبراني أن المشاركين يدركون خطورة الاختراقات وسرقة البيانات وضعف الوعي الأمني كأكثر مظاهر التهديد شيوعًا، حيث بلغت نسبة الاتفاق نحو (81٪)، مما يعكس إدراكًا واضحًا لأهمية الوقاية الرقمية. أما بعد المعلومات والأخبار المضللة فقد كشف عن قلق متزايد من تأثير الشائعات والمحتوى المزيف على ثقة الجمهور بالإعلام، بنسبة وعي بلغت (72.9٪)، مما يشير إلى إدراك المستخدمين لتأثير الحملات التضليلية في تشكيل الرأي العام.

وفي بعد الخصوصية وحماية البيانات، أظهرت النتائج أعلى مستوى وعي (74.45٪)، إذ أكد أغلب المشاركين أن تسريب البيانات ومشاركة المعلومات الشخصية يمثلان تهديدًا حقيقيًا، مع شكوك واضحة في فعالية سياسات الخصوصية الحالية. كما بيّنت نتائج البعد المتعلق بالتأثير الخارجي والرقمي أن المشاركين يُدركون خطورة التدخلات الرقمية والحملات الموجهة التي تؤثر على الإعلام والمجتمع بنسبة (74.44٪)، ما يعكس فهماً لدور القوى الناعمة الرقمية في تشكيل الوعي العام.

أما البعد النفسي والاجتماعي فأظهر أن التهديدات الرقمية تترك آثارًا نفسية واضحة كالقلق والخوف وفقدان الثقة الرقمية بنسبة (74.83٪)، مما يؤكد امتداد التهديدات إلى الجانب الإنساني والاجتماعي للمستخدم. وأخيرًا، في البعد التنظيمي والقانوني عبّر المشاركون عن ثقة نسبية في دور القوانين والمؤسسات الرسمية بنسبة (75.22٪)، مع إدراك لحاجة هذه المنظومات إلى مزيد من التطوير والتحديث.

وبشكل عام، توضح النتائج أن التهديدات الرقمية تُشكل ظاهرة متعددة الأبعاد، تتجاوز الإطار التقني لتشمل الجوانب القانونية، النفسية، والاجتماعية، مما يستدعي استراتيجية شاملة لتعزيز الوعي الرقمي، وتطوير التشريعات، وتكثيف جهود التثقيف المجتمعي لضمان أمن رقمي متوازن ومستدام.

ثالثاً: نتائج اختبار فروض الدراسة

الفرض الأول: توجد علاقة ذات دلالة إحصائية بين تبني النخب للأطر في معالجة قضايا الأمن السيبراني وادراكهم لمستويات التهديدات الرقمية

جدول (13) نتائج اختبار الارتباط بين أطر معالجة الصحف الرقمية لقضايا الأمن السيبراني وادراك النخب الإعلامية للتهديدات الرقمية (Pearson's r)

المتغير	المتوسط الحسابي	الانحراف المعياري	معامل الارتباط (r)	مستوى الدلالة (Sig)
درجة تبني النخب لأطر معالجة قضايا الأمن السيبراني	2.41	0.56	0.782	0.000
إدراك النخب الإعلامية للتهديدات الرقمية	2.37	0.52		

يتضح من الجدول: أن قيمة معامل الارتباط بيرسون (r = 0.782) بين متغيري **درجة تبني النخب لأطر معالجة قضايا الأمن السيبراني** وإدراكهم للتهديدات الرقمية تُعد قيمة موجبة مرتفعة، مما يدل على وجود علاقة ارتباط قوية طردية بين المتغيرين؛ أي أنه كلما زاد تبني النخب للأطر الصحفية في قضايا الأمن السيبراني، ازداد إدراك النخب الإعلامية لطبيعة التهديدات الرقمية ومستويات خطورتها. كما يُظهر الجدول أن مستوى الدلالة (Sig = 0.000) أقل من (0.05)، ما يعني أن العلاقة ذات دلالة إحصائية عالية ويمكن الاعتماد عليها علميًا.

وتشير هذه النتيجة إلى تحقق الفرض الأول القائل بوجود علاقة ذات دلالة إحصائية بين المتغيرين، حيث تبين أن طريقة تبني النخب للقضايا الأمنية — من خلال الأطر المختلفة مثل إطار التهديد، المسؤولية، الوقاية، أو التوعية — تسهم بشكل مباشر في رفع مستوى وعي النخب الإعلامية وفهمهم لطبيعة التهديدات الرقمية وأبعادها التقنية والاجتماعية والقانونية.

ويمكن تفسير ذلك في ضوء نظرية التأطير الإعلامي (Framing Theory) التي تفترض أن طريقة عرض الموضوعات في وسائل الإعلام تؤثر في إدراك الجمهور لها وتشكيل آرائهم حولها. وبناءً على هذه النتيجة، يمكن القول إن الصحف الرقمية تمارس دورًا مؤثرًا في تشكيل الإدراك الإعلامي تجاه قضايا الأمن السيبراني، وأن زيادة جودة وتنوع الأطر المستخدمة في تغطية هذه القضايا يمكن أن تساهم في تعزيز الوعي الرقمي والثقافة الأمنية لدى النخب الإعلامية والمجتمع بشكل عام.

ويمكن تفسير نتائج الفرض الأول في ضوء نظرية الاتصال بالمخاطر (Risk Communication Theory)، التي تؤكد أن طريقة نقل المعلومات المتعلقة بالمخاطر وتفسيرها عبر وسائل الإعلام تؤثر بشكل مباشر في إدراك الأفراد وتفاعلهم مع تلك المخاطر. وتشير النظرية إلى أن الجمهور — بما في ذلك النخب الإعلامية — لا يكتفي باستقبال المعلومات، بل يقوم ببناء تصورات ذهنية حول درجة التهديد وسبل مواجهته بناءً على كيفية عرض الإعلام للمشكلة، ولغة الخطاب، ونوعية الأطر المستخدمة.

في ضوء ذلك، يمكن تفسير الارتباط الإيجابي القوي الذي أظهره التحليل الإحصائي (r = 0.782, Sig = 0.000) **درجة تبني النخب لأطر معالجة قضايا الأمن السيبراني** وإدراكهم للتهديدات الرقمية على أنه دليل على فاعلية الاتصال الإعلامي في إدارة وتوجيه الوعي بالمخاطر الرقمية. إذ أن الصحف الرقمية التي تُبرز أطرًا مثل التهديد والخطر، والمسؤولية، والحلول، والتوعية تسهم في رفع إدراك النخب الإعلامية لمستوى التهديد، وتوضيح أبعاده التقنية والاجتماعية والقانونية، مما يؤدي إلى تعامل أكثر وعياً ومسؤولية مع هذه القضايا.

كما توضح نظرية الاتصال بالمخاطر أن فعالية الرسائل الإعلامية تعتمد على الوضوح، والشفافية، وتوازن الطرح بين التهديد والحلول، وهو ما يعكسه المتوسط المرتفع لمتغير أطر المعالجة (2.41)، ما يدل على أن تغطية الصحف الرقمية لقضايا الأمن السيبراني تتسم بدرجة من الجدية والمصداقية تجعلها قادرة على التأثير في وعي النخب الإعلامية.

وبذلك، تُظهر نتائج الدراسة أن الصحافة الرقمية من خلال توظيفها الواعي لأطر التأطير المرتبطة بالمخاطر تقوم بدور مهم في نقل المعرفة الفنية المعقدة حول الأمن السيبراني إلى الجمهور المتخصص بلغة مفهومة ومؤثرة. وهذا يتفق مع جوهر نظرية الاتصال بالمخاطر التي ترى أن الإعلام ليس مجرد ناقل للمعلومات، بل هو وسيط أساسي في بناء التصورات العامة وتشكيل الاستجابة الاجتماعية للمخاطر.

الفرض الثاني: توجد فروق ذات دلالة إحصائية بين النخب الإعلامية عينة الدراسة فيما يتعلق بحجم اهتماماتهم بقضايا الأمن السيبراني حسب المتغيرات الديموجرافية (النوع ونوع النخب)

جدول (14) نتائج اختبار t للفروق بين النخب الإعلامية عينة الدراسة في استخدامهم للصحف الرقمية لمتابعة قضايا الأمن السيبراني حسب المتغيرات الديموجرافية (النوع ونوع النخب)

المتغير	الفئة	العدد	المتوسط الحسابي	الانحراف المعياري	درجة (ت)	مستوى الدلالة
النوع	ذكور	210	2.48	0.55	**4.32	دال عند0.001
	اناث	212	2.25	0.49		
نوع النخب	أكاديمين	198	2.52	0.53	**3.97	دال عند0.001
	ممارسين	224	2.31	0.51		

يتضح من نتائج الجدول: وجود فروق ذات دلالة إحصائية بين أفراد عينة الدراسة من النخب الإعلامية في حجم اهتمامهم بقضايا الأمن السيبراني، وفقًا لمتغيري النوع (ذكور/إناث) ونوع النخبة (أكاديميون/ممارسون)، وذلك عند مستوى دلالة (Sig = 0.001)، مما يعني أن هذه الفروق حقيقية وليست ناتجة عن الصدفة الإحصائية.

فبالنسبة إلى النوع، بلغ المتوسط الحسابي لاستخدام الذكور (2.48) مقابل (2.25) للإناث، وبقيمة (ت = 4.32**) دالة إحصائيًا، ما يشير إلى أن الذكور أكثر استخدامًا للصحف الرقمية في متابعة قضايا الأمن السيبراني مقارنة بالإناث. ويمكن تفسير ذلك في ضوء أن الذكور غالبًا ما يُظهرون اهتمامًا أكبر بالقضايا التقنية والأمنية، أو أن طبيعة عملهم الإعلامي تتطلب اطلاعًا أوسع على المستجدات الرقمية. كما يمكن أن يعكس هذا الفارق فجوة رقمية نسبية بين الجنسين في مجالات التقنية والأمن المعلوماتي.

أما فيما يتعلق بـ نوع النخبة، فقد أظهر الأكاديميون متوسطًا حسابيًا أعلى (2.52) مقارنة بالممارسين (2.31)، مع وجود فرق دال إحصائيًا (ت = 3.97**). وهذا يشير إلى أن الأكاديميين أكثر اهتمامًا بمتابعة القضايا السيبرانية، ربما بحكم تخصصهم البحثي واهتمامهم بالتحليل العلمي والمنهجي لهذه الظواهر، في حين يميل الممارسون إلى التركيز على الجوانب التطبيقية والمهنية اليومية.

وبناءً على ذلك، يمكن القول إن الفرض الثاني قد تحقق فعلاً، إذ ثبت وجود فروق ذات دلالة إحصائية بين النخب الإعلامية تبعًا للنوع ونوع النخبة. وتُظهر هذه النتائج أن العوامل الديموغرافية تسهم في تفسير أنماط السلوك الإعلامي الرقمي، وأن مستوى الانخراط في متابعة قضايا الأمن السيبراني يتأثر بدرجة التخصص الأكاديمي والاهتمام المهني، إلى جانب الفروق بين الجنسين في الاهتمامات والممارسات الرقمية.

الفرض الثالث: توجد فروق ذات دلالة إحصائية بين النخب الإعلامية عينة الدراسة فيما يتعلق بمستوى إدراكهم للتهديدات الرقمية حسب المتغيرات الديموجرافية.

جدول (15) نتائج اختبار t للفروق بين النخب الإعلامية عينة الدراسة فيما يتعلق بمستوى إدراكهم للتهديدات الرقمية حسب المتغيرات الديموجرافية (النوع ونوع النخب)

المتغير	الفئة	العدد	المتوسط الحسابي	الانحراف المعياري	درجة (ت)	مستوى الدلالة
النوع	ذكور	210	2.47	0.54	4.18**	دال عند 0.001
	اناث	212	2.26	0.50		
نوع النخب	أكاديمين	198	2.53	0.52	3.84**	دال عند 0.001
	ممارسين	224	2.33	0.49		

يتضح من نتائج الجدول: وجود فروق ذات دلالة إحصائية عند مستوى (0.001) بين متوسطات استجابات أفراد العينة تبعًا لمتغيري النوع ونوع النخب الإعلامية، حيث سجّل الذكور متوسطًا حسابيًا أعلى (2.47) مقارنة بالإناث (2.26)، كما حقق الأكاديميون متوسطًا أعلى

(2.53) من الممارسين (2.33). وتشير هذه النتائج إلى أن الذكور يمتلكون إدراكًا أكبر لقضايا الأمن السيبراني، وهو ما قد يُعزى إلى انخراطهم الأكثر في استخدام التكنولوجيا والأدوات الرقمية ذات الطابع الأمني، إضافةً إلى مشاركتهم الأوسع في المجالات التقنية والمعلوماتية.

وتبين كذلك أن الأكاديميين أظهروا مستوى أعلى من الوعي والقدرة على تحليل قضايا الأمن السيبراني مقارنة بالممارسين، وهو ما يتسق مع طبيعة دورهم العلمي والمعرفي الذي يتيح لهم الاطلاع المستمر على المستجدات البحثية والتشريعات الرقمية ذات الصلة. في المقابل، يميل الممارسون إلى التعامل مع الظواهر الرقمية من زاوية عملية دون التعمق في أبعادها النظرية أو القانونية، مما يفسر انخفاض متوسط إدراكهم النسبي.

الفرض الرابع: توجد علاقة ذات دلالة إحصائية بين معدل ثقة النخب في معالجة الصحف لقضايا الأمن السيبراني ومستوى ادراكهم للتهديدات الرقمية.

جدول (16) نتائج اختبار الارتباط بين معدل ثقة النخب في معالجة الصحف لقضايا الأمن السيبراني ومستوى ادراكهم للتهديدات الرقمية (Pearson's r)

المتغير	المتوسط الحسابي	الانحراف المعياري	معامل الارتباط (r)	مستوى الدلالة (Sig)
معدل ثقة النخب في معالجة قضايا الأمن السيبراني	2.44	0.58	0.692	0.000
إدراك النخب الإعلامية للتهديدات الرقمية	2.39	0.55		

يتضح من نتائج الجدول: وجود علاقة ارتباطية قوية وموجبة بين معدل ثقة النخب الإعلامية في معالجة الصحف لقضايا الأمن السيبراني ومستوى إدراكهم للتهديدات الرقمية، حيث بلغ معامل الارتباط ($r = 0.692$) وهو دال إحصائياً عند مستوى دلالة ($Sig = 0.000$)، مما يعني أن العلاقة ليست عشوائية بل ذات دلالة معنوية قوية، وهذا يدل على أن زيادة ثقة النخب في أداء الصحف بمجال الأمن السيبراني يرتبط بارتفاع مستوى إدراكهم للتهديدات الرقمية.

كما يظهر من المتوسطات الحسابية أن معدل ثقة النخب في معالجة الصحف لقضايا الأمن السيبراني كان متوسطاً نسبياً (المتوسط = 2.44، والانحراف المعياري = 0.58)، في حين كان مستوى إدراكهم للتهديدات الرقمية قريباً منه (المتوسط = 2.39، والانحراف المعياري = 0.55). وتشير هذه القيم إلى أن النخب الإعلامية تمتلك درجة متوسطة من الثقة والوعي، ما يعكس إدراكاً متنامياً لأهمية التناول الصحفي لقضايا الأمن السيبراني في تشكيل وعيهم بالمخاطر الرقمية.

ويمكن تفسير هذه العلاقة بأن التغطيات الصحفية المتعمقة والمهنية لقضايا الأمن السيبراني تسهم في تعزيز وعي النخب بخطورة التهديدات الرقمية، من خلال ما توفره من معلومات وتحليلات ومتابعة مستمرة للحوادث والأخطار السيبرانية. وبالتالي، فإن الصحف التي تتسم بالموثوقية والمصداقية في تناول هذه القضايا ترفع من مستوى الثقة لدى النخب، وتدفعهم إلى تكوين إدراك أكثر وعياً واستبصاراً بالتهديدات الرقمية التي تواجه الأفراد والمؤسسات والمجتمع.

مناقشة النتائج وخاتمة البحث:

تُظهر نتائج الدراسة التحليلية والميدانية صورة شاملة لطبيعة معالجة الصحف الرقمية لقضايا الأمن السيبراني، وكيفية إدراك النخب الإعلامية لتلك التهديدات الرقمية المتنامية، في سياق بيئة إعلامية سريعة التغير ومتأثرة بالتحول الرقمي المتسارع. فقد تناولت الدراسة بُعدين متكاملين: الأول تحليلي يركّز على تحليل أطر التغطية الإعلامية لقضايا الأمن السيبراني في الصحف الرقمية المصرية، والثاني ميداني يقيس إدراك النخب الإعلامية لهذه القضايا وسلوكهم الاتصالي تجاهها، وقد أظهرت نتائج البعدين معاً أن العلاقة ليست علاقة نقل معلومات فحسب، بل هي علاقة اتصالية تفاعلية يتأثر فيها وعي الجمهور وطريقة إدراكه لطبيعة المخاطر تبعاً للأسلوب الإعلامي المستخدم في عرض تلك القضايا.

فبالنسبة للجانب التحليلي أوضحت نتائج الدراسة أن الصحف الرقمية المصرية تعتمد في تغطيتها لقضايا الأمن السيبراني على مجموعة من الأطر الإعلامية المتنوعة، إلا أن إطار التهديد والخطر كان الأكثر حضورًا بنسبة بلغت نحو (26.07٪)، يليه إطار الحلول والوقاية بنسبة (20.14٪)، ثم إطار المسؤولية بنسبة (17.77٪)، في حين جاء إطار التوعية والتثقيف بنسبة (16.59٪)، ويُستدل من ذلك أن الصحف الرقمية تميل إلى إبراز الجانب التحذيري والدرامي في معالجة قضايا الأمن السيبراني، من خلال التركيز على المخاطر والاختراقات والتهديدات الإلكترونية، أكثر من اهتمامها بطرح الأطر التوعوية أو التفسيرية التي تشرح للقارئ طبيعة الخطر وسبل التعامل معه، ويرتبط هذا النمط ارتباطاً وثيقاً بنظرية الأطر الإعلامية التي ترى أن وسائل الإعلام لا تخبر الجمهور بما يفكر فيه فحسب، بل تُحدّد أيضًا كيفية تفكيره في القضية، فالتركيز المفرط على الخطر يجعل المتلقي يُدرك الأمن السيبراني كتهديد دائم ومصدر خوف، بينما التركيز على الحلول يخلق شعورًا بالتمكّن والسيطرة على الموقف. ومن ثم، فإن غلبة إطار التهديد في التغطية المصرية يعكس خطابًا إعلاميًا تحذيريًا أكثر منه تثقيفيًا، رغم أهمية البعد المعرفي في بناء ثقافة أمن رقمي مستدامة.

كما أظهرت نتائج الدراسة الميدانية أن الصحف الرقمية الأكثر استخدامًا بين أفراد العينة كانت «اليوم السابع» بنسبة (45٪)، تليها «المصري اليوم» بنسبة (26.1٪)، ثم «بوابة الأهرام» بنسبة (14.2٪). وتُظهر هذه النتائج أن النخب الإعلامية تميل إلى متابعة المنصات الرقمية ذات الإيقاع الإخباري السريع والتفاعل اللحظي، وهو ما يعكس تغير أنماط الاستهلاك الإعلامي

نحو المصادر الإلكترونية المتجددة بدلاً من الوسائل التقليدية. كذلك، أوضحت البيانات أن أغلب المشاركين يدخلون مباشرة إلى مواقع الصحف (40.3٪)، بينما يعتمد 30.8٪ منهم على متابعة الحسابات الرسمية للصحف عبر وسائل التواصل الاجتماعي، ما يدل على أن الجمهور الإعلامي يفضل الوصول المباشر إلى المصدر الموثوق بدلاً من الاعتماد على قنوات وسيطة.

وفيما يتعلق بالموضوعات العلمية التي تحظى بمتابعة دائمة من النخب الإعلامية، برزت موضوعات الذكاء الاصطناعي وتطبيقاته في المقدمة بنسبة (34.36٪)، تليها موضوعات الأمن السيبراني بنسبة (24.88٪)، ثم التحول الرقمي والفضاء والأبحاث الفلكية. وتدل هذه النتائج على أن النخب الإعلامية تُظهر اهتمامًا متزايدًا بالقضايا التقنية والعلمية التي تمس مستقبل العمل الإعلامي ذاته، حيث يشكل الأمن السيبراني أحد أهم التحديات في بيئة الإعلام الرقمي المعاصر. ويبدو أن هذا الاهتمام يعكس وعيًا متناميًا بضرورة حماية البيانات والخصوصية في العمل الإعلامي.

أما من حيث القضايا السيبرانية التي يتابعها أفراد العينة في الصحف الرقمية، فقد تبين أن الاحتيال الإلكتروني جاء في المرتبة الأولى بنسبة متابعة بلغت (90٪)، يليه الاختراقات (78٪)، ثم سرقة الهوية الرقمية (47٪)، وهو ما يشير إلى أن النخب الإعلامية تميل إلى متابعة القضايا التي تمس الأفراد والمستخدمين مباشرة، مثل الاحتيال عبر الإنترنت أو اختراق الحسابات الشخصية، أكثر من اهتمامها بالقضايا المؤسسية الكبرى مثل الهجمات على البنية التحتية أو الجرائم المنظمة عبر الإنترنت. ويدل ذلك على أن الإدراك الإعلامي للتهديدات الرقمية لا يزال موجهاً نحو المستوى الفردي أكثر من المستوى الاستراتيجي، ما يعكس الحاجة إلى تعزيز الفهم الجماعي لمخاطر الأمن السيبراني بوصفه قضية وطنية تتجاوز الأفراد إلى المؤسسات والمجتمع ككل.

ويمكن القول إن الصحف الرقمية المصرية تؤدي دورًا فاعلًا في تشكيل إدراك النخب الإعلامية للأمن السيبراني من خلال طريقة عرضها للقضايا، فمجيء إطار التهديد والخطر في الترتيب الأول جعلت الرسائل الإعلامية تحمل طابعاً تحذيرياً يثير القلق والخوف، وهو ما يرفع الوعي الإدراكي بالمشكلة لكنه لا يدعم بالضرورة الفهم العميق أو السلوك الوقائي، فالنخب الإعلامية أصبحت تدرك أن الأمن السيبراني قضية ملحة، لكنها في الوقت نفسه تميل إلى الشعور بأن المخاطر أكبر من القدرة على السيطرة عليها، هذه النتيجة تتفق مع ما تؤكده نظرية الأطر من أن الإعلام لا ينقل الواقع كما هو، بل يبني له سياقاً إدراكياً يؤثر على تصور الجمهور له.

وفيما يخص الثقة في المحتوى المنشور حول قضايا الأمن السيبراني، أظهرت النتائج أن (43.84٪) من العينة يثقون بدرجة متوسطة، و(28.44٪) بدرجة كبيرة، في حين أعربت نسبة محدودة (7.11٪) عن انعدام الثقة، ويدل ذلك على أن النخب الإعلامية تمتلك وعياً نقدياً في تعاملها مع محتوى الصحف الرقمية، فهي تثق في المعلومات لكنها تدرك احتمال وجود مبالغات أو نقص في التفسير. ويمكن تفسير هذه النتيجة في ضوء مفهوم الثقة الإعلامية ضمن نظرية الاتصال بالمخاطر، إذ أن الاتصال الفعال حول القضايا المعقدة يتطلب درجة عالية من المصداقية والشفافية، وكلما كانت المعلومات المقدمة متوازنة وموثقة زادت ثقة الجمهور.

كما أظهرت النتائج أن إدراك النخب الإعلامية للتهديدات الرقمية كان مرتفعًا في جميع الأبعاد الستة التي تناولها مقياس الدراسة فقد حقق البعد الأمني السيبراني أعلى نسبة (81٪)، ما يدل على إدراك قوي لخطورة الهجمات الإلكترونية وسرقة البيانات وضعف الوعي الأمني كمصدر رئيسي للمخاطر، بينما جاء بعد الخصوصية وحماية البيانات بنسبة (74.45٪) مع إدراك واضح لمخاطر تسريب المعلومات الشخصية، كما أظهر بعد الأخبار المضللة والمعلومات الكاذبة نسبة (72.94٪)، ما يعكس وعياً بأن الشائعات الرقمية تهدد الثقة بالإعلام، أما بعد التأثير الخارجي والرقمي فقد بلغ (74.44٪)، مشيراً إلى إدراك متزايد لتأثير الحملات الرقمية الموجهة على الرأي العام، وحقق البعد النفسي والاجتماعي (74.83٪) تأكيداً على أن التهديدات الرقمية تؤدي إلى القلق والخوف وفقدان الثقة في الآخرين، في حين جاء البعد القانوني والتنظيمي بنسبة (75.22٪)، ما يدل على ثقة معتدلة في دور القوانين والمؤسسات الرسمية مع إدراك لوجود فجوات تشريعية، هذه النتائج مجتمعة تؤكد أن إدراك النخب الإعلامية للتهديدات الرقمية متنوع ومتعدد المستويات، إذ لا يُنظر إلى الأمن السيبراني كمشكلة تقنية فقط، بل كقضية تمس النظام الاجتماعي والنفسي والقانوني بأكمله.

ويمكن القول إن النخب الإعلامية تدرك أن التهديدات الرقمية متعددة الأبعاد، تشمل الجوانب التقنية، والمعلوماتية، والنفسية، والاجتماعية، والقانونية، وأن هذا الإدراك يرتبط بتعرضهم المكثف للخطاب الإعلامي الرقمي الذي غالباً ما يعتمد على إطار التهديد والخطر في المعالجة الصحفية لقضايا الأمن السيبراني. وهذا يعكس نجاح الإعلام الرقمي في رفع الوعي الإدراكي بالمخاطر، لكنه في المقابل يكشف عن حاجة ملحّة لتعزيز الأطر التعليمية والتوعوية التي تُسهم في بناء السلوك الوقائي والقدرة على التمييز النقدي.

أما نتائج اختبار الفروض فقد كشفت أن الفرض الأول الذي ينص على وجود علاقة ذات دلالة إحصائية بين تبني النخب للأطر في معالجة قضايا الأمن السيبراني وإدراكهم للتهديدات الرقمية قد تحقق بوضوح، إذ بلغت قيمة معامل الارتباط ($r = 0.782$) عند مستوى دلالة ($Sig = 0.000$)، ما يشير إلى علاقة قوية موجبة بين المتغيرين. ويُفسر ذلك بأن النخب الإعلامية التي تتعرض لتغطيات صحفية منظمة وتم تأطيرها بإحكام تميل إلى تكوين وعي أكبر بطبيعة التهديدات الرقمية، بما يؤكد فعالية الأطر الصحفية في تشكيل الوعي المعرفي، كما تحقق الفرض الثاني والذي ينص على وجود فروق دالة في حجم الاهتمام بقضايا الامن السيبراني حسب النوع ونوع النخبة، إذ كانت الفروق لصالح الذكور والأكاديميين. وتُفسَّر هذه الفروق بأن الذكور أكثر انخراطًا في المجال التقني والإخباري، بينما الأكاديميون يتعاملون مع القضايا الرقمية بوصفها مجالاً بحثياً وتحليلياً يثير اهتمامهم العلمي.

وتظهر النتائج من منظور نظرية الاتصال بالمخاطر دور الإعلام الرقمي في إدارة التواصل حول قضايا الأمن السيبراني فالاتصال بالمخاطر لا يقتصر على نقل التحذيرات، بل يشمل بناء الثقة وتقديم المعلومات العلمية الدقيقة والموازنة بين التهديد والحل، وتشير النتائج إلى أن الصحف الرقمية المصرية عينة الدراسة نجحت في رفع وعي النخب بالمخاطر، لكنها تحتاج إلى

مزيد من التوازن في خطابها الإعلامي لتجنب نشر القلق دون تقديم بدائل عملية. ويؤكد هذا أن الاتصال بالمخاطر الفعّال يجب أن يكون تفاعلياً وتفسيرياً لا أحادي الاتجاه، بحيث يُشرك الجمهور في عملية الفهم والإدراك بدلاً من أن يكتفي ببث التحذيرات.

وختاماً يمكن القول بأن الدراسة تُظهر أن العلاقة بين أطر المعالجة الصحفية وإدراك النخب الإعلامية للتهديدات الرقمية علاقة وثيقة ومعقدة في آن واحد، وأن الإعلام الرقمي يمارس تأثيراً محورياً في بناء ثقافة الأمن السيبراني، إلا أن هذا التأثير ما زال يحتاج إلى التطوير نحو خطاب أكثر شمولاً يجمع بين التحليل العلمي، والتثقيف الوقائي، والإشارة إلى المسؤولية الاجتماعية في حماية الفضاء الرقمي، ومن ثم، فإن تفعيل مبادئ نظريتي الأطر الإعلامية والاتصال بالمخاطر في الممارسة الصحفية يمكن أن يسهم في تعزيز أمن المعلومات لدى الجمهور، وتكوين وعي جماعي قادر على التعامل الواعي والمسؤول مع التهديدات الرقمية في ظل التحول الرقمي المتسارع.

توصيات البحث: في ضوء نتائج البحث يمكن التوصية بالآتي:

- تنويع الأطر الإعلامية في التغطية الصحفية لقضايا الأمن السيبراني بحيث لا تقتصر على إطار التهديد، بل تشمل أطر الحلول، الوقاية، والتوعية، لضمان خطاب إعلامي متوازن يدمج بين التحذير والمعرفة.

- تدريب الصحفيين والمحررين على مبادئ الاتصال بالمخاطر بهدف تعزيز قدرتهم على تبسيط المفاهيم التقنية وإيصالها للجمهور بلغة دقيقة وواضحة، بعيدًا عن التهويل أو الغموض.

- إنشاء وحدات متخصصة بالأمن السيبراني في المؤسسات الإعلامية تُعنى بالتحقق من الأخبار التقنية، ومتابعة الهجمات الرقمية، وتقديم محتوى موثوق قائم على مصادر رسمية وخبراء.

- رفع الوعي القانوني لدى الصحفيين والجمهور من خلال حملات إعلامية تُعرّف بالقوانين والسياسات الوطنية الخاصة بالجرائم الإلكترونية وحماية الخصوصية، بما يعزز الثقة في البيئة الرقمية.

- تعزيز التعاون بين المؤسسات الإعلامية والهيئات الوطنية للأمن السيبراني لتبادل المعلومات وتنسيق الرسائل التوعوية حول التهديدات الرقمية وطرق مواجهتها.

- دمج مفاهيم الأمن السيبراني والوعي الرقمي في المناهج الجامعية للإعلام والاتصال لإعداد جيل من الإعلاميين القادرين على التعامل مع القضايا التقنية بمسؤولية ومهارة.

- تطوير محتوى توعوي دوري داخل الصحف الرقمية يتناول المخاطر الرقمية بأسلوب مبسط وعملي (مقالات، فيديوهات، إنفوجرافيك)، لتشجيع السلوك الوقائي بين المستخدمين.

- تحديث التشريعات والسياسات الخاصة بالأمن السيبراني بشكل دوري لضمان مواكبتها للتطورات التقنية، مع وضع إطار قانوني واضح ينظم النشر الإعلامي المتعلق بالقضايا السيبرانية.

هوامش الدراسة:

أولا: العربية

البحيري، شيرين. (2023). دور الإعلام الرقمي في تعزيز الأمن السيبراني ومكافحة التهديدات والجرائم السيبرانية. المجلة العلمية لبحوث العلاقات العامة والإعلان، (25)، 47–85. https://doi.org/10.21608/sjocs.2023.299143

البدوي، حبيب. (2024). الحرب الرقمية والأمن السيبراني: خطر التهديدات يقابله تعزيز الدفاعات. مجلة بحوث الإعلامالرقمي،3(3)، 153-180. https://doi.org/10.21608/jsmd.2024.357434

العسكري، هناء راضي. (2024) متطلبات تحقيق الأمن السيبراني والتصدي للجرائم الإلكترونية في ضوء الرقمنة الإعلامية. المجلة العلمية لكلية التربية النوعية، جامعة المنصورة، المجلد 13، العدد 2، ص ص 155–184.

جبار ، صفاء علي (2025). دور الإعلام الرقمي في توعية الجمهور العراقي بمخاطر وجرائم الأمن السيبراني. مجلة واسط للعلوم الانسانية, 21(2), 829-849. https://doi.org/10.31185/wjfh

حشيش، ريهام عصام سيد أحمد، & خيري محمد فتوح، محمد. (2024). تقنيات الذكاء الاصطناعي في الإعلام الرقمي وتأثيرها على آراء الطلاب نحو قضايا الأمن السيبراني داخل الحرم الجامعي. مجلة التربية النوعية والتكنولوجيا: بحوث علمية وتطبيقية، 31(1)، 311–342. https://doi.org/10.21608/maat.2024.330607.1169

زيدان، أسماء مراد صالح مراد. (2024). تنمية ثقافة الأمن السيبراني لطلاب جامعة حلوان في ضوء كفايات التربية الإعلامية الرقمية (تصور مقترح). مجلة دراسات تربوية واجتماعية، 30(1.7)، 11–129. https://doi.org/10.21608/jsu.2024.384687

صالح كلنتن, فريد. (2024). التحديات والمخاطر بفقدان الثقة الإعلامية في ظل الإعلام الرقمي بسبب انتهاك الخصوصية والهجمات السيبرانية في المملكة العربية السعودية. مجلة البحوث والدراسات الإعلامية،29(29), 650-585.

محمد، سارة إبراهيم إبراهيم (2024). دور المواقع الصحفية المصرية والعربية في نشر الوعي السيبراني لدى الجمهور، رسالة دكتوراة غير منشورة، جامعة المنصورة - كلية الآداب - قسم الإعلام.

هلال, محمد عبد الحكيم. تصور مقترح لمواجهة تهديدات الأتمتة في التعليم الثانوى العام بمصر. مجلة كلية التربية فى العلوم التربوية 1 .49 (2025): 206-127.

(*)أسماء السادة محكمي أدوات البحث:

- أ.د/ أحمد عبد الكافي عبد الفتاح – أستاذ الصحافة بقسم الإعلام التربوي كلية التربية النوعية جامعة المنيا.

- أ.د/ أشرف رجب عطا- أستاذ مناهج وطرق تدريس الإعلام كلية التربية النوعية جامعة المنيا.

- أ.د/ وائل صلاح نجيب - أستاذ بقسم الإعلام التربوي كلية التربية النوعية جامعة المنيا.

- أ.د/ محمد أبو الليل – أستاذ تكنولوجيا التعليم المساعد بكلية التربية النوعية جامعة المنيا.

- أ.د/ نهى علي سيد – الأستاذ المساعد تكنولوجيا التعليم بكلية التربية النوعية جامعة المنيا.

- أ.م.د/ محمد يوسف كفافي – أستاذ تكنولوجيا التعليم المساعد بكلية التربية النوعية جامعة المنيا.

- أ.م.د/ عبد المحسن حامد أحمد - أستاذ مساعد بقسم الإعلام التربوي كلية التربية النوعية جامعة المنيا.

المراجع الإجنبية:

Al-Adawy, Z. (2024). Science Communication and Digital Journalism in Egypt: Challenges and Future Perspectives. *Arab Journal of Media & Communication Research*, Cairo University, Issue 44, p. 105-125

Alazrak, N. N. (2020). Cost of online connection: Digital threats for the Egyptian journalists and their awareness of the techniques used to attain their safety – A qualitative study. *Journal of Media Researches* , 54(6), 4299–4338. https://doi.org/10.21608/jsb.2020.110305

Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv*:1901.02672. Retrieved from https://arxiv.org/abs/1901.02672

Bojic, L., Prodanovic, N., & Samala, A. D. (2024, January 7). Maintaining journalistic integrity in the digital age: A comprehensive NLP framework for evaluating online news content [Preprint]. *arXiv*. https://arxiv.org/abs/2401.03467

Centers for Disease Control and Prevention (CDC). (2019). Crisis and Emergency Risk Communication (CERC) Manual. U.S. *Department of Health and Human Services*. Retrieved from https://emergency.cdc.gov/cerc/manual/index.asp

Chen, D., Wawrzynski, P., & Lv, Z. (2021). Cyber security in smart cities: a review of deep learning-based applications and case studies. *Sustainable Cities and Society*, 66, 102655.

Chen, Jing and Henry, Elaine and Jiang, Xi,(2022), Is Cybersecurity Risk Factor Disclosure Informative? Evidence from Disclosures Following a Data Breach (February 20, 2022). *Journal of Business Ethics*, Forthcoming, Available at SSRN: https://ssrn.com/abstract=3780388 or http://dx.doi.org/10.2139/ssrn.3780388

Chen, X., Xu, J., & Li, J. (2020). Risk communication in cyberspace: A brief review of the information-processing and mental models approaches. *Journal of Risk Research*, 23(5), 678–694. https://doi.org/10.1080/13669877.2020.1750456

Clarke, M. A., Patel, M., & Young, H. (2023). Managing cybersecurity risk in healthcare settings: Risk communication and organizational resilience. *Frontiers in Public Health*, 11, 10725101. https://doi.org/10.3389/fpubh.2023.10725101

Dave, D., Sawhney, G., Aggarwal, P., & Silswal, N. (2023). The new frontier of cybersecurity: Emerging threats and innovations [Preprint]. *arXiv*. https://doi.org/10.48550/arXiv.2311.02630

El-Awady, N. (2009), Science journalism: The Arab boom. *Nature*, 459, 1057, https://doi.org/10.1038/4591057a

Elrefai, M. (2019). Transformations and Trends in Science Journalism as Viewed by the Egyptian Media and Scientific Community. *Arab Media & Society*, 28.

Falade, P. V. (2023). Decoding the threat landscape: ChatGPT, FraudGPT, and WormGPT in social engineering attacks. International Journal of Scientific Research in Computer Science, *Engineering and Information Technology*, 9(5), 185-198. https://doi.org/10.32628/CSEIT2390533

Jones, M., & Scott, A. (2022).Media Framing of Cybersecurity Threats: An Analysis of News Narratives in Western Digital Journalism. *Digital Journalism*, 10(4), 512–530.

Knight, R., & Nurse, J. R. C. (2020). A framework for effective corporate communication after cybersecurity incidents. arXiv preprint arXiv:2009.09210. Retrieved from https://arxiv.org/abs/2009.09210

Kolich, H. N. (2014). Risk and Emergency Communications: How to Be Heard. *Clemson University*. Retrieved from https://tigerprints.clemson.edu/cgi/viewcontent.cgi?article=2276&context=joe

Leiss, W. (1996). Three phases in the evolution of risk communication practice. The Annals of the *American Academy of Political and Social Science*, 545(1), 85-94. https://doi.org/10.1177/0002716296545001009

Majebi, N. L., & Drakeford, O. M. (2021). Child safety in the digital age: Historical lessons from media regulation and their application to modern cybersecurity policies. International *Journal of Multidisciplinary Research and Growth Evaluation*, 2(1), 735–742. https://doi.org/10.54660/.IJMRGE.2021.2.1.735-742

Mazzarolo, G., Fernandez Casas, J. C., Jurcut, A. D., & Le-Khac, N.-A. (2021). Protect against unintentional insider threats: The risk of an employee's cyber misconduct on a social media site. arXiv preprint *arXiv*:2103.04744. Retrieved from https://arxiv.org/abs/2103.04744

Meissner, F., Buse, C., & Wilke, A. (2024). Mediated perspectives on cyber risk: A content analysis of news reporting about cyber threats and safety measures. Proceedings of the *International Crisis and Risk Communication Conference (ICRCC)*. p. 45-48 https://www.ssoar.info/ssoar/handle/document/98308

Meissner, F., Wilke, A. J., & Puikytė, M. (2025). How is cybersecurity discussed across media channels? Exploratory analyses of Twitter content and news reporting. *Journal of Risk Research*, 28(8), 855–875. https://doi.org/10.1080/13669877.2025.2553079

Muzykant, V., Burdovskaya, E., Muzykant, E., & Muqsith, M. A. (2023). Digital threats and challenges to netizens generation media education (Indonesian case). *Media Education* (Mediaobrazovanie), 19(1), 97–106. https://doi.org/10.13187/me.2023.1.97

Nganga, A., Khadim, M., & Tesfaye, A. (2025). Cyber risk communication during vessel incidents: Lessons from maritime cybersecurity management. *Computers & Security*, 142, 103053. https://doi.org/10.1016/j.cose.2025.103053

Oltramari, A., & Kott, A. (2018). Towards a reconceptualisation of cyber risk: An empirical and ontological study. arXiv preprint *arXiv*:1806.08349. Retrieved from https://arxiv.org/abs/1806.08349

Okonkwo, P., Njoku, I. A., & Okonkwo, R. N. (2024, November 27). Digital media ethics in generative AI journalism: A framework for accountability [Preprint]. Preprints.org. https://doi.org/10.20944/preprints202411.2157.v1

Othman, Doaa Mohsen. (2025). Cyber threats and legal gaps: A study on Egypt and UAE laws. *The Egyptian Journal of Comparative Legal Studies*, 25(2), 1637–1676. Available at: https://journals.ekb.eg/article_448547_0.html

Ritchie, B. W. (2008). Tourism disaster planning and management: From response and recovery to reduction and readiness. *Current Issues in Tourism*, 11(4), 315-348. https://doi.org/10.1080/13683500802140372

Rodríguez-Priego, N., Martínez-Martínez, A. M., & García-González, M. (2020). Framing Effects on Online Security Behavior. *Frontiers in Psychology*, 11, 527886. https://doi.org/10.3389/fpsyg.2020.527886

Romero-Masters, P. (2021). *The Model of Influence in Cybersecurity with Frames. In Advances in Human Factors in Cybersecurity*, pp.181–192. Springer. https://scispace.com/papers/the-model-of-influence-in-cybersecurity-with-frames-3fv4st8bld

Sandman, P. M. (1993). Responding to community outrage: Strategies for effective risk communication. *Fairfax*, VA: American Industrial Hygiene Association. ISBN: 9780932627299

Sbriz, L. (2021, December 21). Communicating information security risk simply and effectively, part 1. *ISACA Journal*, 6. Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/communicating-information-security-risk-simply-and-effectively-part-1

Schmitt, M. (2023). Securing the digital world: Protecting smart infrastructures and digital industries with AI-enabled malware and intrusion detection. *arXiv*. https://arxiv.org/abs/2401.01342

Sheppard, B., Janoske, M., & Liu, B. (2012). *Understanding Risk Communication Theory: A Guide for Emergency Managers and Communicators*. College Park, MD: National Consortium for the Study of Terrorism and Responses to Terrorism (START), U.S. Department of Homeland Security. Retrieved from https://www.start.umd.edu/pubs/UnderstandingRiskCommunicationTheory.pdf

Sheppard, B., Janoske, M., & Liu, B. (2012). *Understanding Risk Communication Best Practices: A Guide for Emergency Managers and Communicators*. College Park, MD: START, Department of Homeland Security. Retrieved from https://www.start.umd.edu/publication/understanding-risk-communication-best-practices-guide-emergency-managers-and

Silva, M., Raposo de Mello, A. C., & Nishijima, M. (2022). Traditional written media coverage and cybersecurity events: the NSA case. *Opinião Pública*. https://scispace.com/papers/traditional-written-media-coverage-and-cybersecurity-events-299yhwlt

Sufi, F. K. (2025). A new computational method for quantification and analysis of media bias in cybersecurity reporting. *IEEE Transactions on Computational Social Systems. Advance online publication*. https://doi.org/10.1109/TCSS.2025.3560199

Westlund, O., Boyles, J. L., Guo, L., Saldaña, M., Salaverría, R., & Wu, S. (2025). Digital journalism (studies): An agenda for the future. *Digital Journalism*, 13(2), 179–194. https://doi.org/10.1080/21670811.2025.2474530

World Health Organization (WHO). (2015). Chapter 7: *Risk and crisis communication. In Public health for mass gatherings: Key considerations. Geneva: World Health Organization*. Retrieved from https://www.who.int/ihr/publications/WHO_HSE_GCR_2015.5/en