مجلة البحوث الإعلامية

مجلة علمية محكمة تصدر عن جامعة الأزهر/كلية الإعلام

المراسلات:

- القاهرة- مدينة نصر - جامعة الأزهر - كلية الإعلام - ت: ٠٢٢٥١٠٨٢٥٦
- الموقع الإلكتروني للمجلة: http://jsb.journals.ekb.eg
- البريد الإلكتروني: mediajournal2020@azhar.edu.eg

- العدد الخامس والسبعون- الجزء الثاني - محرم ١٤٤٧هـ - يوليو ٢٠٢٥م
- رقم الإيداع بدار الكتب المصرية: ٦٥٥٥
- الترقيم الدولي للنسخة الإلكترونية: ٢٦٨٢ - ٢٩٢ x
- الترقيم الدولي للنسخة الورقية: ٩٢٩٧ - ١١١٠

الهيئة الاستشارية للمجلة

قواعد النشر

تقوم المجلة بنشر البحوث والدراسات ومراجعات الكتب والتقارير والترجمات وفقًا للقواعد الآتية:

- **يعتمد النشر على رأي اثنين من المحكمين المتخصصين في تحديد صلاحية المادة للنشر.**
- **ألا يكون البحث قد سبق نشره في أي مجلة علمية محكمة أو مؤتمرًا علميًا.**
- **لا يقل البحث عن خمسة آلاف كلمة ولا يزيد عن عشرة آلاف كلمة ... وفي حالة الزيادة يتحمل الباحث فروق تكلفة النشر.**
- **يجب ألا يزيد عنوان البحث (الرئيسي والفرعي) عن ٢٠ كلمة.**
- **يرسل مع كل بحث ملخص باللغة العربية وآخر باللغة الانجليزية لا يزيد عن ٢٥٠ كلمة.**
- **يزود الباحث المجلة بثلاث نسخ من البحث مطبوعة بالكمبيوتر .. ونسخة على CD، على أن يكتب اسم الباحث وعنوان بحثه على غلاف مستقل ويشار إلى المراجع والهوامش في المتن بأرقام وترد قائمتها في نهاية البحث لا في أسفل الصفحة.**
- **لا ترد الأبحاث المنشورة إلى أصحابها .... وتحتفظ المجلة بكافة حقوق النشر، ويلزم الحصول على موافقة كتابية قبل إعادة نشر مادة نشرت فيها.**
- **تنشر الأبحاث بأسبقية قبولها للنشر .**
- **ترد الأبحاث التي لا تقبل النشر لأصحابها.**

محتويات العدد

م	القطاع	اسم المجلة	اسم الجهه / الجامعة	ISSN-P	ISSN-O	السنه	نقاط المجله
1	الدراسات الإعلامية	المجلة العربية لبحوث الإعلام و الإتصال	جامعة الأهرام الكندية، كلية الاعلام	2536-9393	2735-4008	2023	7
2	الدراسات الإعلامية	المجلة العلمية لبحوث الإذاعة والتلفزيون	جامعة القاهرة، كلية الإعلام	2356-914X	2682-4663	2023	7
3	الدراسات الإعلامية	المجلة العلمية لبحوث الإعلام و تكنولوجيا الإتصال	جامعة جنوب الوادي، كلية الإعلام	2536-9237	2735-4326	2023	7
4	الدراسات الإعلامية	المجلة العلمية لبحوث الصحافة	جامعة القاهرة، كلية الإعلام	2356-9158	2682-4620	2023	7
5	الدراسات الإعلامية	المجلة العلمية لبحوث العلاقات العامة والإعلان	جامعة القاهرة، كلية الإعلام	2356-9131	2682-4671	2023	7
6	الدراسات الإعلامية	المجلة المصرية لبحوث الإعلام	جامعة القاهرة، كلية الإعلام	1110-5836	2682-4647	2023	7
7	الدراسات الإعلامية	المجلة المصرية لبحوث الرأي العام	جامعة القاهرة،كلية الإعلام، مركز بحوث الراى العام	1110-5844	2682-4655	2023	7
8	الدراسات الإعلامية	مجلة البحوث الإعلامية	جامعة الأزهر	1110-9297	2682-292X	2023	7
9	الدراسات الإعلامية	مجلة البحوث و الدراسات الإعلامية	المعهد الدولي العالي للإعلام بالشروق	2357-0407	2735-4016	2023	7
10	الدراسات الإعلامية	مجلة إتحاد الجامعات العربية لبحوث الإعلام و تكنولوجيا الإتصال	جامعة القاهرة، جمعية كليات الاعلام العربية	2356-9891	2682-4639	2023	7
11	الدراسات الإعلامية	مجلة بحوث العلاقات العامة الشرق الأوسط	Egyptian Public Relations Association	2314-8721	2314-873X	2023	7
12	الدراسات الإعلامية	المجلة المصرية لبحوث الاتصال الجماهيري	جامعة بني سويف، كلية الإعلام	2735-3796	2735-377X	2023	7
13	الدراسات الإعلامية	المجلة الدولية لبحوث الإعلام والاتصالات	جمعية تكنولوجيا البحث العلمي والفنون	2812-4812	2812-4820	2023	7

التشريعات السيبرانية للجرائم الافتراضية في بيئة الإعلام الرقمي: مقترح مسودة قانون للأمن السيبراني في المؤسسات الإعلامية

Cyber Legislation for Virtual Crimes in the Digital Media Environment: Proposed Draft Law on Cybersecurity in Media Organizations

أ.م.د/ شريهان محمود أبو الحسن كشك

أستاذ الصحافة المساعد - كلية الإعلام وتكنولوجيا الاتصال - جامعة قنا

Email: Shreehan.abulhassan@svu.edu.eg

ملخص الدراسة

استهدفت الدراسة استكشاف التهديدات السيبرانية بالمؤسسات الصحفية والإعلامية، وطرق الوقاية منها، مع مراقبة وتحليل الأنشطة السيبرانية عبر الإنترنت، للكشف عن الهجمات ومنعها، وتحديد نقاط الضعف المحتملة في الشبكات، وأهمية تثقيف الإعلاميين بتهديدات الأمن السيبراني، وأفضل الممارسات التي ينبغي اتباعها لمنع مثل هذه الهجمات السيبرانية، بتطبيق أداة الاستبيان على عدد (72) من مديرى مراكز تكنولوجيا المعلومات في المؤسسات الصحفية والإعلامية، علاوة على إجراء المقابلة المتعمقة مع عدد (18) خبيرًا من أساتذة الإعلام والحاسبات والمعلومات والحقوق، والمتخصصين في مجال الأمن السيبراني، بهدف اكتساب فهم أفضل للوضع الراهن للتهديدات السيبرانية، وتوصلت نتائج الدراسة إلى دور الأمن السيبراني في حماية الملكية الفكرية وحماية الأصول من السرقة والقرصنة، حيث تُعدُّ الملكية الفكرية، مثل المحتوى الأصلي والأخبار الحصرية، من أهم أصول المؤسسات الإعلامية، إضافة إلى الامتثال للقوانين واللوائح، حيث تخضع المؤسسات الإعلامية لعديد من القوانين واللوائح المتعلقة بحماية البيانات والخصوصية، كما يساعد الأمن السيبراني على ضمان الامتثال لهذه القوانين، وتجنب العقوبات القانونية، وأيضًا زيادة الوعي الأمني، علاوة على ضرورة اكتساب محللي الأمان البصيرة السيبرانية في المواقع الإعلامية، بمعنى أن يتوفر لديه نظرة ثاقبة على التهديدات السيبرانية وهجمات الأمن السيبراني والمخاطر السيبرانية، مثل نقاط الضعف والاستغلال، والحوادث الأمنية، وخروقات البيانات، والجرائم الافتراضية، خاصة تهديدات الأمن السيبراني في وسائل التواصل الاجتماعي، وهجمات الهندسة الاجتماعية، وعدم وجود سياسة وسائل التواصل الاجتماعي، وفي الختام استطاعت الباحثة أن تقدم مسودة تشريعية سيبرانية تنظم كيفية مواجهة الجرائم الافتراضية في بيئة الإعلام الرقمي.

الكلمات المفتاحية: الأمن السيبراني، الجرائم الافتراضية، دافع الحماية.

Abstract

The study aimed to discover cyber threats to journalistic and media institutions, and ways to prevent them, while monitoring and analyzing cyber activities over the Internet to detect and prevent attacks and identify potential vulnerabilities in networks, and the importance of educating media professionals about cyber security threats and the best practices that should be followed to prevent such cyber attacks by applying the questionnaire tool to (72) managers of information technology centers in journalistic and media institutions, in addition to conducting an in-depth interview with (18) experts from media, computer, information and law professors, and specialists in the field of cyber security, to gain a better understanding of the current status of cyber threats. The results of the study reached the role of cyber security in protecting intellectual property and protecting assets from theft and piracy, as intellectual property, such as original content and exclusive news, is considered one of the most important assets of media institutions, in addition to compliance with laws and regulations, as media institutions are subject to many laws and regulations related to data protection and privacy. Cyber security also helps ensure compliance with these laws and avoid legal penalties and also increases security awareness, in addition to the need for security analysts to acquire cyber insight into sites. Media, meaning that he has insight into cyber threats, cybersecurity attacks, and cyber risks such as vulnerabilities, exploitation, security incidents, data breaches, and cybercrimes, especially cybersecurity threats in social media, social engineering attacks, and the lack of a social media policy. In conclusion, the researcher was able to present a draft of cyber legislation that regulates how to combat virtual crimes in the digital media environment.

Keywords: cybersecurity, virtual crimes, protection motive

مقدمة:

يعد الفضاء الإلكتروني تطوراً جديدًا نسبيًا في تاريخ البشرية، وقد أصبح استخدام الأسلحة السيبرانية، ومناقشات الحروب السيبرانية المحتملة مصدر قلق له آثاره السياسية، كما تشكل حماية المعلومات الشخصية والملكية الفكرية من الهجمات الإلكترونية مصدر قلق آخر، حيث تعرض سلامة أنظمة المعلومات للخطر[1]، وعلى الرغم من وجود عديد من المزايا المرتبطة بالاتجاه المتزايد نحو استخدام التكنولوجيا، فإنه يطرح تحديات جديدة، أبرزها الهجمات الإلكترونية، التي أثَّرت في مختلف القطاعات[2]، كما أدى تطور الأسلحة النووية إلى تغيير الاستراتيجية العسكرية من كسب الحروب إلى تجنبها، حيث يتغير واقع الحروب مع ظهور الحروب السيبرانية[3].

وأوضح "Wall" أن الإنترنت أصبحت ساحة لعب للمجرمين، وأصبح وجود الجريمة المنظمة إلى جانب الخبرة من أقوى المهارات التي أصبحت أكثر إغراءً للنجاح[4]، وأدى انتشار التكنولوجيا إلى خلق نقاط ضعف جديدة داخل المجال السيبراني، التي قد تعمل مباشرة على تقويض أمن البلاد، حيث يطور قراصنة الكمبيوتر برامج وأساليب متقدمة مصممة للتسلل إلى البنية التحتية للدولة وتعطيلها، وسرقة معلومات سرية للدولة أو الشركات، علاوة على سرقة الهوية والاحتيال، وسرقة البنوك والمؤسسات المالية ومؤسسات الإعلام، حتى تقويض العمليات الديمقراطية، مثل الانتخابات، كما تبنى الإرهابيون الفضاء الإلكتروني مجالًا يُمكِّنهم من تجنيد أتباع لهم، ونشر الدعاية المضادة، وتقديم المشورة، وتشجيع من يرغب في تنفيذ عمليات إرهابية[5]، حتى أصبح مصطلح "الحرب الإلكترونية" كلمة طنانة مستخدمة بشكل متكرر للإشارة إلى أي نوع من الصراعات في الفضاء الإلكتروني ذات البعد الدولي[6].

وتشكل التهديدات السيبرانية المتزايدة تهديداً أمنياً للبنية التحتية بمختلف الأنظمة، مثل نقاط ضعف البنية التحتية الحرجة، كنقاط الضعف بوسائل الإعلام التي يمكن استغلالها من قبل المهاجمين الإلكترونيين، مما يتسبب في حدوث اضطرابات واسعة النطاق، نتيجة استخدامهم تقنيات متقدمة، مثل برامج الفدية، والبرامج الضارة، وهجمات التصيد الاحتيالي والفيروسات، وأحصنة طروادة والديدان وشبكات الروبوتات، وهي مصممة للوصول بشكل غير قانوني بغرض التسلل إلى أنظمة البنية التحتية الحرجة وتعطيلها، يليه التصيد الاحتيالي أو البريد الإلكتروني من "صديق" أو رابط موثوق به، وأخيراً هجوم رفض الخدمة، الذي يتضمن هجوم الجهات الفاعلة المهددة خوادم أو أنظمة الكمبيوتر أو الشبكات باستخدام أنظمتها لشن هجوم على الخادم، مما يؤدي إلى زيادة تحميل خوادم الضحية أو نظامها، وإيقاف تشغيلها، مما يجعل النظام/ الخادم غير قابل للتشغيل، فيسبب ضرراً للسمعة أو خسائر مالية فادحة[7]، علاوة على نقاط ضعف أجهزة إنترنت الأشياء (IoT)، وغالباً ما تفتقر هذه الأجهزة إلى تدابير أمنية كافية، مما يسهل الوصول إليها واختراقها[8]، ويمكن لهذه الهجمات أن تجبر المؤسسات على دفع فدية كبيرة لاستعادة السيطرة، مما يؤكد خطورة الموقف، والحاجة إلى اتخاذ إجراءات فورية.

ويُشكِّل الموظفون المتصلون بالمنصات المفتوحة ومنصات التواصل الاجتماعي داخل مؤسساتهم خطراً على الأمن السيبراني للمنظمة، التي تحتوي على نقاط ضعف محتملة، حيث يمكن اختراق أحد قراصنة الأمن السيبراني منصات التواصل الاجتماعي، حال تسجيل الموظفين الدخول إلى حساباتهم على مواقع التواصل الاجتماعي أثناء ساعات العمل، فيسرق المخترق حساب الموظف ومعلومات هويته، ويخترق مواقع الويب الخاصة بالمنظمات الإعلامية، ومن ثم تسهيل مهمة الهجوم السيبراني، لذا ينبغي فحص البيانات التي يجب حمايتها من قبل المؤسسات الإعلامية للتأكد من مخاطر الأمن السيبراني المحتملة[9].

وقد اهتمت حكومة الهند بوضع تشريع سيبراني جزءاً من قانون تقنية المعلومات عام 2015م، كما اهتم الاتحاد الأوروبي بوضع اللائحة العامة لحماية البيانات عام

2016م، وصدر قانون الأمن السيبراني الصيني عام 2016م بعدما خسر الاقتصاد الصيني أكثر من 830 مليون دولار نتيجة الجرائم السيبرانية في عام 2011م، وفي عام 2021م اعتمدت الجمعية العامة للأمم المتحدة مشروع قرار يحدد شروط التفاوض على معاهدة الأمم المتحدة بشأن الجرائم الافتراضية، واتفق زعماء من مجموعة الـ 72 على تطوير قابلية تطبيق القانون الدولي على الأمن السيبراني، وأعلنت مجموعة السبع أن زعماء الدول مسؤولين عن الجهات الفاعلة السيبرانية الخبيثة داخل بلادهم[10]، أما في مصر فلم يصدر حتى الآن قانون خاص بالأمن السيبراني، ولكن اعتمدت الاستراتيجية الخمسية الوطنية للأمن السيبراني من 2023 حتى 2027م، كما صدر قانون مكافحة جرائم تقنية المعلومات في عام 2018م، وقانون حماية البيانات الشخصية عام 2020م.

ومن الضروري تنمية الشعور بالوعي بالأمن السيبراني بين الإعلاميين حتى يتمكنوا من التعرف على حساسية البيانات والمعلومات الخاصة الملموسة وغير الملموسة داخل مؤسساتهم الإعلامية والاعتراف بها، وإنشاء بيئة إلكترونية آمنة ومأمونة ليستفيد الجميع من الفضاء الإلكتروني، وخلق مساحة لمحو الأمية الرقمية.

في ضوء ما سبق، تأتي الدراسة الراهنة محاولة لوضع مسودة قانون للتشريعات السيبرانية المنظمة لطبيعة العمل الصحفي، والحد من الجرائم الافتراضية التي تتعرض لها المؤسسات الإعلامية، والقضاء عليها، وأهمية التفطن الدائم والاستعداد المستمر لأي هجمة قد تتعرض لها، والتعاون الدائم مع الدول من أجل التصدي للهجمات السيبرانية وحماية مجالها، مع تشديد القوانين والعقوبات على المهاجمين، خاصة وأن الفضاء السيبراني أصبح مجالًا للهجمات والحروب وتصفية الحسابات.

أولًا: مشكلة الدراسة:

أدى الاعتماد المتزايد على التكنولوجيا والترابط بين الأنظمة الرقمية إلى ارتفاع هائل في وتيرة التهديدات السيبرانية، مما يشكل تهديدًا خطيرًا على الأمن القومي والاستقرار الاجتماعي والازدهار الاقتصادي والعمل الصحفي، ويمكن أن تؤدي الهجمات السيبرانية في بيئة الإعلام الرقمي إلى خسائر مالية كبيرة، وانتهاكات للبيانات، وتعطيل البنية

التحتية الحيوية، والمساس بالمعلومات الحساسة، وتغييرها أو تحريفها، ويمكن القول بأن تنوع الجهات الفاعلة المشاركة في الهجمات السيبرانية، يزيد من تعقيد مواجهة هذه التهديدات السيبرانية، ويمثل الافتقار إلى التشريعات السيبرانية المنظمة لطبيعة العمل الصحفي عائقًا لمقاضاة مجرمي الإنترنت، لذا وجب التعاون الدولي، وسن التشريعات اللازمة مثل قانون الأمن السيبراني لمواجهة التهديدات السيبرانية، وضمان بيئة إعلام رقمي آمنة ومرنة، كما ينبغي اعتماد آليات الأمن السيبراني لإحباط الهجمات السيبرانية في المؤسسات الإعلامية، من خلال بناء استراتيجيات قوية للأمن السيبراني، وحماية أصول تكنولوجيا المعلومات الخاصة بها.

وتشكل الجرائم الافتراضية تحدياً بين الواقع الافتراضي للفضاء الإلكتروني ونظام العدالة الجنائية، وانتهاكًا للمؤسسات الإعلامية، وهي مخالفة ترتكب ضد أفراد أو جماعات بدافع إجرامي وبنية الإساءة لسمعة الضحية، سواءً بطريقة مباشرة أو غير مباشرة، وباستخدام وسائل الاتصال الحديثة مثل الإنترنت، وغرف الدردشة، والبريد الإلكتروني، وفي نهاية المطاف يعد التعاون أمراً ضرورياً بين مختلف الوكالات الحكومية والخاصة دولياً لمكافحة الجرائم الافتراضية.

تأسيساً على ما سبق، تنبع المشكلة البحثية لهذه الدراسة من الحاجة الملحة لوضع مسودة قانون للتشريعات السيبرانية للجرائم الافتراضية في بيئة الإعلام الرقمي، من خلال إجراء استبيان مع مديرى تكنولوجيا المعلومات بالمؤسسات الصحفية، علاوة على إجراء مقابلات متعمقة مع خبراء ومتخصصين في الأمن السيبراني والعمل الصحفي، وأكاديميين في مجالات القانون والحاسبات والمعلومات والإعلام.

ثانيا: أهمية الدراسة:

- **أهمية الدراسة مهنيا:**

1- توعية الإعلاميين والصحفيين بأمن المعلومات وغيرها من المخاطر السيبرانية عبر الإنترنت.

2- تمثل الأخبار الزائفة أحد أشكال الجرائم الافتراضية في الفضاء الإلكتروني.

3- يؤدي استخدام وسائل التواصل الاجتماعي إلى تهديدات الأمن السيبراني التي من الممكن أن تؤثر في سمعة المؤسسة.

4- البحث عن آليات جديدة للحماية الإلكترونية لدول الشرق الأوسط خاصة مصر.

5- تأمين الفضاء الإلكتروني للمؤسسات الإعلامية ضرورة ملحة في الوقت الحالي، خاصة بعد انتشار الحروب السيبرانية.

6- التعاون الدولي من أجل معالجة تهديدات الأمن السيبراني العالمية دون المساس بالحريات الرقمية.

- **أهمية الدراسة أكاديميا:**

1-تعزيز الأمن السيبراني للبنية التحتية الرقمية في الحقل الإعلامي.

2-تحسين الوضع الأمني للمنظمات الإعلامية، وحماية نفسها من الهجمات الافتراضية.

3-محاولات التأثير في الرأي العام من خلال نشر وبث الأخبار الزائفة التي تخدم أهداف ومصالح دول أخرى عبر اختراق المنصات الإعلامية.

4-قلة تكاليف الحروب السيبرانية مقارنة بنظيرتها التقليدية حيث يتم الهجوم في أي وقت، علاوة على بروز العمليات العدائية في الفضاء الإلكتروني، مثل الصراع بين روسيا وإستونيا عام 2007م، والحرب بين روسيا وجورجيا عام 2008م، والحرب بين كوريا الجنوبية والولايات المتحدة عام 2009، وأخيراً الحرب بين روسيا وأوكرانيا عام 2022.

5-حماية حقوق التعبير والحفاظ على الديمقراطية في الفضاء الإلكتروني.

6-التطور التكنولوجي والتحول الرقمي الذي تشهده البلاد في مختلف القطاعات يحتم علينا وضع أطر قانونية تنظم طبيعة العمل الإعلامي، والحفاظ عليه من الهجمات السيبرانية وتعطيل الأنظمة وسرقة البيانات وتحريفها أو تأويلها، خاصة وأن تأمين الفضاء السيبراني جزء من استراتيجيات الأمن القومي.

7-تساعد الدراسة على سد الفجوة في الأبحاث العلمية، التي توضح مدى الافتقار إلى القوانين والمعايير الدولية للحروب السيبرانية، خاصة في المؤسسات الإعلامية.

ثالثاً: أهداف الدراسة

يتمثل الهدف الرئيس للدراسة في: اقتراح مسودة قانون سيبراني منظم لطبيعة العمل الصحفي بهدف حمايته من الجرائم الافتراضية، وينبع من هذا الهدف عدة أهداف فرعية أخرى تتمثل في:

أولًا: أهداف الدراسة الميدانية:

1- التعرف على أهمية الأمن السيبراني في المؤسسات الصحفية والإعلامية.

2- رصد دور المؤسسات الإعلامية في العمل وفقًا لاستراتيجيات وبروتوكولات الأمن السيبراني.

3- إبراز أهمية توعية الصحفيين بالتهديدات السيبرانية في المؤسسات الإعلامية والصحفية.

4- معرفة آلية تدريب الصحفيين والموظفين على أطر استخدام وسائل التواصل الاجتماعي داخل مقار عملهم.

5- رصد التحديات التي تواجه الأمن السيبراني في المؤسسات الصحفية والإعلامية.

6- معرفة المخاوف الأخلاقية التي يمكن أن يتسبب الأمن السيبراني في حدوثها بالمؤسسات الإعلامية.

7- رصد آليات الأمن السيبراني لإحباط الهجمات السيبرانية في مؤسساتهم الإعلامية.

8- معرفة العوامل التي ينبغي للصحفيين والإعلاميين في المؤسسات الصحفية والإعلامية مراعاتها عند اعتماد آليات الأمن السيبراني لإحباط الهجمات السيبرانية في مؤسساتهم.

9- إبراز أهمية التشريعات السيبرانية التي تنظم بيئة الإعلام الرقمي.

أهداف المقابلة المتعمقة:

1- رصد أهمية الأمن السيبراني في المؤسسات الإعلامية من وجهة نظر خبراء الدراسة.

2- أهمية اكتشاف التهديدات السيبرانية وطرق الوقاية منها من وجهة نظر خبراء الدراسة.

3- أهمية إدارة مخاطر الأمن السيبراني بالمؤسسات الإعلامية، وحماية البنية التحتية التي تستهدفها الجماعات الإرهابية.

4- رصد آليات حماية المعلومات والبيانات من الجرائم السيبرانية من وجهة نظر خبراء الدراسة.

5- معرفة العوامل التي ينبغي مراعاتها عند وضع الأيديولوجية الأخلاقية والمهنية للأمن السيبراني لمنع الجرائم الافتراضية في المؤسسات الإعلامية من وجهة نظر خبراء الدراسة.

6- إبراز أهمية تثقيف الإعلاميين بتهديدات الأمن السيبراني وإدارتها؟ وأسس تطبيق استراتيجيات الدفاع، أو التدابير المضادة من وجهة نظر خبراء الدراسة.

7- رصد دور الدولة المصرية في التخفيف من مخاطر الأمن السيبراني التي تواجه وسائل الإعلام من وجهة نظر خبراء الدراسة.

8- إبراز أهمية التعاون الدولي لحماية الفضاء الإلكتروني لوسائل الإعلام من التهديدات السيبرانية من وجهة نظر خبراء الدراسة.

9- معرفة الأطر القانونية والتشريعات السيبرانية المنظمة لطبيعة العمل الصحفي والتي يمكن الخروج بها من الدراسة الحالية من وجهة نظر خبراء الدراسة.

رابعا: الدراسات السابقة

تنقسم الدراسات السابقة إلى المحاور الآتية:

المحور الأول: التشريعات السيبرانية.

المحور الثانى: الجرائم الافتراضية في الإعلام الرقمى.

وفيما يلي عرض تفصيلي لكل محور على حدة:

المحور الأول: التشريعات السيبرانية

سعت دراسة Brian Chundu ,et al (2025)[11] لتحديد الركائز المناسبة لإطار حوكمة الأمن السيبراني في السلطات المحلية في زيمبابوي، باستخدام أساليب مختلطة (كمية ونوعية وفقًا لفلسفة براجماتية)، واستطلعت الدراسة خمس سلطات محلية حضرية، هي: هراري وبولاوايو وجويرو وموتاري وماسفينغو، وتوصلت نتائج الدراسة إلى أن السرية والنزاهة والمصادقة والتفويض وعدم التنصل هي الركائز الأساسية لإطار حوكمة الأمن السيبراني، كما تسهم العوامل التنظيمية، بما في ذلك الهيكل، والتدريب والتطوير، وإدارة المخاطر، في تطوير إطار حوكمة الأمن السيبراني، ويمكن استخدام

نتيجة هذه الدراسة في البلدان النامية لصياغة أطر متعلقة بتكنولوجيا المعلومات، ويجب أن تركز الدراسات المستقبلية على تقييم حوكمة الأمن السيبراني في السلطات المحلية بالمناطق الريفية في زيمبابوي، واهتمت دراسة Clanton, Elfriede L (2024)[12] بالتشريعات التي تصاحب جهود التقدم في التحول الرقمي في أقل البلدان نمواً، حيث يجب أن يكون الوصول الرقمي الأمن محوراً أساسيًا للمشرعين الإلكترونيين وأصحاب المصلحة في تحقيق أهداف التنمية المستدامة، وغالبًا ما تتفوق الرقمنة على إنشاء وتنفيذ الضوابط الفنية وأطر الحوكمة للأمن السيبراني؛ لذلك توجد حاجة إلى التشريعات الإلكترونية لضمان مواكبة الأمن السيبراني لخطط التنمية الرقمية، وضرورة وصول جهود الدبلوماسية الإلكترونية إلى الوافدين الجدد في الفضاء الإلكتروني، من خلال بناء شراكات لضمان معرفة الأمن السيبراني، وتوفير الأساليب والسياسات والتشريعات لحماية النشاط السيبراني للدول، وتعزيز السلوك المسؤول في الفضاء الإلكتروني.

وهدفت دراسة Ifeanyi-Ajufo, N. (2023)[13] إلى دراسة أجندة الحوكمة السيبرانية في إفريقيا فيما يتعلق بالأمن والسلام، من خلال البحث في السياسات والاستراتيجيات السياسية في إفريقيا للحوكمة السيبرانية، وتفاعل المنطقة مع عمليات الحوكمة السيبرانية الدولية، ومناقشة الآفاق والتحديات التي تواجه الحوكمة السيبرانية في المنطقة، وأساليب الاستفادة من التعاون الدولي في تعزيز الاستقرار السيبراني في المنطقة، وتعتمد دراسة Barber, I. A., & Kumar, S. (2023)[14] على دراسة الحالة لتقديم توصيات يمكن من خلالها تقديم توصيات لمعرفة مدى تأثير التشريعات السيبرانية على حقوق الإنسان، بما في ذلك الآثار الإيجابية والسلبية للتدابير المتخذة في معالجة الجرائم السيبرانية)على سبيل المثال ما يتعلق بنطاق التجريم والسلطات الإجرائية)، التي تشكل جزءاً من المناقشات المتعلقة بالاتفاقية، وكيفية تورطها في حقوق الإنسان، وشرح دور المجتمع المدني في وضع أطر الجرائم السيبرانية التي تعزز حقوق الإنسان، كما تسلط الدراسة الضوء على الكيفية التي يمكن بها لخبرات المجتمع المدني أن تدعم مباشرة تطوير نهج يحترم الحقوق تجاه الجريمة السيبرانية، كما قدمت

توصيات للدول الأعضاء وأصحاب المصلحة، ووضع صك يحترم الحقوق، ويتصدى بفاعلية للجرائم السيبرانية بطريقة تحترم الحقوق.

وركَّزت دراسة Zhang Yan (2022)[15] على اهتمام عديد من الدول بتمرير التشريعات التي تحمي أمنها السيبراني، وتأمين الفضاء السيبراني، وفهم الاختلافات بين قانون الأمن السيبراني لجمهورية الصين الشعبية (2016)، وقانون أمن البيانات لجمهورية الصين الشعبية (2021) بشكل كبير، وأهمية العودة إلى الطبيعة العابرة للأفراد والعابرة للحدود الوطنية والعابرة للفضاء السيبراني نفسه، وبغرض التفكير في تشريعات الأمن السيبراني الحالي في الصين، وتوضيح العلاقة الجدلية بين الدول ذات السيادة والمجتمع ذو المستقبل المشترك في الفضاء الإلكتروني، وإرساء تشريعات الأمن السيبراني، وبناء مجموعة من المعايير الأساسية لمثل هذه التشريعات التي تحتوي على الأفكار التشريعية والمبادئ الأساسية ومكونات النظام التشريعي، بينما سلطت دراسة Dennis Broeders et al (2022)[16] الضوء على تطور القوانين الدولية والمعايير السيبرانية الدولية في الفضاء الإلكتروني، من خلال إعادة تقييم خمس عمليات سيبرانية رئيسية بقيادة الدولة (ستوكسنت 2010، وبلجاكوم 2013-2014، وشبكة الكهرباء الأوكرانية 2015، والانتخابات الرئاسية الأمريكية 2016، ونووت بيتيا 2017)، وباعتبار التطورات المعيارية والممارسات الحكومية الناشئة نقاط مرجعية أساسية، وإلقاء الضوء على طبيعة و(عدم) شرعية هذه العمليات السابقة، وفي كل حالة، يركز التحليل على العناصر التي تؤدي إلى انتهاك القانون الدولي؛ والأهمية القانونية للمصادر الحديثة لتفسير القانون الدولي؛ والعقبات القانونية والسياسية التي لا تزال تكمن وراء تطبيقها، خاصة وأن إعادة تقييم هذه العمليات السيبرانية تكشف كيف قطع المجتمع الدولي شوطًا طويلًا في ضبط لغته وممارساته المعيارية في استنكار السلوك غير المسؤول في الفضاء الإلكتروني، واتخاذ الدول خطوات صغيرة، وغير مسبوقة من خلال الإسناد العلني والتصريحات بشأن القانون الدولي في الفضاء الإلكتروني.

اهتمت دراسة Kubo Mačák (2021)[17] بمعرفة عوامل فصل القانون الدولي عن المعايير الدولية، باعتبارهما الإطارين التنظيميين الرئيسيين اللذين يحكمان سلوك

العمليات السيبرانية العسكرية، والتمييز بين القواعد الخاصة بالمجال والقواعد العامة للقانون الدولي كما تنطبق على العمليات السيبرانية العسكرية، والتمييز بين وقت السلم والصراع المسلح فيما يتصل بتنظيم مثل هذه العمليات، بمجرد اندلاع صراع مسلح، والتمييز بين المقاتلين وغير المقاتلين في الفضاء الإلكتروني، خاصة فيما يتصل ببيانات الكمبيوتر المتأثرة بالعمليات السيبرانية العسكرية أثناء النزاعات المسلحة، ومن ثمَّ الحد من الغموض المحيط بالعلاقة بين العمليات السيبرانية العسكرية والقانون الدولي، من خلال الإسهام في تحقيق الهدف طويل الأمد، المتمثل في جعل الفضاء الإلكتروني بيئة أكثر انفتاحاً وأمناً واستقراراً وإمكانية الوصول، وتناولت دراسة William Akoto et al , (2021)[18] القوانين السيبرانية التي ترعاها الدول، حيث لجأت بعض الدول إلى الاستعانة بوكلاء سيبرانيين غير تابعين للدول لتنفيذ العمليات السيبرانية، وهم جهات فاعلة غير حكومية "تنفذ عمليات سيبرانية هجومية لتحقيق أهداف سياسية نيابة عن دولة راعية"، ولكن من المحير أن نرى لماذا لا تشارك مزيد من الدول في هذه الممارسة، ويمكن للدول أن تبقي وكلاءها قريبين نسبياً، وتراقب أنشطتهم وتوجههم وفقًا لأهدافها وتقنياتها المستخدمة، وقد يضع آخرون مسافات عملياتية أكبر بينهم وبين وكلائهم، مما يوفر لهم الدعم الفكري والمادي في مقابل تعاون الوكيل في استهداف خصوم سياسيين محددين، وقد تضع دول أخرى مسافة أكبر بينها وبين وكلائها، فتتجنب أي مدخلات مباشرة، وتمنح الوكيل حرية التصرف فيما يتصل بالأهداف والتقنيات، وعلى الرغم من أن دعم الدولة يكون سلبياً تماماً، وفي أغلب الحالات، فإن الرابط الوحيد بين هذا الوكيل والدولة هو أن الدولة تغض الطرف عن أنشطة الوكيل طوعاً على الرغم من امتلاكها القدرة على قمعها.

وعرضت دراسة Ebert, H (2020)[19] دوافع السياسات الوطنية والدولية التي اعتمدتها الدولة الهندية لمعالجة التهديدات السيبرانية للأمن القومي في الهند في العقدين الماضيين، وتوصلت نتائج الدراسة إلى الحاجة إلى مزيد من الدراسة للربط بين الأنواع المختلفة من القدرات السيبرانية وهيكل الدولة والأنظمة السياسية إضافة إلى الظروف المحددة التي يمكن للديمقراطيات الرقمية ترجمة قدراتها وأنظمة تكنولوجيا

المعلومات والاتصالات الخاصة بها إلى قدر أكبر من المرونة السيبرانية، كما تبحث دراسة Adams, Jackson (2020)[20] في فعالية قوانين المسؤولية الدولية والوطنية المتعلقة بحماية حقوق الخصوصية، مثل المعلومات الشخصية المتبادلة أثناء المعاملات الإلكترونية، وتهتم الدراسة بالإجابة عن سؤال: "كيف ننظم الخصوصية في الفضاء الرقمي؟"، وتوضح الدراسة الصعوبات القانونية المرتبطة بـ "الاختصاصات السيبرانية"، التي غالبًا ما تؤدي إلى تضارب القوانين بين الدول الوطنية، ولإثبات محدودية قوانين الخصوصية السيبرانية، شرعت الدراسة في التحقيق في البيئات القانونية في كل من الاتحاد الأوروبي والولايات المتحدة للتعامل مع مفهوم "الخصوصية"، وتطوير وحماية "حق الخصوصية"، وملاحقة انتهاكات حماية الخصوصية، وانتهاك القوانين ذات الصلة، وأخيرًا تناولت دراسة Myriam Dunn Cavelty (2018)[21] سياسة الأمن السيبراني بالاتحاد الأوروبي، وتحديد القضايا والتحديات التي تواجه مثل هذا المشروع، من ناحية أخرى، تعمل على نقل المناقشات حول القوة السيبرانية في أوروبا إلى خطوة أبعد، من خلال تقديم قراءات بديلة للقوة السيبرانية في سياق أوروبي محدد، ومن ثمَّ تحفيز مناقشة أوسع نطاقًا تتجاوز مسألة مقدار القوة السيبرانية التي يتمتع بها الاتحاد الأوروبي والتركيز بدلًا من ذلك على نوع القوة السيبرانية التي يتمتع بها.

المحور الثانى: الجرائم الافتراضية في الإعلام الرقمى

اهتمت دراسة Shawe, R (2024)[22] بالهجمات السيبرانية التي يرتكبها أفراد أو مجموعات داخل بلد ما، مستهدفة البنى التحتية الأساسية، كالمؤسسات الإعلامية، وعواقبها الجيوسياسية بعيدة المدى، مما يؤدي إلى خلق مناخ من انعدام الأمن وعدم الثقة بين الدول، ومن ثمَّ يؤثر على التعاون الدولي في معالجة تهديدات الأمن السيبراني، لذا وجب التعاون بين الحكومات والمنظمات الدولية وكيانات القطاع الخاص للتخفيف من التأثير العالمي للإرهاب السيبراني المحلي، وبذل الجهود لتعزيز تبادل المعلومات والتعاون الاستخباراتي لتحسين قدرات الأمن السيبراني والمرونة، مع أهمية اللوائح والتشريعات المعززة لردع وملاحقة الإرهابيين السيبرانيين المحليين بشكل فعال، وتوفير إطار قانوني لمعالجة هذا التهديد، وتهدف دراسة **قادري & نور الهدى** (2023)[23] إلى دراسة الجريمة

السيبرانية باعتبارها من الموضوعات القانونية الحديثة التي ظهرت تزامنا مع ظهور الثورة التكنولوجية التي أثرت على جميع مناحي الحياة، ونظراً لطابع الخصوصية التي تتميز بها الجرائم السيبرانية، إضافة إلى كونها إحدى الجرائم العابرة للحدود، فقد عمل المشرع الجزائري على اتخاذ مجموعة من التدابير والآليات القانونية لمكافحتها وردع مرتكبيها بهدف تحقيق الأمن السيبراني، وهو ما نستشفه من القانون رقم 09/04 المتعلق بالجرائم المتصلة بتكنولوجيا الإعلام والاتصال، كما تهدف دراسة **دايرى لبنى & , بن خليف سارة** (2023)[24] إلى التعرف على الجريمة السيبرانية من حيث ماهيتها، وخصائصها وأهمية الحماية الجنائية للمعلومات من السلوكيات الإجرامية التي قد تقع عليها، وإيضاح السلوكيات المتبعة من طرف المجرم السيبراني التي ارتكبت سواء بواسطة المعلوماتية أو تكنولوجيا المعلومات، التي أثبتت النصوص التقليدية فشلها في محاربة هذه السلوكيات، وتعرضت الدراسة لموقف المشرع الجزائري في مجال مكافحة الجريمة السيبرانية وكيفية معالجته لها ضمن القانون الجنائي الوطني، وذلك من خلال القانون 04-15 من قانون العقوبات والمتعلق بالمساس بأنظمة المعالجة الآلية للمعلومات والقانون 09-04، المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الإعلام والاتصال ومكافحتها، حيث أفرد المشرع بعض الإجراءات والوسائل لمحاربة هذا السلوك المستحدث.

واهتمت دراسة Zafar Abbas , et al (2023)[25] بالقوانين السيبرانية والإعلامية التي أحدثت تغيرات جذرية في تكنولوجيا المعلومات وفي جميع قطاعات المجتمع، ولكن الجانب السلبي لهذا التقدم هو ظهور الجرائم الرقمية، المعروفة باسم الجرائم الافتراضية، فضلًا عن تكثيف الجرائم التقليدية من خلال التقنيات الناشئة، إضافة إلى السلوك الإجرامي خاصة تأثيراته المتعددة مقارنة بالماضي، حيث لا توجد جريمة أو مجرم مقيد بالحدود الوطنية أو القيود الجغرافية، ولا شك أن البلاد أكثر اندفاعاً لاتباع تكنولوجيا المعلومات والاتصالات، ولكنها في الوقت نفسه تسعى لإيجاد وسائل لمواجهة السلبيات، ويتم حاليًا استخدام الخطوات القانونية، جنبًا إلى جنب مع التدابير التكنولوجية، لحماية شبكات المعلومات وتثبيط وتجنب النشاط غير القانوني، وقد تم

اعتماد قوانين الجرائم الافتراضية للسيطرة على الجرائم الرقمية ومكافحة مجرمي الإنترنت الناشئين، وملاحظة عديد من التطورات والابتكارات في هذا الصدد على المستوى العالمي خاصة في العقد الماضي، وألقت دراسة Ian , Sheetal Kumar Andrew Barber (2023)[26] الضوء على مفاوضات الأمم المتحدة لتطوير اتفاقية الجرائم الافتراضية في عام 2022، وتهتم الدراسة بتأثير تشريعات الجرائم الإلكترونية على حقوق الإنسان، بما في ذلك الآثار الإيجابية والسلبية للتدابير المتخذة في معالجة الجرائم الافتراضية، كما تقدم أمثلة لمجالات تشريعات الجرائم الافتراضية (على سبيل المثال فيما يتعلق بنطاق التجريم والسلطات الإجرائية) التي تشكل جزءاً من المناقشات الخاصة بالاتفاقية وتشرح كيف تؤثر على حقوق الإنسان، ودور المجتمع المدني في دعم تطوير الأطر والاستجابات للجرائم الافتراضية التي تعزز حقوق الإنسان وتحميها، وتقدم الدراسة دراسات حالة من مناطق مختلفة، وتسلط الضوء على كيف يمكن لخبرة المجتمع المدني أن تدعم بشكل مباشر تطوير مناهج تحترم الحقوق في التعامل مع الجرائم الإلكترونية، كما تقدم الدراسة توصيات للدول الأعضاء وأصحاب المصلحة الآخرين، ووضع أداة تحترم الحقوق وتعالج الجرائم الافتراضية بشكل فعال بطريقة تحترم الحقوق.

وتناولت دراسة Masduki (2022)[27] الهجمات الإلكترونية على وسائل التواصل الاجتماعي وتأثيرها على حرية الإعلام في إندونيسيا، من خلال تحليل متعمق للهجمات الرقمية التي أجريت قبل وبعد الانتخابات الرئاسية لعامي 2014 و2019، التي نشر خلالها معلومات مضللة، وشنت حرباً إلكترونية لتحقيق أهداف سياسية، وتوضح هذه الدراسة انتهاك الهجمات الرقمية بشكل متزايد وتأثيرها على استقلالية وسائل الإعلام وإعاقة خدمتها للمصلحة العامة.

وتهتم دراسة **زناتى, محمد السعيد, جواج & يمينة** (2022)[28] بمكافحة الجرائم السيبرانية بالتشريع الجزائري كقانون 04-09 المتضمن القواعد الخاصة لوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، أو التعديلات الواقعة على قانون العقوبات الجزائري بموجب القانونين 04-15، 06-23، وعلى الرغم من ذلك،

فإن المنظومة القانونية في التشريع الجزائري ما زالت دون الحد الكافي لتأطير هذه العملية بما يضمن الحماية للحقوق والحريات الخاصة للأفراد، نظراً للآثار السلبية الواقعة على هذه الأخيرة جراء تغليب مصلحة وسلامة كيان الدولة على الحريات الفردية الخاصة، كما أجرت دراسة Ryan Shandler ,et al (2021)[29] تجربتين مسحيتين على عينة تقدر بـ 2585 مفردة لفحص الدعم للجرائم السيبرانية مقابل الضربات العسكرية التقليدية في الولايات المتحدة والمملكة المتحدة وإسرائيل، في الدراسة الأولى، وعرض على المستجيبين تقارير إخبارية تلفزيونية تصور أشكالًا مختلفة من الهجمات الإرهابية، وتشير النتائج إلى أن الدعم العام العالي لنشر الأسلحة السيبرانية تبدد بالكامل بين المستجيبين المعرضين لهجمات سيبرانية قاتلة، وفي الدراسة الثانية، تم كشف الدعم المتلاشي، ووجد أن التعرض للهجمات السيبرانية المدمرة يقوض تصور الإنترنت كمجال أقل فتكًا، ومن ثمَّ يقلل من جاذبيته، وأخيراً كيفية تشجيع التفضيل العام الهش للأسلحة السيبرانية التصعيد العسكري في الأمد القريب.

واهتمت دراسة McCurdy,Michael (2020)[30] بدراسة تطور الجرائم الافتراضية والتشريعات الإلكترونية في نيجيريا لتحديد كيفية تطور الجرائم الافتراضية، والتأثير الذي أحدثته التشريعات الإلكترونية على فعالية إنفاذ القانون وجهود الحد من الجريمة، علاوة على تأثيرها على المكانة الاقتصادية العالمية لنيجيريا، خاصة نتيجة تأخر التشريعات السيبرانية النيجيرية، ولم تواكب التهديدات السيبرانية الجديدة، حيث وصف منتقدو قانون الجرائم السيبرانية لعام 2015، كونه جزءاً رئيسياً من التشريعات النيجيرية التي مهدت الطريق لتطبيق الأمن السيبراني، حيث يعد القانون غير فعال في أفضل الأحوال وخطير في أسوأ الأحوال، ليس فقط على حقوق الخصوصية للنيجيريين، ولكن أيضًا يشكل تهديداً للصحافة النيجيرية الحرة، واهتمت دراسة Masood, Ummi Hani Binti (2017)[31] بطبيعة الجرائم الافتراضية بموجب قانون ماليزيا والقانون الدولي، وتستخدم الأنطولوجيات لتحليل ظاهرة الهجمات الافتراضية في المؤسسات الحكومية ومنها المؤسسات الإعلامية، من خلال البحث في المعايير الدولية فيما يتعلق بالهجمات الافتراضية، وفحص فعالية ونزاهة

القانون الدولي في التعامل مع الهجمات الإلكترونية، وتظهر النتائج وجود اختلافات في تصور الهجمات الافتراضية على المستوى الوطني والدولي، حيث تؤثر الثقافة الاجتماعية والسياسية في ماليزيا على فهم الهجمات الافتراضية والتدابير المتخذة لمواجهتها، وأكدت **دراسة** Corlane Barclay (2017)[32] على زيادة الوعي بقانون الجرائم الافتراضية لعام 2015 في جامايكا، التي تم فحصها من خلال اتفاقية الجرائم الافتراضية، وتوصلت الدراسة إلى أن قوانين الجرائم الإلكترونية في جامايكا عبارة عن جملة من التشريعات ذات الصلة التي يجب أخذها في الاعتبار في أي تحليل لمكافحة الجرائم الافتراضية.

التعليق على الدراسات السابقة:

1- اهتمت دراسات المحور الأول بالتشريعات السيبرانية المنظمة للأنشطة المتعلقة بالفضاء السيبراني، التي تناولت قوانين حماية البيانات الشخصية، وحقوق الملكية الفكرية، والجرائم السيبرانية، ومكافحة المحتوى الضار، وتنظيم قوانين البث، وقوانين الخصوصية، ومكافحة الأخبار الزائفة، وهنا يأتي دور هذه الدراسة لسد الفجوة في الدراسات العربية والأجنبية، حيث لا توجد دراسة واحدة تتناول أهمية التشريعات السيبرانية في بيئة الإعلام الرقمي، حيث تناولت الدراسات الأجنبية التشريعات السيبرانية في مجال حقوق الإنسان، والأمن القومي، والسلطات المحلية، والحوكمة، والاتحاد الأوروبي، والهند.

2- تناولت دراسات المحور الثاني الجرائم السيبرانية التي تحدث بشكل غير قانوني عبر الإنترنت وفي الفضاء الإلكتروني، ومنها القرصنة، وتزييف الحقائق، وتضليل المعلومات، والهجمات على البنية التحتية، والتجسس الإلكتروني، وانتهاك حقوق الملكية الفكرية، والتصيد الاحتيالي.

3- تبين من واقع القراءة المتأنية التحليلية المقارنة بين المحاور السابقة، تهتم بالتنويع بين أدوات جمع البيانات، ويأتي في أغلبها الدراسة التحليلية لقوانين وتشريعات الأمن السيبراني بين الدول وبعضها، وما بين المقابلة المتعمقة مع خبراء ومتخصصين في مجال الأمن السيبراني للتعرف على قوانين وتشريعات الأمن السيبراني دولياً.

4- التعرف على الإطار النظري للدراسة، المتمثل في نظرية دافع الحماية.

5- تحديد منهجية علمية سليمة تتلاءم وموضوع الدراسة.

6- تحديد المشكلة البحثية للدراسة وصياغتها على نحو يحقق تكاملًا معرفيًا ومنهجيًا بين هذه الدراسة والدراسات سابقة الذكر.

7- تأتي الدراسة الحالية لتضيف ما أغفلته الدراسات السابقة في تناول التشريعات السيبرانية التي تنظم طبيعة العمل الإعلامي والتي كثيراً ما أغفلته الدراسات العربية والأجنبية معًا.

8- التعرف على القوانين المنظمة للفضاء السيبراني التي ساعدت الباحثة على صياغة مسودة تشريعية سيبرانية تنظم طبيعة العمل الإعلامي.

خامسا: الإطار النظري للدراسة:

نظرية دافع الحماية (PMT):

تنص نظرية دافع الحماية، لصاحبها Rogers، على اتخاذ أي إجراء للتغلب على الخوف يتأثر بحجم الحدث، واحتمالية وقوعه، وفعالية الاستجابة، ولن يتغلب الفرد على التهديد حتى يتجاوز مستوى التهديد الحد الذي يدركه، وينص الافتراض النظري للنظرية على وجود علاقة بين الخوف والسلوك، ولهذا الخوف والسلوك تأثيرٌ بالغ على تصور خبير الأمن السيبراني للهجمات الإلكترونية وفائدة أدوات وآليات الأمن المستخدمة[33]، وتقترح النظرية خمسة مفاهيم أساسية تؤثر على الأفراد الذين يعتزمون حماية أنفسهم: (1) الخطورة المُتصورة لحادث هجوم إلكتروني (على سبيل المثال، إصابة جهاز الكمبيوتر بفيروس نتيجة فتح مرفق بريد إلكتروني مشبوه)؛ (2)الاحتمال المُتصوّر للتعرض لهجوم ضار(مثل التعرض لهجوم عبر بريد إلكتروني تصيدي)؛ (3)فعالية الاستجابة المُتصوّرة (مثل تنفيذ الإجراءات الوقائية الموصي بها)؛ (4) الكفاءة الذاتية المُتصوّرة (مثل إيمان الموظف بقدرته على تنفيذ الإجراءات الموصوفة بنجاح)؛ (5) تكاليف الاستجابة (مثل الامتثال لسياسات أمن المعلومات للحد من خروقات الأمن)[34].

ويُراعي الموظف خطورة التهديد واحتمالية وقوعه قبل اتخاذ أي إجراء، وإذا بدأ التهديد ضئيل الأهمية أو غير محتمل الحدوث، فقد يتجاهله الفرد، وحاولت نظرية دافع

الحماية شرح كيف يمكن مساعدة الصحفيين في التغلب على المخاوف المتعلقة بالأمن السيبراني، ويختلف الأفراد في تصوراتهم للخوف والدافع الفردي لاتخاذ إجراء حماية، ووجود إطار عمل لفهم دوافع الفرد يمكن أن يساعد على تعديل استجابات الصحفي وتشجيعه على اتخاذ الإجراءات الوقائية المطلوبة، كما تُقدم رؤيةً ثاقبةً حول أسباب عدم اتخاذ مستخدمي الحاسوب إجراءات وقائية، مثل إجراء النسخ الاحتياطية، واتباع سياسات المؤسسة، واستخدام برامج مكافحة الفيروسات[35]، وقد لا ينفذون إجراءات وقائية إلا إذا أدركوا أن التهديد مهم، ومحتمل الحدوث، ويمكن أن يُسبب أضراراً مُحددة، كما إن زيادة الوعي بأمن المعلومات يزيد من دوافع المستخدمين وامتثالهم، ويمكن للإجراءات الوقائية التي يتخذها المستخدم أن تخفف من حدة بعض هجمات الحاسوب، مثل هجمات برامج الفدية، إذا كان المستخدمون على دراية باحتمالية وقوع الهجمات وشدتها المحتملة، ويمكن لدراسة دوافع الحماية التي يستخدمها متخصصو أمن معلومات المؤسسات الصحفية والإعلامية أن تساعد في تحديد ما إذا كانت المؤسسة تستخدم دوافع حماية مناسبة لتشجيع الصحفيين بشكل كاف على اتخاذ تدابير الأمن السيبراني المناسبة، ويمكن لنظرية دوافع الحماية أن تساعد الصحفيين على تطبيق أساليب أفضل للأمن السيبراني، من خلال زيادة توعية المستخدمين بخطورة التهديد واحتمالية وقوعه وفعالية الاستجابة لأمن المعلومات، كما يمكن للمؤسسة تحسين فعالية الأمن السيبراني من خلال تحفيزهم بشكل أفضل[36].

وتوظف الدراسة الحالية نظرية دافع الحماية (PMT) لأهمية تزويد الصحفيين بنظام معلومات مؤسساتهم الصحفية، وأن الصحفي المُعرّض للخطر هو أكثر ميلًا لاتخاذ خطوات وقائية، ووفقًا لبعض الدراسات، فإن ضعف الصحفي المُدرك للهجمات الإلكترونية يُحفّز على الالتزام بلوائح الأمن السيبراني، والضعف المُدرك هو تقييم الصحفي لاحتمالية مواجهة مواقف مُهدّدة، مثل الوقوع ضحية لجريمة إلكترونية، علاوة على التأكيد بأهمية الإجراءات الوقائية التي يتخذها الصحفي داخل مؤسسته الصحفية بما يخفف من حدة بعض هجمات الحاسوب، مثل هجمات برامج الفدية، كما تساعد النظرية في تحديد ما إذا كانت المؤسسة الصحفية تستخدم دوافع حماية مناسبة لتشجيع

الصحفيين بشكل كاف على اتخاذ تدابير الأمن السيبراني المناسبة، ومساعدة الصحفيين على تطبيق أساليب أفضل للأمن السيبراني، مع زيادة توعيتهم بخطورة التهديد واحتمالية وقوعه وفعالية الاستجابة لأمن المعلومات.

سادسا: تساؤلات الدراسة الميدانية:

1- ما أهمية الأمن السيبراني في المؤسسات الصحفية والإعلامية؟

2- ما دور المؤسسات الإعلامية في العمل وفقًا لاستراتيجيات وبروتوكولات الأمن السيبراني؟

3- ما أهمية توعية الصحفيين بالتهديدات السيبرانية في المؤسسات الإعلامية والصحفية؟

4- ما آلية تدريب الصحفيين والموظفين على أطر استخدام وسائل التواصل الاجتماعي داخل مقار عملهم؟

5- ما التحديات التي تواجه الأمن السيبراني في المؤسسات الصحفية والإعلامية؟

6- ما المخاوف الأخلاقية التي يمكن ان يتسبب الأمن السيبراني في حدوثها بالمؤسسات الإعلامية؟

7- ما آليات الأمن السيبراني لإحباط الهجمات السيبرانية في مؤسساتهم الإعلامية؟

8- ما العوامل التي ينبغي على الصحفيين والإعلاميين في المؤسسات الصحفية والإعلامية مراعاتها عند اعتماد آليات الأمن السيبراني لإحباط الهجمات السيبرانية في مؤسساتهم؟

9- ما أهمية التشريعات السيبرانية التي تنظم بيئة الإعلام الرقمي؟

تساؤلات المقابلة المتعمقة:

1- ما أهمية الأمن السيبراني في المؤسسات الإعلامية؟

2- كيف يمكن اكتشاف التهديدات السيبرانية وطرق الوقاية منها؟

3- كيف يتم إدارة مخاطر الأمن السيبراني بالمؤسسات الإعلامية؟ وحماية البنية التحتية التي تستهدفها الجماعات الإرهابية؟

4- ما آليات حماية المعلومات والبيانات من الجرائم السيبرانية؟

5- ما العوامل التي ينبغي مراعاتها عند وضع الأيديولوجية الأخلاقية والمهنية للأمن السيبراني لمنع الجرائم الافتراضية في المؤسسات الإعلامية؟

6- كيف يتم تثقيف الإعلاميين بتهديدات الأمن السيبراني وإدارتها؟ وأسس تطبيق استراتيجيات الدفاع، أو التدابير المضادة؟

7- كيف يمكن للدولة المصرية التخفيف من مخاطر الأمن السيبراني التي تواجه وسائل الإعلام؟

8- كيف يتم التعاون الدولي لحماية الفضاء الإلكتروني لوسائل الإعلام من التهديدات السيبرانية؟

9- ما الأطر القانونية والتشريعات السيبرانية المنظمة لطبيعة العمل الصحفي والتي يمكن الخروج بها من الدراسة الحالية؟

سابعا: مفاهيم الدراسة والتعريفات الإجرائية:

التعريف الاصطلاحى (التشريعات السيبرانية): مجموعة قوانين قامت الحكومات في جميع أنحاء العالم بسنها لمعالجة التأثير العالمي للتهديدات السيبرانية، وتتمثل هذه الأطر القانونية في قانون الأمن السيبراني وCIA، وهي ليست مجرد أدوات بل هي دروع تهدف إلى تعزيز تدابير الأمن السيبراني وتسهيل الاستجابات الفعّالة للتهديدات السيبرانية وحماية البنية التحتية الحيوية، ويوفر وجودها شعوراً بالطمأنينة والحماية في مواجهة التهديدات السيبرانية[37].

التعريف الإجرائى (التشريعات السيبرانية): مجموعة القوانين المنظمة لطبيعة العمل الإعلامي في الفضاء السيبراني، تحدد حقوق وواجبات المستخدمين في الفضاء الإلكتروني، بغرض توفير إطار قانوني يحمي العمل الإعلامي من المخاطر المرتبطة بالجرائم السيبرانية، وتعزيز الثقة في استخدام التكنولوجيا الحديثة.

التعريف الاصطلاحى (الجريمة الافتراضية): أعمال غير قانونية، ينطوي ارتكابها على استخدام تكنولوجيا المعلومات والاتصالات، وهي أي جريمة جنائية أو غيرها من الجرائم التي يتم تسهيلها أو تنطوي على استخدام الاتصالات الإلكترونية أو أنظمة المعلومات بما في ذلك أي جهاز أو الإنترنت أو أي واحد أو أكثر منها[38]

التعريف الإجرائى (الجريمة الافتراضية): سلوكيات غير قانونية تنتهك الفضاء الإلكتروني، ويمتد تأثيرها إلى مختلف المجالات بما فيها المجال الإعلامي وتؤثر على الأفراد والمؤسسات والحكومات.

ثامنا: الخطوات المنهجية للدراسة:

نوع الدراسة:

تنتمي هذه الدراسة إلى الدراسات الاستكشافية الاستطلاعية، التي ابتكرها J. W. Tukey في ستينيات القرن العشرين، وتهتم الدراسات الاستكشافية بأهمية فهم عملية توليد البيانات التي تنتج البيانات المراد تحليلها، وكيف يمكن أن تؤدي إلى هيكلة البيانات بطرق مختلفة، أو إلى ظهور أخطاء بداخلها، ويعد هذا الاستكشاف للبيانات أمراً أساسياً لتوليد فرضيات حولها أو نماذج لتلخيصها، على عكس التأكيد أو الرفض اللاحق لهذه الفرضيات أو النماذج، ويعد التصور أمراً أساسياً في تحليل الدراسات الاستكشافية سواء الفحص الأولي للبيانات أو لعرض نتائج التحليل[39]، ويوصي Creswell and Creswell باتباع نهج نوعي للبحث عندما يكون الهدف هو فهم المشكلة بشكل أعمق، ويكون الموضوع جديداً، ولا توجد نظريات كافية لمعالجته[40]، وتعتمد الدراسات الاستكشافية على أدوات البحث المتنوعة ومنها الاستبيان، والمقابلات المتعمقة التي يتم الاستعانة بها في تحليل الرؤي ووجهات النظر المختلفة للخروج بمسودة قانون للتشريعات السيبرانية للجرائم الافتراضية في بيئة الإعلام الرقمي.

منهج الدراسة:

تنتمي هذه الدراسة إلى منهج المسح الإعلامي، الذي يعد أحد الأساليب البحثية المستخدمة في تحليل ودراسة ظاهرة أو موضوع ما من خلال جمع بيانات ومعلومات حول موضوع الدراسة، والوصول إلى استنتاجات أو توصيات محددة، وتُركز هذه الدراسة على التهديدات المحتملة التي قد تظهر في الهجمات السيبرانية، والاستراتيجيات المُمكنة للتخفيف من حدتها، وتأثير الوعي ببروتوكولات الأمن السيبراني على الإدارة الفعالة لهذه التهديدات للحد من مخاطرها المحتملة على المؤسسات الإعلامية والصحفية، وفي إطار الدراسة الحالية قامت الباحثة بوصف ورصد وتحليل التشريعات السيبرانية

المنظمة للفضاء السيبراني لحماية المؤسسات الإعلامية ضد الأنشطة السيبرانية الخبيثة والاهتمام بدعم الديمقراطية دون المساس بالحريات الرقمية، وتحصين البنية التحتية للمجلس الأعلى للإعلام من الجرائم الافتراضية.

أدوات جمع البيانات:

اعتمدت الدراسة على أداة الاستبيان الإلكتروني على عدد من مديرى أمن تكنولوجيا المعلومات بالمؤسسات الصحفية والإعلامية، علاوة على أداة المقابلة المتعمقة مع عينة من الخبراء والأكاديميين في العمل الصحفي والمتخصصين في الأمن السيبراني.

عينة الدراسة: تنقسم عينة الدراسة الميدانية إلى تطبيق الاستبيان الإلكتروني مع عدد (72) من مديرى أمن تكنولوجيا المعلومات بالمؤسسات الصحفية والإعلامية، خاصة وأن أفراد هذه الإدارة هي الجهة المنوطة بحماية المؤسسات الإعلامية من أية هجمات سيبرانية والحفاظ على معلوماتها وأخبارها من القرصنة، والحفاظ على منصاتها على مواقع التواصل الاجتماعي من التصيد ونشر أخبار زائفة، وبغرض تطبيق أفضل ممارسات الأمن السيبراني في المؤسسات الصحفية والإعلامية، وتثقيف صانعي القرار والصحفيين في هذه المؤسسات من خلال توفير المعلومات والأدوات التي تُمكّن من حماية معلوماتها وبياناتها، خاصة وانه مع تزايد تعقيد الهجمات الإلكترونية، ستظل المؤسسات الصحفية تواجه عدداً من التحديات.

ويمثل الجدول الآتي الخصائص الديموغرافية لعينة الدراسة الميدانية:

جدول (1) الخصائص الديموغرافية لعينة الدراسة الميدانية

الخصائص الديموغرافية		ك	٪
النوع	ذكر	65	90.3
	أنثى	7	9.7
العمر	من 20 إلى 30 عاما	9	12.5
	من 31 إلى 40 عاما	39	54.2
	من 41 إلى 50 عاما	22	30.6
	من 51 فيما فوق	2	2.8
الدرجة العلمية	مؤهل عال	64	88.9
	حاصل على ماجستير	8	11.1
	حاصل على دكتوراة	-	0.0
سنوات الخبرة في مجال تكنولوجيا المعلومات	من 5 إلى 10 سنوات	4	5.6
	من 11 سنة إلى 15 سنة	23	31.9
	من 16 سنة إلى 20 سنة	36	50
	من 21 فيما فوق	9	12.5
الإجمالى		72	٪100

كما أجرت الباحثة عدداً من المقابلات المتعمقة مع مجموعة من الخبراء والأكاديميين في العمل الصحفي وفي مجال تكنولوجيا الإعلام والأمن السيبراني والإعلام، ممثلة في عينة مكونة من 18 خبيراً منقسمين إلى عدد (9) من خبراء العمل الصحفي، وعدد (9) من أساتذة الإعلام والحاسبات والمعلومات والحقوق، والمتخصصين في مجال الأمن السيبراني[41]، بهدف اكتساب فهم أعمق من المشاركين في المقابلات، وفهم أفضل للوضع الراهن للتهديدات السيبرانية، مع التركيز بشكل خاص على مجال الأمن السيبراني، ويكمن مبرر استخدام المقابلات وهذا النوع من البيانات لتوليد المعلومات ووجهات النظر في تطوير فهم متعمق لتصورات المشاركين للمخاطر السيبرانية، والآثار المترتبة عليها داخل المؤسسات الإعلامية.

نتائج الدراسة الكمية (ميدانية):

تسعى الدراسة الميدانية للإجابة عن التساؤلات الآتية:

- **أولًا: أهمية الأمن السيبرانى في المؤسسات الصحفية والإعلامية:**

جدول (2) أهمية الأمن السيبرانى في المؤسسات الصحفية والإعلامية

أهمية الأمن السيبرانى	ك	٪
حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية	10	13.9
يؤدي الأمن السيبرانى دورا مهما في حماية الأصول الرقمية والمعلومات الحساسة لمؤسساتهم الصحفية	9	12.5
تُسبب الهجمات الإلكترونية اضطرابات كبيرة، مما يؤدي إلى الإضرار بالسمعة المؤسسية	13	18.1
يعدّ تخفيف مخاطر الأمن السيبرانى أمرا ضروريا لحماية المؤسسات الإعلامية والصحفية والموظفين من هجمات الأمن السيبرانى	3	4.2
ضرورة قصر الوصول إلى المعلومات الحساسة على موظفى المؤسسة الإعلامية الذين لديهم ضرورة قصوى لذلك	4	5.6
يمكن ان تتخذ الحوادث السيبرانية أشكالًا مختلفة، بما في ذلك انتهاكات البيانات، أو تلوث البرمجيات الخبيثة، أو حوادث رفض الخدمة	10	13.9
إجراء تقييمات دورية للثغرات الأمنية	12	16.7
ضرورة وجود خطة استجابة واضحة المعالم للجرائم السيبرانية لإدارة التهديدات المتنوعة بالمؤسسات الصحفية	11	15.3
الإجمالى	72	٪100

توضح نتائج الجدول السابق أهمية الأمن السيبراني في المؤسسات الصحفية والإعلامية، وتتمثل في تسبب الهجمات الإلكترونية اضطرابات كبيرة، مما يؤدي إلى الإضرار بالسمعة المؤسسية بنسبة 18.1٪ في المرتبة الأولى، يليها ضرورة إجراء تقييمات دورية للثغرات الأمنية بنسبة 16.7٪، يليها أهمية وجود خطة استجابة واضحة المعالم للجرائم السيبرانية لإدارة التهديدات المتنوعة بالمؤسسات الصحفية بنسبة 15.3٪، يليها حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية، ويمكن أن تتخذ الحوادث السيبرانية أشكالًا مختلفة، بما في ذلك انتهاكات البيانات، أو تلوث البرمجيات الخبيثة، أو حوادث رفض الخدمة بنسبة واحدة ممثلة في 13.9٪، يليها دور الأمن السيبراني في حماية الأصول الرقمية والمعلومات الحساسة لمؤسساتهم الصحفية بنسبة 12.5٪، يليها ضرورة قصر الوصول إلى المعلومات الحساسة على موظفي المؤسسة الإعلامية الذين لديهم ضرورة قصوى لذلك بنسبة 5.6٪، وأخيراً يعدّ تخفيف مخاطر الأمن السيبراني أمراً ضرورياً

لحماية المؤسسات الإعلامية والصحفية والموظفين من هجمات الأمن السيبراني بنسبة 4.2٪.

ويمكن القول بأن وعي موظفي إدارة تكنولوجيا المعلومات بالمؤسسات الصحفية والإعلامية على دراية كبيرة بالهجمات الإلكترونية التي تسبب اضطرابات كبيرة بالمؤسسات الإعلامية، مما يؤدي إلى الإضرار بالسمعة المؤسسية، وأصبح الأمن السيبراني جانبًا أساسيًا في عالمنا الرقمي، وهو حماية الأنظمة المتصلة بالإنترنت، بما في ذلك الأجهزة والبرامج والبيانات، من السرقة أو التلف أو الوصول غير المصرح به، ومع تزايد التقدم التكنولوجي واستخدام الإنترنت في جميع جوانب حياتنا، أصبح الأمن السيبراني جانبًا حيويًا للحفاظ على أمان معلوماتنا، ويمثل الأمن السيبراني أمرًا أساسيًا للحماية من الهجمات السيبرانية، مثل البرامج الضارة والتصيد الاحتيالي والقرصنة، كما يُمكن أن تُسبب هذه الهجمات أضرارًا جسيمة للمؤسسات والأفراد، مما يؤدي إلى فقدان البيانات الحساسة والتسبب في خسائر مالية فادحة.

- **ثانيا: دور المؤسسات الإعلامية في العمل وفقًا لاستراتيجيات وبروتوكولات الأمن السيبراني:**

جدول (3) دور المؤسسات الإعلامية في العمل وفقًا لاستراتيجيات وبروتوكولات الأمن السيبراني

استراتيجيات وبروتوكولات الأمن السيبراني	ك	٪
يجب على المؤسسات الصحفية اعتماد استراتيجية قيادية تُعطى الأولوية لموقفها المتعلق بالأمن السيبراني	14	19.4
تطبيق بروتوكولات أمنية قوية، مثل التشفير وضوابط الوصول	10	13.9
يجب أن تُعطى استراتيجية أو سياسة وسائل التواصل الاجتماعى الأولوية لتوجيه الصحفيين بشأن استخدام وسائل التواصل الاجتماعى.	12	16.7
أن تراجع المؤسسات الصحفية إجراءاتها الأمنية وتحديثها بانتظام لضمان مواكبتها لأحدث التهديدات.	11	15.3
الاعتماد على الاستراتيجية الخمسية الوطنية المصرية للأمن السيبرانى ٢٠٢٣-٢٠٢٧	6	8.3
تنفيذ استراتيجيات الدفاع الأمنى بناء على نقاط الضعف المحددة	7	9.7
اعتماد استراتيجيات استباقية، مثل عمليات التدقيق الدورية وتقييمات التهديدات، يؤدي دورا حاسما في التخفيف من المخاطر للتكامل مع برامج الأمن السيبرانى	12	16.7
الإجمالى	72	٪100

تشير نتائج الجدول السابق إلى دور المؤسسات الإعلامية في العمل وفقًا لاستراتيجيات وبروتوكولات الأمن السيبراني وتتمثل في ضرورة اعتماد المؤسسات الصحفية على استراتيجية قيادية تُعطي الأولوية لموقفها المتعلق بالأمن السيبراني بنسبة 19.4٪، يليها ضرورة أن تُعطي استراتيجية أو سياسة وسائل التواصل الاجتماعي الأولوية لتوجيه الصحفيين بشأن استخدام وسائل التواصل الاجتماعي، وتتساوى في النسبة مع اعتماد استراتيجيات استباقية، مثل عمليات التدقيق الدورية وتقييمات التهديدات، يؤدي دوراً حاسماً في التخفيف من المخاطر للتكامل مع برامج الأمن السيبراني بنسبة 16.7٪، يليها ضرورة مراجعة المؤسسات الصحفية لإجراءاتها الأمنية وتحديثها بانتظام لضمان مواكبتها لأحدث التهديدات بنسبة 15.3٪، يليها تطبيق بروتوكولات أمنية قوية، مثل التشفير وضوابط الوصول بنسبة 13.9٪، يليها تنفيذ استراتيجيات الدفاع الأمني بناءً على نقاط الضعف المحددة بنسبة 9.7٪، وأخيراً الاعتماد على الاستراتيجية الخمسية الوطنية المصرية للأمن السيبراني ٢٠٢٣-٢٠٢٧. بنسبة 8.3٪.

ويمكن القول بأنه مع تحوّل صناعة الإعلام نحو التقنيات الرقمية، وجب تطبيق تدابير أمنية سيبرانية فعّالة وبروتوكولات أمن سيبرانية للحماية من الهجمات الإلكترونية المحتملة باتباع أفضل الممارسات والامتثال للوائح حكومية، حيث تعقد المؤسسات الصحفية بروتوكولات واستراتيجيات محددة في حالة وقوع حادث أمن سيبراني، وتحدد هذه البروتوكولات تسلسل الإجراءات الواجب اتخاذها، بما في ذلك العزل الفوري للأنظمة المتأثرة، والتحقيق في مصدر الاختراق، وتنفيذ تدابير التخفيف لاحتواء التهديد، ويعتُبر الوضوح والهيكلية في هذه البروتوكولات أمراً أساسياً، لضمان اتساق الاستجابات وفعاليتها، ويُمكن للمؤسسات الصحفية تعزيز أمنها وتقليل مخاطر التهديدات السيبرانية من خلال اعتماد استراتيجيات استباقية للتكامل مع برامج الأمن السيبراني، بحيث لا تقتصر على الأبعاد التكنولوجية للأمن السيبراني فحسب، بل تأخذ أيضاً في الاعتبار التداعيات الاجتماعية والقانونية والأخلاقية المرتبطة بهذا المجال، وتؤدي الاستراتيجيات الاستباقية، مثل عمليات التدقيق الدورية وتقييم التهديدات دوراً حاسماً في التخفيف من

المخاطر السيبرانية (مثل اتخاذ موقف استباقي، مصحوباً بوعي يقظ بمشهد التهديدات المتطور) حيث يُعدّ عاملًا أساسيًا في حماية المؤسسات الصحفية من المخاطر السيبرانية.

وتوجد عديد من الأدلة التي تعزز ضرورة اعتماد المؤسسات الصحفية على استراتيجية قيادية تُعطي الأولوية لموقفها المتعلق بالأمن السيبراني، ومنها عندما نشر موقع " The Intercept" تقريرًا سريًا سرّبته "Reality Winner " في عام ٢٠١٧[42]، المتعاقدة السابقة مع وكالة الأمن القومي، ويتناول التدخل الروسي في الانتخابات الأمريكية عام ٢٠١٦، وتشمل هذه القضية "The Intercept" و"Reality Winner "، ووكالة الأمن القومي، ووزارة العدل الأمريكية، وهي تغطي التسلسل الزمني من حصول " Reality Winner" على الوثائق حتى اعتقالها والتداعيات اللاحقة على "The Intercept"، حيث اطلعت "Reality Winner" على وثيقة سرية وطبعتها أثناء عملها كمتعاقدة مع وكالة الأمن القومي، إلى أن حدث سهوٌ أمنيٌ سمح لشركة وينر بسحب مواد سرية من منشأة آمنة، وألقت الضوء على أوجه القصور في إجراءات الأمن المادي والرقمي لوكالة الأمن القومي، كما يُغطّي التقرير بعض الحقائق التي قادت المحققين مباشرةً إلى " Winner، وتم الكشف عن معلومات حساسة، ورؤى مهمة في التدخل بالانتخابات، وألقت الضوء على الدور الحاسم للصحافة في كشف الحقائق الخفية، وأثار هذا التسريب نقاشات واسعةً حول الإجراءات الأمنية التي تُطبّقها الجهات الإعلامية عند التعامل مع الوثائق الحساسة والمُسرّبة، والتي كشفت المصدر عن غير قصد، كما أدى تسريب "Winner إلى تداعيات قانونية سريعة، وتم اعتقالها والحكم عليها بالسجن لأكثر من نصف عقد، وهي أطول عقوبة على الإطلاق تُفرض على الإطلاق بتهمة الإفصاح غير المصرح به عن بيانات حكومية لوسائل الإعلام في ذلك الوقت، وهذا يشير بشكل واضح إلى الحاجة إلى تنظيم بروتوكولات أمنية أكثر صرامةً في الإعلام.

● **ثالثًا: أهمية توعية الموظفين والصحفيين بالتهديدات السيبرانية في المؤسسات الإعلامية والصحفية:**

جدول (4) أهمية توعية الصحفيين بالتهديدات السيبرانية

توعية الصحفيين بالتهديدات السيبرانية	ك	٪
ضرورة توفير التدريب للصحفيين حول كيفية حماية أنفسهم والمؤسسة من التهديدات السيبرانية	19	26.4
أهمية الحصول على برامج أو دورات تدريبية مقترحة لتعليم الصحفيين كيفية استخدام منصات التواصل الاجتماعي بشكل صحيح	21	29.2
وضع سياسة أمنية لتطبيق إجراءات التخفيف من المخاطر السيبرانية	9	12.5
تثقيف الصحفيين بالمخاطر المحتملة المرتبطة ببيانات المؤسسة الإعلامية وشبكاتها	11	15.3
أن تشتمل برامج التوعية بالأمن السيبرانى على تقنيات وعمليات لحماية سرية وتوافر أنظمة الحاسوب والبيانات من الهجمات السيبرانية أو الوصول غير المصرح به	12	16.7
الإجمالى	72	٪100

توضح نتائج الجدول السابق مدى أهمية توعية الصحفيين بالتهديدات السيبرانية في المؤسسات الإعلامية والصحفية والتي تتمثل في أهمية الحصول على برامج أو دورات تدريبية مقترحة لتعليم الصحفيين كيفية استخدام منصات التواصل الاجتماعي بشكل صحيح بنسبة 29.2٪، يليها ضرورة توفير التدريب للصحفيين حول كيفية حماية أنفسهم والمؤسسة من التهديدات السيبرانية بنسبة 26.4٪، يليها ضرورة أن تشتمل برامج التوعية بالأمن السيبراني على تقنيات وعمليات لحماية سرية وتوافر أنظمة الحاسوب والشبكات والبيانات من الهجمات السيبرانية أو الوصول غير المصرح به بنسبة 16.7٪، يليها تثقيف الصحفيين بالمخاطر المحتملة المرتبطة ببيانات المؤسسة الإعلامية وشبكاتها بنسبة 15.3٪، يليها وضع سياسة أمنية لتطبيق إجراءات التخفيف من المخاطر السيبرانية بنسبة 12.5٪، ويمكن القول بأن التوعية بالأمن السيبراني جزءاً من أمن المعلومات بالمؤسسات الصحفية والإعلامية لتثقيف الصحفيين بالتهديدات السيبرانية الشائعة، مثل عمليات الاحتيال بالهندسة الاجتماعية، والتصيد الاحتيالي، وهجمات برامج الفدية (مثل Wanna Cry)، وغيرها من البرامج الضارة المصممة لسرقة الملكية الفكرية أو البيانات الشخصية.

وينبغي أن تسلط المؤسسات الصحفية والإعلامية الضوء على توعية الصحفيين لأنهم يُسلّطوا الضوء على قضايا تهمّ الرأي العام، والمصلحة العامة، مثل الحرب والإرهاب والفساد والجريمة، ويبدو أن قطاع الإعلام مُستهدفٌ للتضليل الإعلامي، أكثر من القطاعات الأخرى، وغالبًا ما يُستغلّ غياب التنظيم في وسائل التواصل الاجتماعي، ويتم التعرض لتقنيات المراقبة الإلكترونية الحديثة وغيرها من برامج التجسس، لذا وجب على الصحفيين أن يكونوا على دراية بالتهديدات السيبرانية المتعلقة بالمواقع الإعلامية وباستخدام وسائل التواصل الاجتماعي وحماية أصول المعلومات، حيث يتم تخزين المعلومات الشخصية، مثل أرقام الضمان الاجتماعي وتفاصيل الحسابات المصرفية ومعلومات بطاقات الائتمان، على منصات إلكترونية مُختلفة، ويقوم الأمن السيبراني بحماية هذه البيانات الحساسة من الوصول إليها من قِبل أشخاص غير مُصرّح لهم، مما يحمي الأفراد من سرقة الهوية.

كما يجب أن يتوقف الصحفيين والإعلاميين للتفكير قبل النقر على أي روابط في رسائل البريد الإلكتروني، مع ضرورة حذف التطبيقات الغير مستخدمة، واستخدام الرسائل التي تختفي عند الإمكان، وضرورة إعادة تشغيل الجهاز قبل إجراء مكالمة هاتفية حساسة، وإذا كانت بيانات الصحفي تُحفظ تلقائيًا على السحابة، فهذا يُعرّضها لتهديدات إضافية، علاوة على ضرورة استخدام أدوات التشفير وهو ما يعني تأمين البيانات والاتصالات بقفل رقمي أكثر أمانًا وقوة، وفي بعض الحالات، جعل الاتصالات مجهولة المصدر أو غير قابلة للتتبع من قِبل جهات خارجية، ويمكن استخدام برامج التشفير للبيانات أثناء نقلها أو تخزينها على جهاز للتواصل، وينصح باستخدام خدمة الرسائل الرقمية المشفرة Signal، ومن الأدوات الأخرى التي يوصي بها للتواصل مع المُبلغين عن المخالفات Secure Drop.

تعرّضت شركة Sony Pictures Entertainment في عام 2014، لهجوم إلكتروني ضخم من قِبل مجموعة تُدعى "حراس السلام"[43]، مما أدى إلى تسريب كمية هائلة من البيانات السرية، بما في ذلك رسائل بريد إلكتروني شخصية، وأفلام غير منشورة، وبيانات مُفصّلة عن الموظفين، وشمل الحادث جهات معنية، بما في ذلك مسؤولون تنفيذيون في Sony، ونجوم سينما، ومختلف وسائل الإعلام زعمت أن الاختراق من قِبَل

قراصنة من كوريا الشمالية، ومن خلاله تم استغلال ثغرات أمنية في أنظمة شبكات Sony، بما في ذلك عدم كفاية حماية كلمات المرور وتحديث البرامج القديمة، ولقد واجهت المؤسسات الإخبارية الكبرى صعوبة في تحديد ما إذا كان ينبغي نشر اتصالات شخصية حساسة من مسؤولي Sony التنفيذيين ومشاهيرها، وكان على وسائل الإعلام الموازنة بين إعلام الجمهور والضرر المحتمل الناجم عن انتهاك الخصوصية.

لذا يمكن أن يؤدي نقص التدريب على الأمن الرقمي في غرف الأخبار إلى آثار مُخيفة على المصادر الذين يخشوا بشكلٍ متزايد من انكشافهم عن غير قصد، وتُمثل هذه الأنماط انعدام ثقة الجمهور في سلامة البيانات الشخصية، بما في ذلك تلك الموجودة في أيدي ناشري الأخبار، وفي الحالات التي تكون فيها المصادر أقل وعيًا بمخاوف الأمن الرقمي، يتضح أن الصحفيين غالبًا ما يترددون في طلب تدابير الحماية خوفًا من إخافة المصادر، وتعد هذه التهديدات مكلفة ويصعب على غرف الأخبار معالجتها بمفردها.

- **رابعا: آلية تدريب الصحفيين والموظفين على أطر استخدام وسائل التواصل الاجتماعى داخل مقار عملهم وحماية أنفسهم من التهديدات السيبرانية:**

جدول (5) آلية تدريب الصحفيين على وسائل التواصل الاجتماعى

تدريب الصحفيين على استخدام وسائل التواصل الاجتماعى	ك	٪
التدريب على استخدام وسائل التواصل الاجتماعى لتوعية الصحفيين بحماية معلوماتهم وحماية المؤسسة من مخاطر الأمن السيبرانى	11	15.3
يجب على الصحفيين دائما اختيار إعدادات الخصوصية الأكثر صرامة عند استخدام وسائل التواصل الاجتماعى	9	12.5
يُمكّن تعطيل خاصية تحديد الموقع الحالى تجنبا من تتبع التركيبة السكانية الجغرافية للصحفيين	6	8.3
ينبغى للصحفيين اختيار كلمات مرور قوية ومميزة تُصعّب على القراصنة الوصول إلى حساباتهم على وسائل التواصل الاجتماعى	4	5.6
ينبغى للصحفيين الامتناع عن قبول طلبات الصداقة التى تبدو مشكوكًا فيها.	8	11.1
يجب أن تُشجع برامج التدريب في المؤسسة الصحفيين على توخى الحذر من المخططات الاحتيالية عند استخدام وسائل التواصل الاجتماعى أثناء ساعات العمل	7	9.7
اتخاذ إجراءات تأديبية ضد صحفييها لإساءة استخدام وسائل التواصل الاجتماعى خلال ساعات العمل.	10	13.9
تزويد الصحفيين بالمهارات اللازمة للتعرف على التهديدات السيبرانية المحتملة عبر وسائل التواصل الاجتماعى يمكن أن يقلل من فرص التعرض لهجوم سيبرانى	17	23.6
الإجمالى	72	٪100

توضح نتائج الجدول السابق آلية تدريب الصحفيين والموظفين على أطر استخدام وسائل التواصل الاجتماعي داخل مقار عملهم وكيفية حماية أنفسهم من التهديدات السيبرانية، وتتمثل في تزويد الصحفيين بالمعرفة والمهارات اللازمة للتعرف على التهديدات السيبرانية المحتملة عبر وسائل التواصل الاجتماعي يمكن أن يقلل بدرجة كبيرة فرص التعرض لهجوم سيبراني بنسبة23.6٪، يليه التدريب على استخدام وسائل التواصل الاجتماعي لتوعية الصحفيين بحماية معلوماتهم وحماية المؤسسة من مخاطر الأمن السيبراني بنسبة 153٪، يليه اتخاذ إجراءات تأديبية ضد صحافييها لإساءة استخدام وسائل التواصل الاجتماعي خلال ساعات العمل بنسبة 13.9٪، كما يجب على الصحفيين دائمًا اختيار إعدادات الخصوصية الأكثر صرامة عند استخدام وسائل التواصل الاجتماعي بنسبة 12.5٪، وينبغي للصحفيين الامتناع عن قبول طلبات الصداقة التي تبدو مشكوكًا فيها بنسبة 11.1٪، ويجب أن تُشجع برامج التدريب في المؤسسة الصحفيين على توخي الحذر من المخططات الاحتيالية عند استخدام وسائل التواصل الاجتماعي أثناء ساعات العمل بنسبة 97٪، كما يُمكّن تعطيل خاصية تحديد الموقع الحالي تجنبا من تتبع التركيبة السكانية الجغرافية للصحفيين بنسبة 8.3٪، وأخيرًا ينبغي للصحفيين اختيار كلمات مرور قوية ومميزة تُصعّب على القراصنة الوصول إلى حساباتهم على وسائل التواصل الاجتماعي بنسبة 5.6٪.

ينبغي أن تهتم المؤسسات الصحفي بتدريب الصحفيين على كيفية تحديد التهديدات المحتملة وتجنبها، إضافة إلى مراقبة نشاط وسائل التواصل الاجتماعي بحثًا عن أي سلوك مشبوه، وحماية الملكية الفكرية والبيانات الحساسة، وعند استخدام وسائل التواصل الاجتماعي، من الضروري إعطاء الأولوية لإعدادات الخصوصية على هذه الوسائل بما يُساعد على الحماية من سرقة الهوية، والوصول غير القانوني، وهجمات الهندسة الاجتماعية.

وتتضمن تحديات الأمن السيبراني التي تواجه وسائل الإعلام العالمية تهديدات واسعة النطاق فيما يتعلق بخصوصية البيانات وأمنها، بما في ذلك المخاوف المتزايدة بشأن ثغرات البرامج التي يستخدمها الصحفيين بشكل دائم، إضافة إلى استخدام مراقبة

المنصات الرقمية، على سبيل المثال، تسعى بعض الحكومات لتقليص حماية التشفير التي توفرها تطبيقات آمنة مثل Signal, WhatsApp, Proton Mail, Secure Drop، إضافةً إلى ثمة مخاوف تتعلق بالسلامة والخصوصية الرقمية على منصات التواصل الاجتماعي القديمة، مثل إكس (المعروفة سابقًا باسم تويتر)، وهي منصة أساسية في ممارسات الصحافة العالمية ومصادرها، حيث أصبحت البيانات والاتصالات أقل أمانًا للصحفيين ومنظمات المجتمع المدني في أعقاب تغييرات الملكية والبنية التحتية.

وينبغي أن تتضمن التدريبات آليات استخدام الصحفيين لكلمات المرور بمجموعة متنوعة من الأحرف، وتشمل الأحرف الخاصة والأرقام والأحرف الكبيرة والصغيرة، وذلك بغرض إنشاء كلمات مرور أكثر مقاومة لهجمات القوة الغاشمة ومحاولات الوصول غير المصرح به، علاوة على فرض قيود على استخدام الأرقام التسلسلية وحظر العبارات سهلة التخمين أو كلمات المرور الشائعة مثل "password123" أو "admin" ، ومن ثمَّ تمثل سياسات كلمات المرور القوية عنصرًا أساسيًا في آليات الحماية السيبرانية الخاصة بالصحفيين، وقد صُممت هذه السياسات السيبرانية لإنشاء خط حماية أولي قوي، يحمي من الوصول غير المصرح به والاختراقات المحتملة.

وتهدف برامج التدريب رفع مستوى وعي الصحفيين بالجوانب الأساسية للأمن السيبراني، بما في ذلك أهمية التحكم في الوصول، كما تهدف إلى غرس ثقافة الأمن السيبراني داخل المؤسسات الصحفية، فيصبح الصحفي مسهمًا فعالًا في تعزيز المعلومات الحساسة وفي أنظمة تكنولوجيا المعلومات، كما يعد الصحفي المطلع واليقظ خط دفاع أساسي ضد التهديدات المحتملة، إذ يمكن التعرف على حالات الأمن والاستجابة لها بفعالية.

وينبغي تثقيف الصحفيين بكيفية التعرف على محاولات التصيد الاحتيالي والاستجابة لها، وأهمية إجراء تدريبات محاكاة للتصيد الاحتيالي لتقييم مدى جاهزية الصحفيين وتعزيز وعيهم، وضرورة أن تركز برامج التدريب على ضمان فهم الصحفيين لسياسات وممارسات الأمن السيبراني المعمول بها ومدي التزامهم بها، مما يسهم في بناء ثقافة

تنظيمية واعية بالأمن السيبراني، ومن ثمَّ يستطيع أن يدرك الصحفي دوره الرئيسي في حماية المعلومات الحساسة.

كما تحرص المؤسسات الإعلامية الكبرى على تسليط الضوء باستمرار على برامج التدريب الخاصة بالأمن السيبراني كوسيلة لضمان إلمام الموظفين وتزويدهم بالمعلومات اللازمة للإسهام في تعزيز الوضع الأمني السيبراني للمؤسسة، وتشمل برامج التدريب الأمني مجموعة واسعة من الموضوعات، بما في ذلك أفضل ممارسات التحكم في الوصول، وأمن كلمات المرور، والالتزام بسياسات الأمن المعمول بها، وتهدف هذه التدريبات إلى تعزيز ثقافة الأمن السيبراني داخل المؤسسات الصحفية، وتثقيف الصحفيين بكيفية التعرف على التهديدات الأمنية المحتملة، وفهم أهمية التحكم في الوصول، علاوة على الالتزام ببروتوكولات الأمن السيبراني المقررة .

- **خامسا: التحديات التى تواجه الأمن السيبرانى في المؤسسات الصحفية والإعلامية:**

جدول (6) التحديات التى تواجه الأمن السيبرانى في المؤسسات الصحفية والإعلامية

التحديات التى تواجه الأمن السيبرانى	ك	٪
تطبيق تدابير صارمة للحماية من الهجمات الإلكترونية، وتقييم جاهزيتها في المجال الإعلامى	7	9.7
تعزيز قدرات المؤسسات الإعلامية على الصمود أمام التهديدات السيبرانية	6	8.3
تبنى تشريعات وبرامج أمنية خاصة بالأمن السيبرانى	10	13.9
استخدام تقنيات أمنية مثل أنظمة كشف ومنع التسلل عبر جدران الحماية، وفلاتر البريد العشوائى، وحلول مكافحة البرامج الضارة، ومكافحة الفيروسات للحماية من هجمات الأمن الإلكترونى	12	16.7
استخدام نص برمجى (أوامر حاسوبية) لجمع البيانات لمراقبة سلوك الصحفيين بطريقة فعالة لتعزيز مبادرات الأمن السيبرانى	6	8.3
حماية تسجيل الدخول والمصادقة لدى الصحفيين، ومصادقة البيانات، وفحص البرامج الضارة، وتطبيقات مكافحة الفيروسات، وجدران الحماية	3	4.2
التهديدات والاختراقات السيبرانية المستمرة التى تتعرض لها المؤسسات الإعلامية تجعل من تعزيز الأمن السيبرانى بشكل جيد ميزة تنافسية في قطاعاتها المعنية	8	11.1
افتقارها للموارد المالية اللازمة لتطبيق دفاعات قوية ضد الهجمات السيبرانية	9	12.5
زيادة نقاط ضعف الأمن السيبرانى في المؤسسات الصحفية والإعلامية	5	6.9
غياب تقييم المخاطر الداخلية السنوية لتقييم قيمة الضوابط الداخلية للمؤسسات الصحفية والإعلامية بناء على مستوى المخاطر	6	8.3
الإجمالى	72	٪100

تشير نتائج الجدول السابق إلى التحديات التي تواجه الأمن السيبراني في المؤسسات الصحفية والإعلامية، وتتمثل في استخدام تقنيات أمنية مثل أنظمة كشف ومنع التسلل عبر جدران الحماية، وفلاتر البريد العشوائي، وحلول مكافحة البرامج الضارة، ومكافحة الفيروسات للحماية من هجمات الأمن الإلكتروني بنسبة 16.7٪، يليه تبني تشريعات وبرامج أمنية خاصة بالأمن السيبراني بنسبة 13.9٪، يليه افتقارها للموارد المالية اللازمة لتطبيق دفاعات قوية ضد الهجمات السيبرانية بنسبة 12.5٪، يليها التهديدات والاختراقات السيبرانية المستمرة التي تتعرض لها المؤسسات الإعلامية تجعل من تعزيز الأمن السيبراني بشكل جيد ميزة تنافسية في قطاعاتها المعنية بنسبة 11.1٪، يليه تطبيق تدابير صارمة للحماية من الهجمات الإلكترونية، وتقييم جاهزيتها في المجال الإعلامي بنسبة 9.7٪، يليه تماثل تعزيز قدرات المؤسسات الإعلامية على الصمود أمام التهديدات السيبرانية واستخدام نص برمجي (أوامر حاسوبية) لجمع البيانات لمراقبة سلوك الصحفيين بطريقة فعالة لتعزيز مبادرات الأمن السيبراني وغياب تقييم المخاطر الداخلية السنوية لتقييم قيمة الضوابط الداخلية للمؤسسات الإعلامية بناءً على مستوى المخاطر بنسبة 8.3٪، يليه زيادة نقاط ضعف الأمن السيبراني في المؤسسات الإعلامية بنسبة 6.9٪، وأخيراً حماية تسجيل الدخول والمصادقة لدي الصحفيين، ومصادقة البيانات، وفحص البرامج الضارة، وتطبيقات مكافحة الفيروسات، وجدران الحماية بنسبة 4.2٪.

ويمكن القول بأن تغير مشهد التهديدات السيبرانية ساعد على زيادة اشكال الهجمات الإلكترونية التي تؤدي إلى اختراق البيانات وسرقتها، وسرقة الهوية بالمؤسسات الصحفية، كما يخترق مجموعات مجرمي الإنترنت الأكثر مهارة البنية التحتية الرقمية للمؤسسات الإعلامية الأكثر أمانًا باستخدام الذكاء الاصطناعي، ويعطل المتسللون الخدمات من خلال هجمات حجب الخدمة الموزعة (DDoS) أو هجمات التشويه، علاوة على برامج الدردشة الآلية التي سهّلت على مجرمي الإنترنت العثور على شفرات لإنشاء برامج ضارة مثل Chat GPT.

وتتخذ تهديدات الأمن السيبراني أشكالًا متعددة، بما في ذلك برامج التجسس المحلية والعابرة للحدود التي تزداد تعقيدًا، وهجمات حجب الخدمة (DDoS) والبرامج الضارة (وهي برامج خبيثة تُستخدم للوصول غير المصرح به إلى أنظمة تكنولوجيا المعلومات وتنتشر عبر الشبكة)، وبرامج الفدية (وهي برامج خبيثة يطلب فيها المهاجمون مبلغًا أو فدية مقابل استعادة الوصول)، وهجمات التصيد الاحتيالي، ويمكن أن تقف وراء هذه الأساليب مجموعة من الجهات الفاعلة، بما في ذلك الدول والسياسيون، والأفراد ذوي النفوذ، والشركات، والشبكات الإجرامية، والمنظمات المتطرفة.

- **سادسا: المخاوف الأخلاقية التى يمكن أن يتسبب الأمن السيبرانى في حدوثها بالمؤسسات الإعلامية:**

جدول (7) المخاوف الأخلاقية التى يمكن أن يتسبب الأمن السيبرانى في حدوثها

المخاوف الأخلاقية	ك	٪
اختراق خصوصية البيانات	3	4.2
تغيير الأخبار أو تحريفها على المواقع الإعلامية والصحفية	10	13.9
نشر أخبار زائفة على المواقع الإعلامية	17	23.6
سرقة روابط التواصل الاجتماعى للمؤسسات الإعلامية وتحريف اخبارها	11	15.3
الإضرار بالسمعة المؤسسية	8	11.1
ارتفاع الجرائم السيبرانية	5	6.9
الابتعاد عن مساءلة الجانى في الفضاء السيبرانى	4	5.6
انعدام الشفافية والنزاهة	8	11.1
انعدام سرية الأصول الرقمية وسلامتها	6	8.3
الإجمالى	72	٪100

توضح نتائج الجدول السابق المخاوف الأخلاقية التي يمكن أن يتسبب الأمن السيبراني في حدوثها بالمؤسسات الإعلامية، وتتمثل في نشر أخبار زائفة على المواقع الإعلامية بنسبة 23.6٪، يليها سرقة روابط التواصل الاجتماعي للمؤسسات الإعلامية الكبرى وتحريف أخبارها ومعلوماتها بنسبة 15.3٪، يليها تغيير الأخبار أو تحريفها على المواقع الإعلامية والصحفية بنسبة 13.9٪، يليها الإضرار السمعة المؤسسية، وانعدام الشفافية

والنزاهة بنسبة 11.1٪، يليها انعدام سرية الأصول الرقمية وسلامتها بنسبة 8.3٪، يليها ارتفاع الجرائم السيبرانية بنسبة 6.9٪، يليها الابتعاد عن مساءلة الجاني في الفضاء السيبراني بنسبة 5.6٪، يليها اختراق خصوصية البيانات بنسبة 4.2٪، وبذلك يمثل التداخل بين الصحافة والأمن السيبراني في عصرنا الرقمي أمرًا بالغ الأهمية، إذ يطرح تحديات فريدة ومعضلات أخلاقية.

ويتضح ذلك جليًا من تعرض اللجنة الوطنية الديمقراطية (DNC) في عام ٢٠١٦ لاختراق أمني كبير، حيث تم اختراق آلاف رسائل البريد الإلكتروني الخاصة بها وتسريبها، من خلال ويكيليكس[44]، وتمكن المُخترقون من الوصول إلى خوادم البريد الإلكتروني للجنة الوطنية الديمقراطية عبر هجمات تصيد إلكتروني مُعقدة، مستغلين ثغرات الأمن السيبراني، وأثّر هذا التسريب بشكل مباشر في الممارسات الصحفية، وأجبر المؤسسات الإخبارية على اتخاذ قرار سريع بشأن كيفية التعامل مع المعلومات المُسربة، إلى أن واجه الصحفيون تحديات أخلاقية كبيرة في اتخاذ قرار بشأن نشر رسائل البريد الإلكتروني المسروقة، حيث تم عقد مقارنة بين حق الجمهور في المعرفة والآثار الأخلاقية لنشر المعلومات المُخترقة، كما تضمنت عملية اتخاذ القرار توازنًا دقيقًا بين أهمية المحتوى الإخباري والاعتبارات الأخلاقية لاستخدام المواد التي تم الحصول عليها بوسائل غير مشروعة، واتبعت مختلف وسائل الإعلام مناهج متباينة، حيث اختار بعضها نشر تفاصيل مستفيضة من التسريبات، بينما اختارت أخرى تغطية أكثر تحفظًا، مما يُبرز غياب معيار موحد للتعامل مع مثل هذه المواقف، ودفعت هذه الحادث إلى إعادة تقييم المعايير الصحفية المتعلقة بالتعامل مع المعلومات المخترقة، مما أثر على السياسات والممارسات المستقبلية في غرف الأخبار بمختلف أنحاء العالم.

ومن هنا برزت الحاجة إلى وضع إرشادات ومعايير أوضح للتعامل مع التسريبات والمعلومات المخترقة، بهدف حماية نزاهة الصحافة والمعايير الأخلاقية، وفي أعقاب التسريب أطلقت السلطات الأمريكية تحقيقات لتحديد مدى التدخل الأجنبي، الذي أدى بدوره إلى مناقشات مستفيضة حول التداعيات القانونية للأمن السيبراني والصحافة، استجابةً لذلك الأمر، ينبغي أن تراجع وسائل الإعلام سياساتها المتعلقة بالتعامل مع

المعلومات المسربة، مع التركيز على الاعتبارات الأخلاقية وتحسين إجراءات الأمن السيبراني لمنع حدوث خروقات مماثلة.

- **سابعا: آليات الأمن السيبرانى لإحباط الهجمات السيبرانية في مؤسساتهم الإعلامية:**

جدول (8) آليات الأمن السيبرانى لإحباط الهجمات السيبرانية

إحباط الهجمات السيبرانية	ك	٪
ضرورة وضوح استراتيجية الحماية لمواجهة المخاطر التى تواجهها المؤسسات الصحفية.	11	15.3
التعاون مع مؤسسات خارجية مرموقة لتوفير خدمات سيبرانية فائقة الجودة	12	16.7
وضع خطة واضحة للتعاون مع فرق أخرى معنية بالأمن السيبرانى لاكتشاف الثغرات الأمنية الهيكلية في المؤسسات الصحفية	10	13.9
إدراك العوامل التى تساعد على تبنى آليات الأمن السيبرانى مما يعزز الدفاع السيبرانى في المؤسسات الصحفية	8	11.1
وجود فرق مخصصة للاستجابة للحوادث (IRTs) كعنصر أساسى في استراتيجيات للأمن السيبرانى	13	18.1
يحمى ضمان المعلومات البيانات والأخبار من الاختراقات، وسرقة الهوية، والفيروسات، وبرامج الفدية	10	13.9
تُساعد إعدادات الخصوصية على الحماية من سرقة الهوية، والوصول غير القانونى، وهجمات الهندسة الاجتماعية	8	11.1
الإجمالى	72	٪100

تبين نتائج الجدول السابق آليات الأمن السيبراني لإحباط الهجمات السيبرانية في مؤسساتهم الإعلامية ممثلة في وجود فرق مخصصة للاستجابة للحوادث (IRTs) كعنصر أساسي في استراتيجيات للأمن السيبراني بنسبة 18.1٪، يليه التعاون مع مؤسسات خارجية مرموقة لتوفير خدمات سيبرانية فائقة الجودة بنسبة 16.7٪، يليه ضرورة وضوح استراتيجية الحماية لمواجهة المخاطر التي تواجهها المؤسسات الصحفية بنسبة 153٪، يليه وضع خطة واضحة للتعاون مع فرق أخرى معنية بالأمن السيبراني لاكتشاف الثغرات الأمنية الهيكلية في المؤسسات الصحفية، ويحمي ضمان المعلومات البيانات والأخبار من الاختراقات، وسرقة الهوية، والفيروسات، وبرامج الفدية بنسبة 13.9٪، ثم إدراك العوامل التي تساعد على تبني آليات الأمن السيبراني مما يعزز الدفاع السيبراني في المؤسسات الصحفية، تُساعد إعدادات الخصوصية على الحماية من سرقة الهوية، والوصول غير القانوني، وهجمات الهندسة الاجتماعية بنسبة 11.1٪.

ويمثل وجود فرق مخصصة للاستجابة للحوادث (IRTs) عنصراً أساسياً في استراتيجيات المؤسسات الصحفية للأمن السيبراني (تتكون فرق الاستجابة للحوادث في المؤسسات الصحفية من محترفين مهرة، وتوفير تدريب وموارد مستمرة لهذه الفرق حول أفضل ممارسات الأمن السيبراني وإجراءات الاستجابة للحوادث، مما يساعدهم على استعادة العمليات بسرعة عند وقوع أي حادث، واستعادة النظام، واستعادة البيانات، والتحقق من صحة التدابير الأمنية لمنع تكرار الحادث)، وتعمل هذه الفرق على أساس أن الاستجابة السريعة والمنسقة ضرورية للحد من تأثير الاختراق ومنع تفاقمه إلى حادث أكثر شمولًا وضرراً، وتمثل الاستجابة الفعالة للحوادث والتعافي منها جزءاً لا يتجزأ من إدارة مخاطر الأمن السيبراني، كما تعزز من قدرة المؤسسة الصحفية على الصمود في مواجهة التهديدات المستقبلية، وبذلك تعد عمليات الاستجابة للحوادث عنصراً لا غنى عنه في استراتيجيات المؤسسات الإعلامية الشاملة للأمن السيبراني، حيث تعمل جنباً إلى جنب مع الإجراءات الوقائية لحماية مواردهم الرقمية ومعلوماتهم الحساسة.

- **ثامنا: العوامل التى ينبغى للصحفيين والإعلاميين في المؤسسات الصحفية والإعلامية مراعاتها عند اعتماد آليات الأمن السيبرانى لإحباط الهجمات السيبرانية في مؤسساتهم:**

جدول (9) العوامل التى ينبغى مراعاتها عند اعتماد آليات الأمن السيبرانى

اعتماد آليات الأمن السيبراني	ك	٪
اتباع بروتوكول القفل التلقائى لمحطات العمل بعد فترة محددة مسبقًا من عدم النشاط، وعادة ما تكون 10 دقائق	13	18.1
أهمية برامج معرفة المستخدم وفهمه في دعم الصحفيين لإنشاء وإدارة كلمات مرور آمنة وسهلة التذكر	11	15.3
أهمية إجراء عمليات تدقيق داخلية منتظمة لشبكاتهم وأنظمتهم وبروتوكولاتهم الأمنية	8	11.1
التحديث المنتظم للأنظمة والبرمجيات بالمؤسسات الإعلامية	9	12.5
الصحفيين المطلعون على الأمن السيبرانى يمثل خط دفاع أساسى ضد التهديدات المحتملة	8	11.1
منع الأفراد غير المصرح لهم من الوصول المادي إلى البنية التحتية الحيوية لتكنولوجيا المعلومات ومصادر المعلومات الحساسة	7	9.7
ضرورة فهم مختلف التكتيكات والاستراتيجيات التى يستخدمها مجرمو الإنترنت	5	6.9
أهمية البقاء على اطلاع بأحدث أساليب الهجوم في ظل بيئة الأمن السيبرانى المتطورة باستمرار كتهديدات شائعة يجب على المؤسسات الصحفية توخى الحذر منها	11	15.3
الإجمالى	72	٪100

توضح بيانات الجدول السابق العوامل التي ينبغي على الصحفيين والإعلاميين في المؤسسات الصحفية والإعلامية مراعاتها عند اعتماد آليات الأمن السيبراني لإحباط الهجمات السيبرانية في مؤسساتهم، وتتمثل في اتباع بروتوكول القفل التلقائي لمحطات العمل بعد فترة محددة مسبقًا من عدم النشاط، وعادةً ما تكون 10 دقائق بنسبة 18.1٪، يليها أهمية برامج معرفة المستخدم وفهمه في دعم الصحفيين لإنشاء وإدارة كلمات مرور آمنة وسهلة التذكر، وأهمية البقاء على اطلاع بأحدث أساليب الهجوم في ظل بيئة الأمن السيبراني المتطورة باستمرار كتهديدات شائعة يجب على المؤسسات الصحفية توخي الحذر منها بنسبة 15.3٪، يليها التحديث المنتظم للأنظمة والبرمجيات بالمؤسسات الإعلامية بنسبة 12.5٪، يليها أهمية إجراء عمليات تدقيق داخلية منتظمة لشبكاتهم وأنظمتهم وبروتوكولاتهم الأمنية، والصحفيين المطلعون على الأمن السيبراني يمثل خط دفاع أساسي ضد التهديدات المحتملة بنسبة 11.1٪، يليها منع الأفراد غير المصرح لهم من الوصول المادي إلى البنية التحتية الحيوية لتكنولوجيا المعلومات ومصادر المعلومات الحساسة بنسبة 9.7٪، وأخيراً ضرورة فهم مختلف التكتيكات والاستراتيجيات التي يستخدمها مجرمو الإنترنت بنسبة 6.9٪.

ويمكن للصحفيين اتباع بروتوكول القفل التلقائي لمحطات العمل بعد فترة محددة مسبقًا من عدم النشاط، وعادةً ما تكون10 دقائق (وقد شكّل هذا البروتوكول كضمان ضد الاختراقات المحتملة التي قد تنشأ عن محطات العمل غير المراقبة ومن خلال تطبيق القفل التلقائي لمحطات العمل، ويسعى الصحفيون للتخفيف من المخاطر المرتبطة بترك الصحفيين لأجهزة الكمبيوتر الخاصة بهم دون مراقبة مما يعزز دفاعات المؤسسات الصحفية في مجال الأمن السيبراني، وتقليل فرص الجهات الخبيثة التي تسعى إلى الدخول غير المصرح به).

وتعتبر سياسة القفل التلقائي ثغرة أمنية يُمكن استغلالها من قِبل جهات خبيثة بما يتماشى مع قفل محطات العمل التلقائي مع مبدأ إدارة الوصول الموضح في إطار عمل الأمن السيبراني للمعهد الوطني للمعايير والتكنولوجيا(NIST)، الذي يركز على التحكم في الوصول المادي والمنطقي إلى الأصول والبيانات (إطار عمل الأمن السيبراني للمعهد

الوطني للمعايير والتكنولوجيا، 2020)، وقيدت هذه الأنظمة الدخول إلى مناطق محددة داخل المؤسسات الإعلامية، مما يضمن وصول الموظفين المعتمدين فقط إلى البنية التحتية لتكنولوجيا المعلومات والبيانات الحساسة"، مما يقلل من خطر دخول الأفراد غير المصرح لهم إلى المناطق الآمنة"، ويمثل الهدف الرئيسي من هذا الإجراء التخفيف من المخاطر المرتبطة بمحطات العمل غير المراقبة، فعندما تُترك محطات العمل دون مراقبة، قد تُصبح بوابات الأفراد غير مُصرّح لهم للوصول إلى أنظمة وبيانات تكنولوجيا المعلومات الخاصة بالمؤسسة، ومن خلال القفل التلقائي لمحطات العمل، يسعى الصحفيون إلى تقليل هذه الثغرة وتعزيز أمن أصولهم الرقمية، وقد شكّلت هذه التدابير الأمنية المادية كخط دفاع أول قوي مما يضمن دخول الأشخاص الذين لديهم أسباب أو أذونات مشروعة فقط إلى هذه المناطق الآمنة، وبذلك تمتلك المؤسسات الصحفية " استراتيجية صارمة للتحكم في الوصول بما يضمن وصول الصحفيين فقط إلى ما هو ضروري لمهامهم المحددة، مما يمنع الوصول غير المبرر إلى المعلومات الحساسة.

وتوفر عمليات التدقيق من قِبل جهات خارجية منظوراً موضوعياً لوضع الأمن السيبراني لمؤسساتهم الصحفية (ومن خلال دعوة خبراء مستقلين لفحص الإجراءات الأمنية للمؤسسات الصحفية، ويعتبر هذا التحقق الخارجي بمثابة إجراء تأميني قوي، بما يضمن قوة ومرونة استراتيجياتهم الأمنية)، إضافة إلى التحديث المنتظم للأنظمة والبرمجيات (الثغرات الأمنية غالبًا ما تنبع من برامج قديمة ذات عيوب أمنية معروفة)، وأهمية البقاء على اطلاع بأحدث أساليب الهجوم في ظل بيئة الأمن السيبراني المتطورة باستمرار(مثل هجمات حجب الخدمة الموزعة (DDoS) ومحاولات التصيد الاحتيالي كتهديدات شائعة يجب على المؤسسات الصحفية توخي الحذر منها.

- **تاسعا: أهمية التشريعات السيبرانية التى تنظم بيئة الإعلام الرقمى:**

جدول (10) أسباب الاهتمام بالتشريعات السيبرانية،

أسباب الاهتمام بالتشريعات السيبرانية	ك	٪
وجود إطار تنظيمى لتنظيم استخدام وحماية المعلومات	9	12.5
أهمية إضفاء صفة الشرعية على التعاملات السيبرانية وبيان ضوابطها ومحدداتها	6	8.3
حماية المتعاملين سواء صحفيين أو إعلاميين أو موظفين عبر الفضاء السيبرانى	10	13.9
بناء ثقة المستخدم في خدمات وتطبيقات الفضاء السيبرانى	5	6.9
دعم وتحفيز الإعلام الرقمى إقليميا ودوليا	8	11.1
نتيجة تزايد عدد التطبيقات ووسائل التواصل الاجتماعى	6	8.3
انتشار الأخبار الزائفة	7	9.7
ظهور استخدامات مسيئة للفضاء السيبرانى	9	12.5
انتشار الحروب الإلكترونية بين البلاد	12	16.7
الإجمالى	72	٪100

تشير نتائج الجدول السابق إلى أسباب الاهتمام بالتشريعات السيبرانية، المنظمة لبيئة الإعلام الرقمي والتي تتمثل في انتشار الحروب الإلكترونية بين البلاد بنسبة16.7٪، يليها حماية المتعاملين سواء صحفيين أو إعلاميين أو موظفين عبر الفضاء السيبراني بنسبة 13.9٪، يليها وجود إطار تنظيمي لتنظيم استخدام وحماية المعلومات، و ظهور استخدامات مسيئة للفضاء السيبراني بنسبة 12.5٪، يليها دعم وتحفيز الإعلام الرقمي إقليمياً ودولياً بنسبة 11.1٪، يليها انتشار الأخبار الزائفة بنسبة9.7٪، يليها أهمية إضفاء صفة الشرعية على التعاملات السيبرانية وبيان ضوابطها ومحدداتها، وتزايد عدد التطبيقات ووسائل التواصل الاجتماعي بنسبة 8.3٪، وأخيراً بناء ثقة المستخدم في خدمات وتطبيقات الفضاء السيبراني بنسبة 6.9٪، ويمكن القول بأن قوانين ولوائح الأمن السيبراني تؤدي دوراً محورياً في حياتنا اليومية، وتضمن هذه السياسات المهمة حماية معلوماتنا من التهديدات السيبرانية، ومن هنا وجب وضع لوائح وسياسات جديدة لحماية معلوماتنا داخل المؤسسات الصحفية، ومناقشة التشريعات السيبرانية التي تهدف

إلى ضمان استخدام بياناتنا "بإنصاف وقانونية وشفافية"، وأهمية "التعامل معها بطريقة تضمن الأمن المناسب، بما في ذلك الحماية من المعالجة غير القانونية أو غير المصرح بها، أو الوصول إليها، أو فقدانها، أو إتلافها"، وهناك تداعيات قانونية لعدم حماية البيانات والمعلومات الشخصية، مما يتطلب تعزيز الأمن السيبراني بالمؤسسات الصحفية، وضرورة صياغة تشريعات الأمن السيبراني التي تنظم بيئة العمل الصحفي، مثل حماية البيانات، والحد من المخاطر الإلكترونية، والحماية من مخططات التصيد الاحتيالي، وهجمات برامج الفدية، وسرقة الهوية، واختراق البيانات، ويمكن القول بأن قوانين الأمن السيبراني تهدف إلى تعزيز تتبع التهديدات السيبرانية والوقاية منها والحد منها.

نتائج المقابلات الكيفية:

أجرت الباحثة عدداً من المقابلات المتعمقة مع مجموعة من الخبراء والأكاديميين في العمل الصحفي وفي مجال تكنولوجيا الإعلام والأمن السيبراني والإعلام، ممثلة في عينة مكونة من 18 خبيراً منقسمين إلى عدد (9) من خبراء العمل الصحفي، وعدد (9) من أساتذة الإعلام والحاسبات والمعلومات والحقوق، والمتخصصين في مجال الأمن السيبراني، بهدف فهم الوضع الراهن للتهديدات السيبرانية داخل المؤسسات الإعلامية، ومعرفة كافة أشكال الجرائم الافتراضية التي تشكل خطراً على بيئة الإعلام الرقمي، وتسعي الدراسة الحالية إلى وضع مسودة قانون للتشريعات السيبرانية للجرائم الافتراضية في بيئة الإعلام الرقمي، وتوصلت نتائج المقابلات إلى ما يلي:

أولًا: أهمية الأمن السيبراني في المؤسسات الإعلامية.

تهتم الباحثة بمعرفة مدى إلمام الخبراء بأهمية الأمن السيبراني داخل مؤسساتهم الإعلامية، وحماية تطبيقاتها وبياناتها وبنيتها التحتية من التهديدات الإلكترونية.

يرى **محمود المملوك**[1] أن الفضاء السيبراني يشكل ميدان المعركة الخامس بين القوى الدولية بعد الأرض والبحر والجو والفضاء، وأصبح الأمن السيبراني مصدر قلق مجتمعي خاصة في المؤسسات الإعلامية، نتيجة عديد من التهديدات ونقاط الضعف، مثل البريد المزعج، والمتسللين، واختراق البيانات، والتجسس، وفيروسات الكمبيوتر، وسرقة الهوية،

1) مقابلة مع محمود المملوك.. رئيس تحرير موقع القاهرة 24، بتاريخ 10 فبراير 2025، الساعة 4:00م.

وتجاهل جدران الحماية، وهجمات رفض الخدمة الموزعة، والنقر على روابط احتيالية مرسلة عبر البريد الإلكتروني، والقرصنة عبر الإنترنت، والمراقبة الدولية الجماعية، والتسلط عبر الإنترنت، كما تمثل الحرب الإلكترونية أمثلة حية للمخاوف الإلكترونية والمتصيدون عبر الإنترنت والإيذاء السيبراني، ويؤدي الأمن السيبراني دوراً حيوياً في المؤسسات الإعلامية، حيث تواجه هذه المؤسسات تحديات فريدة منها حماية البيانات والمعلومات الحساسة حيث تحتفظ المؤسسات الإعلامية بكميات هائلة من البيانات، بما في ذلك المعلومات السرية للمصادر، والبيانات الشخصية للمشتركين، والملكية الفكرية للمحتوى، كما يهدف الأمن السيبراني إلى حماية هذه البيانات من الوصول غير المصرح به، والسرقة، والتلاعب، والتدمير، علاوة على الحفاظ على سمعة المؤسسة حيث يمكن أن يؤدي اختراق البيانات أو الهجوم السيبراني إلى الإضرار بسمعة المؤسسة وفقدان ثقة الجمهور، كما يساعد الأمن السيبراني في منع الهجمات والحفاظ على سمعة المؤسسة كمصدر موثوق للمعلومات.

ويعلق **إسلام مصطفى**[2] بأن الأمن السيبراني يقوم على حماية الأنظمة من الهجمات الرقمية، وتبحث المنظمات الإعلامية عن حلول فعالة لإدارة وحماية أصولها خاصة المؤسسات الإعلامية الكبرى، وينبغي حماية حقوق التعبير في الفضاء الإلكتروني بالمؤسسات الإعلامية من التهديدات السيبرانية، والتي تساعد على ضمان استمرارية العمل حيث يمكن أن تؤدي الهجمات السيبرانية إلى تعطيل العمليات الإعلامية، مثل البث والنشر والتوزيع، كما يساعد الأمن السيبراني في ضمان استمرارية العمل وتجنب الخسائر المالية الناجمة عن التوقف، إضافة إلى مكافحة المعلومات المضللة والأخبار الكاذبة حيث تؤدي المؤسسات الإعلامية دوراً حيوياً في مكافحة المعلومات المضللة والأخبار الكاذبة، ويساعد الأمن السيبراني في حماية الأنظمة الإعلامية من التلاعب والاختراق الذي يمكن استخدامه لنشر المعلومات المضللة.

---

2) مقابلة مع إسلام مصطفى.. مدير تحرير الـ Social Media بموقع القاهرة 24، بتاريخ 10 فبراير 2025، الساعة 4:30م.

ويتفق معه **جمعة حمد الله**[3] بأن الأمن السيبراني يركز على حماية الأنظمة والشبكات من التهديدات الإلكترونية، بينما يعتبر أمن المعلومات أوسع نطاقًا ويشمل حماية المعلومات بشكل عام بغض النظر عن الوسائط المستخدمة، ويساعد الأمن السيبراني في حماية الملكية الفكرية وحماية الأصول من السرقة والقرصنة، حيث تعتبر الملكية الفكرية، مثل المحتوى الأصلي والأخبار الحصرية، من أهم أصول المؤسسات الإعلامية، إضافة إلى الامتثال للقوانين واللوائح حيث تخضع المؤسسات الإعلامية للعديد من القوانين واللوائح المتعلقة بحماية البيانات والخصوصية، ويساعد الأمن السيبراني في ضمان الامتثال لهذه القوانين وتجنب العقوبات القانونية، وأيضا زيادة الوعي الأمني حيث لا يقتصر الأمن السيبراني على التكنولوجيا فقط، بل يشمل أيضًا التدريب والتوعية، ويجب على المؤسسات الإعلامية توعية موظفيها بأهمية الأمن السيبراني وتدريبهم على أفضل الممارسات.

ثانيا: كيفية اكتشاف التهديدات والجرائم السيبرانية في المؤسسات الإعلامية وطرق الوقاية منها

يُعد اكتشاف التهديدات السيبرانية في المؤسسات الإعلامية والوقاية منها أمرًا بالغ الأهمية لحماية البيانات الحساسة والحفاظ على سمعة المؤسسة، وتشمل التهديدات الجرائم السيبرانية مثل الهجمات الإلكترونية، وسرقة البيانات، وانتشار الأخبار الزائفة، ويجب على المؤسسات الإعلامية تنفيذ تدابير أمنية شاملة، مثل المصادقة متعددة العوامل، والتشفير، وتقييمات الثغرات الأمنية الدورية، وتدريب الصحفيين على الأمن السيبراني .

يؤكد **هشام أبو حديد**[4] الهجوم الإلكتروني أنه عملية إلكترونية، سواء كانت هجومية أو دفاعية، ومن المتوقع أن يتسبب في إلحاق الضرر أو التدمير بالأشياء، وتعتبر الهجمات الإلكترونية جرائم إلكترونية حتمية باستثناء شن هجوم إلكتروني داخل دولة أخرى، حيث تعد الهجمات الإلكترونية التي تنفذها الدول التي تحدث في سياق صراع مسلح هي

3) مقابلة مع جمعة حمد الله، رئيس تحرير جريدة المصري اليوم، بتاريخ 11 فبراير 2025، الساعة 3:00م.
4) هشام أبو حديد .. رئيس تحرير جريدة المصري اليوم، بتاريخ 11 فبراير 2025، الساعة 3:30م.

وحدها التي تؤدي إلى حروب إلكترونية، ومن ثمَّ أصبح الهجوم السيبراني غير مسلح، وأصبح عصر المعلومات بلا دماء، وأصبحنا في عصرٍ إلكترونيا يتحدى حقيقة أن بنيتنا التحتية الرقمية وقدراتنا المادية متكاملة من أجل دعم الحروب الحديثة، وأصبحت المعلومات هي الأداة الرئيسية للحروب السيبرانية، لدرجة أنه عندما نناقش الفضاء الإلكتروني لا يمكننا تهميش تأثير شبكات المعلومات باعتبارها أهدافًا وأدوات للهجمات السيبرانية، ويمكن لتقنيات الأتمتة والذكاء الاصطناعي تعزيز قدرات أنظمة الأمن السيبراني واكتشاف التهديدات السيبرانية، كما يمكن لخوارزميات التعلم الآلي تحليل مجموعة البيانات الضخمة عبر المواقع الإعلامية لتحديد الأنماط والشذوذ، مما يتيح اكتشاف التهديدات بشكل أسرع وتوفير حماية أفضل، مثل اتجاهات وسائل التواصل الاجتماعي والمنتديات عبر الإنترنت والبيانات العامة.

ويتفق معه **حجاج سلامة**[5]، مؤكدًا تعزيز الشراكات بين القطاعين العام والخاص لمكافحة التهديدات السيبرانية بغرض تبادل المعلومات والموارد والخبرات اللازمة لاتباع نهج شامل للأمن السيبراني بمختلف المؤسسات الإعلامية، خاصة وأنه يحمي البنية التحتية الحيوية، ويحدد نوعية التهديدات السيبرانية ويمنعها، ويرفع الوعي العام، ويعزز التعاون بين أصحاب المصلحة، ومع تقدم التكنولوجيا، تعد هذه الجهود وحدها غير كافية، مما يؤكد الحاجة الملحة لاتخاذ تدابير استباقية لمواجهة هذه التهديدات المتطورة، وهناك عديد من المخاطر المحتملة المرتبطة بأمن وسائل التواصل الاجتماعي، نظرًا للطبيعة التفاعلية للإعلاميين مع وسائل التواصل الاجتماعي، وهناك تهديد محتمل بإدخال برامج ضارة إلى شبكات المنظمات الإعلامية، حيث يمكن أن يؤثر الهجوم الإلكتروني على البنية التحتية الحيوية لكل مؤسسة صحفية، وتعتبر هجمات اليوم الصفري خطيرة بشكل خاص لأنه يمكن استخدامها لاستهداف أكثر الأنظمة أمانا ولا يتم اكتشافها لفترات طويلة من الزمن.

5) مقابلة مع حجاج سلامة.. مدير تحرير جريدة الوفد، بتاريخ 13 فبراير 2025، الساعة 2:00م.

ويعقب **محمود فرج**[6] بأن الأمن السيبراني يمثل تحدياً متزايداً في العصر الرقمي، حيث تتطور التهديدات السيبرانية وتصبح أكثر تعقيداً، وغالبا ما تكون التدابير الأمنية التقليدية غير كافية للدفاع ضد التهديدات الديناميكية، وتشكل الجرائم الافتراضية ببساطة مجموعة فرعية من الجرائم التقليدية، حيث تُستخدم تكنولوجيا المعلومات والاتصالات وسيلة أو أداة لارتكابها، ولها أشكال عدة مثل التلاعب بوثائق مهمة، والاختراق وإرسال رسائل مسيئة، وسرقة الهوية، والغش عبر الإنترنت من خلال انتحال الشخصية، وانتهاك الخصوصية عبر الإنترنت، والإرهاب الإلكتروني، ونشر أخبار زائفة، ومعلومات تشهيرية في شكل إلكتروني، والاحتفاظ بالمعلومات بشكل غير قانوني من قبل وسيط.

يضاف لما سبق، الفشل في المساعدة في فك تشفير المعلومات، ومنع الوصول العام إلى المعلومات والوثائق الهامة التي تصب في المصلحة الوطنية، والفشل في توفير الوصول عبر الإنترنت إلى أجهزة الكمبيوتر بالمؤسسات الإعلامية، ومحاولة تأمين الوصول غير المصرح به إلى النظام المحمي، وفشل مزودي خدمة الإنترنت في تقديم المعلومات إلى الوكالات الدولية، والتضليل، وانتهاك السرية والخصوصية، ونشر شهادة توقيع رقمية مزورة لقيادات إعلامية لأغراض احتيالية، ومحاولة ارتكاب جريمة باستخدام الوسائط الإلكترونية، واختلاق أدلة إلكترونية كاذبة، وتدمير الأدلة الإلكترونية لمنع إنتاجها كدليل في بعض القضايا المجتمعية والسياسية الهامة المطروحة على الساحة وتشغل الرأي العام، والتزوير لغرض الغش والتشهير، واستخدام وثائق مزورة على أنها أصلية مما يؤدي إلى تضليل الرأي العام.

ويتفق معه **د. أحمد حلمى**(7)، معبراً بأن المؤسسات الإعلامية تواجه تحديات هائلة في مجال الأمن السيبراني، حيث إنها تتعامل مع معلومات حساسة وذات قيمة عالية، وتعتمد

---

6) مقابلة مع محمود فرج.. مدرب دولي معتمد في الذكاء الاصطناعي شركة هواوي العالمية، بتاريخ 20 فبراير 2025، الساعة 8:00 م

7) مقابلة مع أ.د / أحمد حلمي.. أستاذ تكنولوجيا المعلومات.. كلية التربية النوعية، جامعة قنا، بتاريخ 14 فبراير 2025، الساعة 11:00 ظ.

بشكل كبير على الأنظمة الرقمية في عملها، ويمكن اكتشاف التهديدات والجرائم السيبرانية في المؤسسات الإعلامية عن طريق الاستعانة ببرامج مكافحة الفيروسات والبرامج الضارة، حيث ينبغي أن يتم تثبيت برامج مكافحة الفيروسات والبرامج الضارة على جميع الأجهزة والأنظمة، وتحديثها بانتظام، وإجراء فحوصات دورية للأجهزة والأنظمة للكشف عن أي برامج ضارة، ويمكن الاستعانة بأنظمة كشف التسلل (IDS) وأنظمة منع التسلل (IPS)، حيث تراقب هذه الأنظمة حركة مرور الشبكة للكشف عن الأنشطة المشبوهة، ويمكنها منع الهجمات تلقائيًا، وضرورة تحليل سجلات النظام التي تحتوي على معلومات حول كافة الأنشطة التي تحدث على الأجهزة والأنظمة، وأهمية تحليل هذه السجلات بانتظام للكشف عن أي أنشطة مشبوهة.

وينبغي أن تحرص المؤسسات الإعلامية على مراقبة حركة مرور الشبكة للكشف عن الأنشطة المشبوهة، مثل محاولات الوصول غير المصرح به، مع أهمية الوعي البشري داخل المؤسسات الإعلامية والصحفية، والتعرف على رسائل البريد الإلكتروني الاحتيالية والروابط المشبوهة، وتشجيع الموظفين على الإبلاغ عن أي أنشطة مشبوهة، وتتعدد طرق الوقاية من التهديدات والجرائم السيبرانية داخل المؤسسات الإعلامية والصحفية مثل استخدام كلمات مرور قوية، وتغييرها بانتظام، إضافة إلى تحديث البرامج بانتظام لاحتوائها على إصلاحات أمنية تسد الثغرات التي يمكن للمهاجمين استغلالها، مع أهمية استخدام جدار الحماية الذي يمنع الوصول غير المصرح به إلى الأجهزة والأنظمة داخل المؤسسات الإعلامية، إضافة إلى ضرورة تشفير البيانات التي تحمي من الوصول غير المصرح به، حتى في حالة سرقتها، مع أهمية النسخ الاحتياطي للبيانات وذلك لإمكانية استعادتها في حالة فقدها أو تلفها.

ثالثًا: كيفية إدارة مخاطر الأمن السيبراني في المؤسسات الإعلامية، وحماية البنية التحتية التي تستهدفها الجماعات الإرهابية

ينبغي إدارة مخاطر الأمن السيبراني في المؤسسات الإعلامية، وحماية البنية التحتية من الجماعات الإرهابية، كما يجب اتباع استراتيجية متعددة الأوجه تشمل تقييم المخاطر، وتطبيق ضوابط أمنية قوية، وتوعية الصحفيين، والاستجابة للحوادث بفعالية

ترى **أ.د. نجلاء فارس** [8] بأن خصوصية المستخدم في الفضاء الإلكتروني أصبحت مصدر قلق كبير للأفراد وللمؤسسات الإعلامية، وعلي الرغم من أن الهجمات الإلكترونية لا تستخدم أي أسلحة مادية، إلا أنها أكثر الأسلحة خطورة وضرراً، والتي قد تتسبب في الكشف عن أكثر المعلومات السرية لدي المؤسسات الإعلامية فيما يخص المنظمات الحكومية من خلال التجسس أو التصيد الاحتيالي، وهناك 162 هجوما على برامج الفدية تم الإبلاغ عنها علناً ضد حكومات الولايات والحكومات المحلية في الولايات المتحدة عام 2017 فقط، كما تسببت الهجمات الإلكترونية في أضرار بقيمة 5 مليار دولار أمريكي وستزداد في المستقبل، وعلى سبيل المثال، قد يصل الضرر إلى 20 تريليون دولار أمريكي سنويا بحلول عام 2030م.

ويجب اقتراح منهجية لإنشاء انطولوجيا خاصة بالمؤسسات الإعلامية لإنشاء سيناريوهات خاصة بالمجال تتعلق بالتهديدات السيبرانية ونقاط الضعف والهجمات والتدابير المضادة، وإثراء هذه الانطولوجيا برؤي محدثة من خلال تكاملها مع البرمجة اللغوية العصبية ومصادر البيانات المتنوعة، مع ضرورة استفادة المؤسسات الإعلامية من البرمجة اللغوية العصبية لاستخراج المعلومات ذات الصلة من مصادر متنوعة مثل التقارير والمدونات ووسائل التواصل الاجتماعي، وإنشاء أدوات توصي باتخاذ التدابير المضادة المناسبة والتقنيات الدفاعية للمحلل الأمني عند الاستعلام عن تقنية الهجوم، وأتمتة العلاقة بين التقنيات الهجومية والدفاعية والتدابير المضادة باستخدام نماذج اللغة، وضرورة بناء نموذج لغوي لربط التدابير المضادة الدفاعية بالتقنيات الهجومية، حيث يمكن ان تدمر الهجمات الإلكترونية سمعة المؤسسة الإعلامية، ومن ثمَّ ستفقد ثقة الجمهور والرأي العام.

8) مقابلة مع أ.د/ نجلاء فارس.. أستاذ تكنولوجيا المعلومات، كلية التربية النوعية، جامعة قنا، بتاريخ 12 فبراير 2025، الساعة 12:10 ظ.

ويتفق معها أ.د. **عماد على**[9]، معبراً بأن الهجمات السيبرانية والتجسس والاختراقات الإلكترونية فرضت فكرة النظر في سيادتها الكاملة، لذا من الضروري سرعة جمع معلومات حول نوايا الخصم ودوافعه وقدرته على إلحاق الأذى والضرر بالنظام أو الشبكة، خاصة نتيجة تطور أشكال العنف السيبراني في وسائل الإعلام من عنف لغة واحدة في الماضي إلى نمط هجوم شامل مثل مسح الشاشة بالرصاص والتحرير الخبيث وتزييف الصور ونشر الشائعات وتوجيه الإهانة في الرسائل الخاصة وانتهاك الخصوصية الشخصية والسمعة خاصة عبر وسائل التواصل الاجتماعي، إضافة إلى الترويج لمحتوى المعلومات الكاذبة مما يجبر أصحاب المصلحة على دفع رسوم حذف المنشورات الضخمة علاوة على توجيه الرأي العام، خاصة وأن الحروب السيبرانية التي يقوم بها المهاجم تحتم على المدافع أن يوفر أكبر قدر من الإمكانات اللازمة من أجل الحماية، وفي المقابل يسعي القائم بالهجمة أو الحرب إلى تطوير إمكانياته لاختراق المجالات السيبرانية.

ويؤكد **محمود فرج**[10] أنه ينبغي تقييم المخاطر، وتحديد الأصول الحيوية مثل البيانات السرية للمصادر، والبيانات الشخصية للمشتركين، والملكية الفكرية للمحتوى، وأنظمة البث والنشر والتوزيع، وضرورة تحليل التهديدات المحتملة، مثل الهجمات الإلكترونية (برامج الفدية، هجمات حجب الخدمة)، والتجسس السيبراني، ونشر المعلومات المضللة، والتهديدات من الجماعات الإرهابية، وضرورة تقييم الثغرات، وتحديد نقاط الضعف في الأنظمة والإجراءات الأمنية، وتقدير الأضرار المحتملة التي قد تنجم عن وقوع هجوم سيبراني، مع وضع استراتيجية للأمن السيبراني، وتحديد الأهداف الأمنية التي تسعى المؤسسات الإعلامية إلى تحقيقها، وتحديد الضوابط الأمنية والإجراءات والتقنيات التي يجب تطبيقها لحماية الأصول، وتخصيص الموارد المالية والبشرية اللازمة لتنفيذ الاستراتيجية، ووضع خطة للتعامل مع الهجمات السيبرانية، مع أهمية تنفيذ الضوابط

---

9) مقابلة مع أ.د عماد على.. عميد كلية الحاسبات والمعلومات – جامعة قنا، بتاريخ9 فبراير 2025، الساعة 2:00م.

10) مقابلة مع محمود فرج.. مدرب دولي معتمد في الذكاء الاصطناعي شركة هواوي العالمية، بتاريخ 20 فبراير 2025، الساعة 8:00 م

الأمنية، ومنها تطبيق تقنيات الحماية، وتطبيق إجراءات التحكم في الوصول إلى البيانات والأنظمة، وتشفير البيانات الحساسة لحمايتها من الوصول غير المصرح به.

ويمكن حماية البنية التحتية للمؤسسات الإعلامية من الجماعات الإرهابية من خلال تعزيز الأمن السيبراني، وتطبيق ضوابط أمنية مشددة، ومراقبة التهديدات الإرهابية على الإنترنت، وضرورة التعاون مع الجهات الأمنية، ووضع خطط للطوارئ، وإجراء تدريبات للطوارئ، مع أهمية التعاون مع المؤسسات الإعلامية الأخرى لتبادل المعلومات والخبرات، ومواكبة أحدث التطورات في مجال الأمن السيبراني، مع أهمية حصول المؤسسات الإعلامية والصحفيين على شهادات الاعتماد في مجال الأمن السيبراني.

رابعا: آليات حماية معلومات وبيانات المؤسسات الإعلامية من الجرائم السيبرانية

يمكن الحفاظ على معلومات وبيانات المؤسسات الإعلامية من الجرائم السيبرانية، باتخاذ تدابير أمنية متعددة، مثل استخدام جدار حماية قوي، وتثبيت برامج مكافحة الفيروسات، وتدريب الصحفيين على الأمن السيبراني، وإنشاء كلمات مرور قوية، وتطبيق أفضل الممارسات الأمنية.

يرى **بسام رجب**[11] أن الأمن السيبراني يحمي الشبكات والأجهزة من الوصول غير المصرح به والهجمات، مثل القرصنة والتصيد الاحتيالي والبرامج الضارة، ويمثل ضمان الأمن السيبراني أمراً بالغ الأهمية لحماية المنظمات الإعلامية، التي تواجه تهديدات يومية من الهجمات الإلكترونية، والتي تعرض شبكاتها وبياناتها للخطر، ويمكن لتطبيقات الحماية من تقييم مخاطر الأمن السيبراني ديناميكيًا واكتشاف الأنشطة الاحتيالية بدقة وبسرعة غير مسبوقة، حيث يمكن التنبؤ بالجرائم الافتراضية باستخدام خوارزميات التعلم الآلي، ويمكن الكشف التلقائي للهجمات الأمنية من خلال معالجة البيانات من المواقع الإعلامية.

11) مقابلة مع بسام رجب.. مدير تحرير جريدة الفجر، بتاريخ 2 فبراير 2025، الساعة 5:00م.

ويتابع **محمد حمدي**[12] بأن هناك عديدًا من المخاوف بالغة الأهمية بشأن إدارة معلومات المؤسسات الإعلامية منها حماية الخصوصية بشأن الاتصالات المخزنة إلكترونيًا؛ وضمان صحة المعلومات؛ وحماية حقوق الملكية أو الملكية المرتبطة بالمعلومات؛ وتسهيل الوصول إلى المعلومات، وقد تواجه المؤسسات الإعلامية المزيد من التعقيدات بسبب إمكانية وجود أشكال عديدة متناقضة وغير متوافقة من التكنولوجيا تتعايش في وقت واحد، مما يجعل من الصعب على المؤسسات الإعلامية تحديد نقطة دخول مخاطر الأمن السيبراني بسرعة، وهناك عديد من التهديدات السيبرانية الموجودة على صفحات المواقع الإعلامية بمنصات التواصل الاجتماعي مثل: فقدان الإنتاجية- التنمر الإلكتروني – المطاردة الإلكترونية – سرقة الهوية – العلامات التجارية– تلف السمعة الشخصية – خرق البيانات – البرامج الضارة – انقطاع الخدمة – الاختراق – الوصول غير المصرح به إلى حسابات القيادات الحكومية وحسابات الإعلاميين على وسائل التواصل الاجتماعي وصولًا إلى حسابات الجمهور، علاوة على نشر الأخبار الزائفة التي تعد أحد أشكال الجرائم الافتراضية في الفضاء الإلكتروني، حيث أسست الحكومات في الأنظمة الاستبدادية، مثل روسيا وكمبوديا وفيتنام، الأخبار الزائفة كتهديد وجودي للأمن القومي بما يضاهي الإرهاب والحروب الإلكترونية، في حين سعت لتمرير قوانين تهتم بحرية وسائل الإعلام وحرية الرأي والتعبير.

وتؤكد أ.د. **نجلاء فارس**[13] أهمية استخدام تقنيات التشفير لحماية البيانات الحساسة أثناء النقل والتخزين، وتثبيت جدران حماية قوية لمراقبة حركة البيانات، وضرورة حرص المؤسسات الإعلامية على تحديث الأنظمة والبرامج بانتظام لسد الثغرات الأمنية، كما تستطيع المؤسسات الإعلامية ان تطبق سياسات صارمة للتحكم في الوصول إلى المعلومات الحساسة، ومنع الوصول إليها باستثناء الأشخاص المصرح لهم فقط، ويمكن

12) مقابلة مع محمد حمدي.. مدير تحرير جريدة المصري اليوم، بتاريخ 5 فبراير 2025، الساعة 10:00 ص.

13) مقابلة مع أ.د/ نجلاء فارس.. أستاذ تكنولوجيا المعلومات، كلية التربية النوعية، جامعة قنا، بتاريخ 12 فبراير 2025، الساعة 10:12 ظ.

عمل نسخ احتياطية للمعلومات المهمة لضمان استعادتها في حال حدوث اختراق أو فقدان، ويمكن الاستعانة بأدوات لرصد وتحليل الأنشطة غير المعتادة على الشبكة لاكتشاف الهجمات مبكراً، وأخيراً يمكن للمؤسسات الإعلامية التعاون مع جهات مختصة في الأمن السيبراني لتبادل التقنيات الحديثة وتعزيز أمن معلوماتها وبياناتها بانتظام.

خامساً: العوامل التى يجب مراعاتها عند وضع الأيديولوجية الأخلاقية والمهنية للأمن السيبرانى لمنع الجرائم الافتراضية في المؤسسات الإعلامية

ينبغي مراعاة عدة عوامل عند وضع الأيديولوجية الأخلاقية والمهنية للأمن السيبراني لمنع الجرائم الافتراضية في المؤسسات الإعلامية، تشمل تحديد مبادئ أساسية، ووضع سياسات واضحة، وتعزيز الوعي، وبناء شراكات، وتنفيذ تدابير وقائية.

يرى **جمعة حمد الله**[14] أنه على الرغم من أهمية الأمن السيبراني في مكافحة الجرائم الافتراضية، فإنها يمكن أن يكون لها تأثير مخيف على حرية التعبير وإتاحة المعلومات، على سبيل المثال يمكن أن يؤدي الاستخدام المفرط لمراقبة المحتوى إلى الرقابة غير المقصودة على المحتوى الشرعي، الذي يزيل المحتوى المثير للجدل ولكنه غير قانوني، وهذه الرقابة غير مقصودة لا تقمع الأصوات الفردية فحسب، ولكن تقلل من تنوع وجهات النظر المتاحة عبر الإنترنت.

تستطيع الدول بذلك أن تستخدم ذريعة الأمن السيبراني لتبرير مراقبة الاتصالات الرقمية، مما ينتهك حقوق الخصوصية ويخنق حرية التعبير ويقمع المعارضة السياسية، وبذلك قد تنخفض حرية المواطن مع سعي الدول إلى تأمين أنظمتها سيبرانياً، ويجب أن تكون جميع عمليات الأمن السيبراني شفافة وقائمة على مبادئ النزاهة، وأن تكون سياسات الأمن واضحة ومفهومة للجميع، ويجب تجنب أي ممارسات خادعة أو مخادعة، حتى لو كانت بهدف حماية المعلومات، وحماية خصوصية المعلومات الشخصية والمعلومات الحساسة للمصادر والجمهور وهي واجب أساسي، وينبغي تطبيق إجراءات صارمة لحماية هذه المعلومات من الوصول غير المصرح به، وتحمل المسئولية عن أي فشل أمني أو انتهاك للقواعد الأخلاقية والمهنية، ويجب أن تتضمن الايديولوجية إجراءات واضحة

14) مقابلة مع جمعة حمد الله، رئيس تحرير جريدة المصري اليوم، بتاريخ 11 فبراير 2025، الساعة 3:00م.

لتحديد المسئولية اتخاذ الإجراءات الموضوعية، وحماية البنية التحتية الرقمية ودعم الحق في حرية التعبير واتاحة المعلومات وعدم تغييرها أو تزييفها.

ويضيف أ.د. **حلمى محسب**[15] بأن تزايد التصيد الاحتيالي في الآونة الأخيرة والذي يتضمن تثبيت برامج ضارة على أجهزة الحاسب الآلي بالمؤسسات الإعلامية، والحصول على البيانات الشخصية وكافة المعلومات المخزنة على الحاسب، كما يستطيع الفيروس المنتشر بأجهزة المؤسسات الإعلامية تشفير محركات أقراص الشبكة وقواعد البيانات والنسخ الاحتياطية مما يضر المؤسسة الإعلامية المستهدفة، ولذا ينبغي وضع سياسات واضحة للأمن السيبراني تشمل كيفية التعامل مع المعلومات الهامة، واستخدام الأجهزة والتواصل الإلكتروني، وضرورة استخدام تقنيات متقدمة مثل التشفير، وأنظمة الكشف عن التسلل، وجدران الحماية لحماية البيانات، علاوة على تطوير استراتيجية المخاطر المحتملة للتخفيف من حدتها، بما في ذلك خطط الاستجابة للحوادث، وضرورة تعزيز الثقافة المؤسسية داخل المؤسسات الإعلامية، وتنفيذ آليات لمراقبة الأنظمة وتقييم فعالية السياسات والإجراءات المتبعة، وتعزيز الشفافية في التعامل مع قضايا الأمن السيبراني وتحديد المسئوليات بوضوح، وضرورة إدارة الثغرات الأمنية في وسائل التواصل الاجتماعي داخل المؤسسات الإعلامية، وحماية المؤسسات الإعلامية ضد الأنشطة السيبرانية الخبيثة والالتزام بدعم الديمقراطية، ومعالجة خصوصية المستخدم والتهديدات السيبرانية.

ويؤكد أ.د. **أحمد حلمى**[16] **على** تأمين الفضاء الإلكتروني كونه مهمة شاقة تتطلب تقنية كبيرة مقترنة برؤي سلوكية، مع ضرورة وضع إطار أخلاقي شامل يوجه القرارات المتعلقة بالأمن السيبراني في المؤسسات الإعلامية، حيث يعد الأخلاق ذريعة مهمة لاتخاذ القرارات السليمة في بيئة متغيرة، مع تحديد ممارسات الأمن السيبراني الموصي بها

15) مقابلة مع أ.د حلمي محمود محسب.. عميد كية الإعلام وتكنولوجيا الاتصال، جامعة قنا، بتاريخ 5 مارس 2025، الساعة 10:00ص.

16) مقابلة مع أ.د / أحمد حلمي.. أستاذ تكنولوجيا المعلومات.. كلية التربية النوعية، جامعة قنا، بتاريخ 14 فبراير 2025، الساعة 11:00 ظ.

لمستخدمي وسائل التواصل الاجتماعي، وأهمية الامتثال للقوانين واللوائح الخاصة بالأمن السيبراني لضمان حماية البيانات وعدم إساءة استخدام الصلاحيات، مع أهمية حماية سرية وخصوصية البيانات ومراقبة التهديدات الداخلية والخارجية، كما ينبغي على المؤسسات الإعلامية التي تستفيد من وسائل التواصل الاجتماعي أن تجعل الأمن السيبراني أولوية قصوى لحماية بياناتها ومعلوماتها من التعرض للهجوم أو إساءة الاستخدام أو الاستيلاء عليها والاستفادة من الأطراف غير المسئولة لمصلحتهم.

سادسا: آليات تثقيف الإعلاميين بتهديدات الأمن السيبراني وإدارتها، وأسس تطبيق استراتيجيات الدفاع، أو التدابير المضادة

ينبغي أن تحرص المؤسسات الإعلامية على تثقيف الإعلاميين بتهديدات الأمن السيبراني، واستخدام مجموعة من الآليات التي تشمل تدريب متخصصين، وتوفير موارد تعليمية، وتشجيع التفاعل مع خبراء الأمن السيبراني، إضافة إلى تعزيز الوعي العام من خلال الحملات الإعلامية.

يرى **أبو المعارف الحفناوي**[17] بأن زيادة عدد الأجهزة المتصلة داخل المؤسسات الإعلامية قد يزيد من مستوي الهجوم ويقدم نقاط ضعف جديدة، وينبغي للمؤسسات الإعلامية وصحافييها وإعلاميها أن يكونوا على دراية بالتهديدات الرئيسية للأمن السيبراني مثل برامج الفدية، والتصيد الاحتيالي، وتسريب البيانات والمعلومات الهامة، والقرصنة، والتهديد الداخلي، وأهمية تزويد المؤسسات الإعلامية بأفضل الممارسات بهدف التخفيف من مخاطر الأمن السيبراني من استخدام الصحفيين لوسائل التواصل الاجتماعي بالتوازي مع حماية المؤسسة، حيث يكشف الصحفيين والإعلاميين عن معلوماتهم الشخصية على منصات التواصل الاجتماعي، مما يعرضهم لهجمات أمنية سيبرانية محتملة، كما تؤدي منصات الشبكات الاجتماعية أحيانًا إلى فقدان البيانات الشخصية للمؤسسات الإعلامية، والصحفيين أو تحفيز المتسللين على استغلال حسابات

17) مقابلة مع أبو المعارف الحفناوي.. مدير تحرير جريدة أخبار اليوم، بتاريخ 28 فبراير 2025، الساعة 3:00م.

الصحفيين لأغراض خبيثة، ويتضح ذلك جلياً من خلال زيادة خطاب الكراهية على مواقع التواصل الاجتماعي نتيجة المزيد من الهجمات السيبرانية.

ويتفق معه **محمد حمدي**[18]، خاصة وأن الاختراقات الأمنية قد تحدث بسبب الأخطاء البشرية، التي يمكن أن تعزى إلى نقص التدريب أو الوعي بالأمن السيبراني، لذا ينبغي تزويد الإعلاميين بالمعرفة من أجل التنقل في المشهد الرقمي بشكل أمن وفهم حقوقهم وخلق إعلامي رقمي مرن ومستنير، وتؤدي ثقافة الأمن السيبراني للمؤسسات الإعلامية دوراً كبيراً في تشكيل سلوك الإعلاميين والصحفيين، علاوة على أهمية فهمهم لنقاط الضعف في مكونات نظام الشبكة داخل مؤسساتهم الإعلامية والتهديدات التي يتم التعرض لها.

ويضيف **محمد عصام**[19] أن التكنولوجيا ضرورة ملحة في تعزيز الأمن السيبراني ولكن تدريب العنصر البشري له القدر نفسه من الأهمية، ويجب أن يستخدم الجيل الصاعد من الإعلاميين والصحفيين نصائح انطولوجيا مخاطر النظام الجديد في تلك الحقبة السيبرانية والتكتيكات العدائية وبيانات النظام التقني ونقاط الضعف، وأهمية التكامل بين حماية البنية التحتية الرقمية ودعم الحق في حرية التعبير وتوافر المعلومات، ويجب على الدول والهيئات والأشخاص والعاملين في مجال الإعلام التفطن الدائم والاستعداد المستمر لأي هجمة قد يتم التعرض لها، والتعاون الدائم أيضاً بين الدول بغرض التصدي للهجمات وحماية مجالها.

ويؤكد **محمد حمدي**[20] أهمية خلق ثقافة مستنيرة للأمن السيبراني في المؤسسات الإعلامية، تشمل تنفيذ حملات توعية مفصلة لبرامج التدريب، وبناء شعور بالمسئولية الجماعية تجاه المرونة السيبرانية، وتعزيز الوعي بين الإعلاميين والصحفيين، من خلال مبادرات التدريب، وتعزيز الشعور بالمسئولية، والالتزام بالحفاظ على التدابير الأمنية

18) مقابلة مع محمد حمدي.. مدير تحرير جريدة المصري اليوم، بتاريخ 5 فبراير 2025، الساعة 10:00ص.

19) مقابلة مع محمد عصام.. نائب رئيس القسم الاقتصادي، القاهرة 24، بتاريخ 15 فبراير 2025، الساعة 3:00م.

20) مقابلة مع محمد حمدي.. مدير تحرير جريدة المصري اليوم، بتاريخ 5 فبراير 2025، الساعة 10:00 ص.

طول الوقت، وتأثير الوعي السيبراني على سلوك الإعلاميين والصحفيين على وسائل التواصل الاجتماعي، وضرورة تحذير الإعلاميين والصحفيين من رسائل البريد الإلكتروني الاحتيالية والروابط المشبوهة، وتوعيتهم بأهمية الأمن السيبراني وتدريبهم على أفضل الممارسات.

ويستكمل **بسام رجب**[21] الحوار، مؤكدًا أهمية تدريب الصحفيين والإعلاميين على كيفية استخدام المصادقة الثنائية، التي تضيف طبقة حماية إضافية للحسابات، وأهمية وضع سياسات وإجراءات أمنية واضحة لتحديد مسؤوليات الموظفين في مجال الأمن السيبراني، وأهمية إجراء اختبارات الاختراق الدورية التي تساعد على تحديد نقاط الضعف في الأنظمة والشبكات الخاصة بالمؤسسات الإعلامية، ويبقى الوعي بأهمية الأمن السيبراني هو الأساس في مواجهة التهديدات، وينبغي على المؤسسات الإعلامية أن تكون على دراية تامة بأحدث التهديدات والأساليب التي يستخدمها المجرمون السيبرانيون.

سابعا: دور الدولة المصرية في التخفيف من مخاطر الأمن السيبرانى التى تواجه وسائل الإعلام

تتخذ الدولة المصرية عدة خطوات للتخفيف من مخاطر الأمن السيبراني التي تواجه وسائل الإعلام، بما في ذلك إنشاء الهيئة الوطنية للأمن السيبراني، ووضع استراتيجية وطنية للأمن السيبراني، وتأسيس المركز المصري للاستجابة للطوارئ المعلوماتية (سيرت)، إضافة إلى تشريع قوانين تحمي الفضاء السيبراني.

يؤكد **محمود فرج**[22] أهمية دور الدولة في الاهتمام بالأمن السيبراني في الحماية من التدخل الأجنبي في الشئون الداخلية للبلاد، خاصة عقب ارتفاع مخاوف الأمن السيبراني حول وسائل التواصل الاجتماعي في السنوات الأخيرة، وأصبحت أكثر عرضة للهجمات الإلكترونية، وذلك لأن هذه المنصات تعتمد على المحتوى الذي ينشئه المستخدمون لشعبيتها وإيرادات الاعلانات، حيث استفاد مجرمي الإنترنت من الوصول

21) مقابلة مع بسام رجب.. مدير تحرير جريدة الفجر، بتاريخ 2 فبراير 2025، الساعة 5:00 م.

22) مقابلة مع محمود فرج.. مدرب دولي معتمد في الذكاء الاصطناعي شركة هواوي العالمية، بتاريخ 20 فبراير 2025، الساعة 8:00 م.

الواسع لهذه المنصات وسهولة استخدامها حيث تسمح منصات التواصل الاجتماعي للمتسللين بمشاركة المحتوى الضار، والتواصل مع الأصدقاء، ومن ثم ينتشر هذا المحتوى الضار كالنار في الهشيم على هذه المنصات، مما يؤدي إلى انتشار الأخبار الزائفة وتضليل المعلومات على المواقع الصحفية والإعلامية.

وتؤكد أ.د **نجلاء فارس**[23] اهتمام الدولة بالأمن السيبراني هدف رئيسي لتعزيز الأمن القومي والمعلومات المضللة ومكافحة خطاب الكراهية، وقد قدمت الحكومة المصرية الحالية، تحت قيادة الرئيس عبد الفتاح السيسي، قوانين بشأن الإرهاب والإعلام والجرائم الافتراضية، ووسعت نطاقها، وأنشأت هيئات وطنية وإقليمية متخصصة للأمن السيبراني، وحدث تحول كبير في نهج الدولة تجاه الأمن السيبراني، وسلطت الضوء على الأهمية السياسية للفضاء الإلكتروني، وفي الآونة الأخيرة، قررت شركات التكنولوجيا المتعددة الجنسيات الكبيرة مثل جوجل وأمازون منع التضليل عبر النطاقات لأنها تشكل خطراً على الأمن السيبراني، إلا أن بعض الناشطين لجأوا بدلًا من ذلك إلى منصات بديلة، باستخدام ألعاب الفيديو مع غرف الدردشة مثل League of Legends و.World of Warcraft ، وفي أغسطس 2018 أعيد صياغة قانون الجرائم الافتراضية، الذي يلزم مزودي خدمات الإنترنت بتخزين بيانات المستخدم ومحتوى نظام المعلومات والمعدات المستخدمة وتقديمها للحكومة، كما يعاقب القانون مسؤولي المواقع الإلكترونية إذا فشلوا في الإبلاغ للسلطات حال تعرضهم لهجوم إلكتروني، وعدم اتخاذ التدابير الاحترازية اللازمة لتأمين اتصالاتهم، دون تحديد هذه التدابير، ويجرم القانون تشغيل أو استخدام "موقع إلكتروني" يحرض على الجريمة، ويعرّف "الموقع الإلكتروني" على نطاق واسع ليشمل الصفحات العامة والحسابات الشخصية على فيسبوك وتويتر ومنصات أخرى.

---

23) مقابلة مع أ.د/ نجلاء فارس.. أستاذ تكنولوجيا المعلومات، كلية التربية النوعية، جامعة قنا، بتاريخ 12 فبراير 2025، الساعة 10:12 ظ.

ويرى أ. د. **أحمد حلمى**[24] بأن تقنيات الأمن السيبراني جزء أساسي من السياسة المصرية نظراً للأهمية الاستراتيجية لوسائل الإعلام في تشكيل الرأي العام ونشر الأخبار والمعلومات، ويعد حمايتها من أية تهديدات سيبرانية ضرورة وطنية، وبناء عليه تحرص الدولة على سن قوانين تجرم مختلف أنواع الجرائم السيبرانية التي تستهدف المواقع الصحفية والإعلامية، مثل الاختراق وسرقة البيانات أو تعديلها أو تحريفها أو حذفها، ونشر معلومات زائفة، علاوة على هجمات حجب الخدمة، ومن ثم ينبغي وضع أطر قانونية تنظم طبيعة عمل الفضاء السيبراني بما يضمن الأمن والأمان والاستقرار ويحمي المؤسسات الإعلامية، مع أهمية تشكيل فرق استجابة للطوارئ السيبرانية بهدف سرعة التعامل مع الهجمات السيبرانية التي تستهدف وسائل الإعلام في مصر.

ويتطابق معه في الرأي أ.د. **حلمى محسب**[25] في ضرورة اكتساب محللي الأمان للبصيرة السيبرانية في المواقع الإعلامية، بمعني اني يتوفر لديه نظرة ثاقبة على التهديدات السيبرانية وهجمات الأمن السيبراني والمخاطر السيبرانية مثل نقاط الضعف والاستغلال والحوادث الأمنية واختراق البيانات والجرائم الافتراضية، خاصة تهديدات الأمن السيبراني في وسائل التواصل الاجتماعي، وهجمات الهندسة الاجتماعية، وعدم وجود سياسة وسائل التواصل الاجتماعي، وتتمثل الهندسة الاجتماعية في هجوم على أمن المعلومات للوصول إلى الأنظمة ويتضمن هجوم الهندسة الاجتماعية على وسائل التواصل الاجتماعي عدة خطوات وهي جمع المعلومات وفحص وسائل التواصل الاجتماعي والمعلومات الداخلية الحساسة.

وفي ظل البيئة الرقمية سريعة التطور أحدثت التقنيات الناشئة مثل الذكاء الاصطناعي، والمركبات ذاتية القيادة، وإنترنت الأشياء، والتعلم الآلي، والبلوكتشين، والحوسبة السحابية والثورة في مختلف القطاعات، يجب على المؤسسات الإعلامية أن

---

24) مقابلة مع أ.د / أحمد حلمي.. أستاذ تكنولوجيا المعلومات.. كلية التربية النوعية، جامعة قنا، بتاريخ 14 فبراير 2025، الساعة 11:00 ظ.

25) مقابلة مع أ.د حلمي محمود محسب.. عميد كية الإعلام وتكنولوجيا الاتصال، جامعة قنا، بتاريخ 5 مارس 2025، الساعة 10:00ص.

تحرص على إدارة مخاطر الأمن السيبراني الجديدة بشكل فعال، فعلي سبيل المثال، يمكن لخوارزميات الذكاء الاصطناعي تحليل كميات هائلة من البيانات لتحديد الشذوذ والنشاط المشبوه الذي قد يشير إلى هجوم إلكتروني على المواقع الصحفية والإعلامية، إضافة إلى تقنية البلوكتشين التي يمكن استخدامها لإنشاء سجل أمن وشفاف للمحتوي، مما يسهل عليها مشاركة البيانات الآمنة وإدارة الهوية، كما يساعد البلوكتشين على منع اختراق البيانات، ويجعل من الصعب على المهاجمين العبث بالبيانات والمعلومات الصحفية، أما إنترنت الأشياء فهو يقدم مخاطر تتعلق بخصوصية البيانات والوصول غير المصرح به، وإساءة استخدام المعلومات الحساسة.

ويضيف **أ.د. عبد العزيز السيد**[26] بأن قانون مكافحة جرائم تقنية المعلومات (قانون الجرائم الافتراضية 175 لسنة 2018) يحدد العقوبات الخاصة بجرائم الاختراق والاحتيال الإلكتروني ونشر الأخبار المضللة، إضافة إلى قانون تنظيم الإعلام رقم 180 لسنة 2018 الذي ينظم عمل المؤسسات الإعلامية الرقمية وينظم معايير الأمن المعلوماتي، علاوة على إنشاء المجلس الأعلى لتنظيم الإعلام الذي يشرف على المحتوى الإعلامي، ويضمن عدم التلاعب بالمعلومات والأخبار عبر الفضاء الإلكتروني، مع ضرورة إلزام المؤسسات الإعلامية بتطبيق معايير الأمن السيبراني مثل تشفير البيانات وتأمين الشبكات من الاختراقات السيبرانية، وأهمية دعم استخدام الذكاء الاصطناعي وتقنيات تحليل البيانات في رصد المحتوى المشبوه والمعلومات الزائفة، وتطوير أنظمة المراقبة الإلكترونية لشبكات وسائل الإعلام بما يضمن رصد الهجمات السيبرانية التي تتصيد وتترصد المواقع الإعلامية.

26) مكالمة هاتفية مع أ.د / عبد العزيز السيد عبد العزيز.. أستاذ الصحافة، وعميد كلية الإعلام جامعة بني سويف، بتاريخ 2028 فبراير 2025، الساعة 10:00م.

سابعا: التعاون الدولى لحماية الفضاء الإلكترونى للمواقع الإعلامية والصحفية من التهديدات والجرائم السيبرانية

التعاون الدولي ضروري لحماية المواقع الإعلامية والصحفية من التهديدات والجرائم السيبرانية، وأهمية تبادل المعلومات والخبرات، وتعزيز القدرات السيبرانية، وتطوير المعايير العالمية للأمن السيبراني.

يرى أ.م.د **عباس مصطفى**[27] أن تزايد اعتماد الدول على الأنظمة الإلكترونية في جميع قطاعاتها الحيوية جعل من السهل الإضرار بمصالحها من خلال هجمات إلكترونية خاصة في حالات العداء، علاوة على اتساع نطاق مخاطر الأنشطة العدائية التي يمارسها الفاعلون (دول – غير دول) في الحروب السيبرانية، مما يدفع إلى شن هجمات إلكترونية عبر اجهزتها الأمنية الدفاعية، فتلجأ الدول إلى تجنيد قراصنة أو موالين لشن هجمات ضد الخصوم، إضافة إلى استهداف البنية التحتية للدول سواء مدنية أو عسكرية بهجمات إلكترونية مما يؤدي إلى شلل أنظمتها وتدمير أنظمة التشغيل الخاصة بها والتأثير على تدفق المعلومات إلى المواطنين عبر المواقع الإعلامية والصحفية، ومن هنا أصبح التعاون الدولي ضرورة قصوي لضمان تعزيز المصالح الأمنية والاقتصادية، وبناء على ذلك فإن دور برامج التعاون الدولي هو تطوير معايير سلوك الدول قبل وأثناء وبعد الهجمات السيبرانية وتطبيق القانون الدولي، وتيسير سبل الاستثمار في مجال الأمن السيبراني، وأهمية التعاون الدولي لحماية الفضاء السيبراني للمؤسسات الإعلامية من الهجمات السيبرانية المتكررة، خاصة وأن مفتاح التغلب على التهديدات السيبرانية المتطورة يكمن في التكيف والابتكار المستمر في مجال الأمن السيبراني

ويؤكد **أ.م.د هانى فوزي عبد الغنى**[28] أن هجمات برامج الفدية على مدى السنوات القليلة الماضية توضح عدم وجود حكومة محلية محصنة، لذا يعد تأمين الفضاء السيبراني جزءاً من استراتيجيات الأمن القومي للدول، التي أصبحت تتسابق في اقتناء

---

27) مقابلة مع أ.م.د/ عباس مصطفى.. استاذ القانون المساعد.. كلية الحقوق.. جامعة قنا، بتاريخ 7 فبراير 2025، الساعة 12 ظهراً بمكتب سيادته.

28) مقابلة مع أ.م.د / هاني فوزي عبد الغني.. أستاذ العلاقات العامة المساعد، ورئيس قسم العلاقات العامة، كلية الإعلام، جامعة قنا، بمكتب سيادته بتاريخ 1 مارس 2025، الساعة 10:00 ص.

مضادات للفيروسات الإلكترونية وأنظمة منع التشويش، ومن هنا وجب التعاون وتبادل المعلومات بين مختلف أصحاب المصلحة، بما في ذلك الحكومات والمنظمات الدولية والكيانات الخاصة، وتبادل المعلومات الاستخباراتية حول التهديدات وأفضل الممارسات وتنسيق الجهود لمنع الهجمات السيبرانية والاستجابة لها، وينبغي أن تشمل برامج تعزيز التعاون الدولي تطوير استراتيجية التعاون الدولي في مجال الأمن السيبراني بالمؤسسات الإعلامية، والتي تختص بإرساء مبادئ واتجاهات الدبلوماسية السيبرانية المصرية وفتح آفاق التعاون عربياً وإفريقياً وعالمياً ورفع مستوى الابتكار بالتعاون مع الشركاء الدوليين، على أن تكون وزارة الخارجية المصرية هي الجهة الوطنية المعنية بإدارة هذا الملف.

ويضيف **أ.م.د أحمد أبو ذكير**[29] بأن التهديدات السيبرانية المتصاعدة تتسبب في حدوث اضطرابات اجتماعية حادة وتقليل الثقة في المؤسسات الديمقراطية، ومنها المؤسسات الإعلامية وفيما تقدمه من معلومات وأخبار، كما يشكل الهجوم لبنية المعلومات ضربة قاضية لاقتصاد الدول وإلحاق الضرر الفادح في العلاقات الدولية، واستطاع الفضاء السيبراني خلق تهديدات جعلت الدول تهتم باستراتيجيات معدة خصيصاً لتحقيق الأمن السيبراني الوطني، ومن هنا وجب على المشرعين في مختلف البلاد وضع قوانين اتحادية قبل الاتفاقيات بين الدول للحد من التهديدات السيبرانية، والتعاون مع الشركاء الدوليين لتبادل أفضل الممارسات ومعالجة التهديدات العالمية للبنية التحتية القومية دون المساس بالحريات الرقمية.

وتؤكد **د. لامان محمد**[30] أن السيطرة في الفضاء السيبراني ستكون لمن يملك التقنيات المتقدمة ويتحكم فيها بشكل منفرد، ومن ثمَّ يمتلك السيطرة في هذا المجال، وستكون الحروب القادمة حروباً في الفضاء السيبراني، وينبغي دعم مبادرات البحث والتطوير للنهوض بالتكنولوجيا والمنهجيات، ووضع معايير عالمية في الفضاء الإلكتروني أمر بالغ

---

29) مقابلة مع أ.م.د/ أحمد أبو ذكير.. أستاذ القانون المساعد.. كلية الحقوق.. جامعة قنا، بمكتب سيادته بتاريخ 5 مارس 2025، الساعة 12 ظهراً.

30) محادثة هاتفية مع د. لامان محمد.. رئيس قطاع الذكاء الاصطناعي والميتافيرس في big cloud والرئيس التنفيذي لمنصة bulls club في الولايات المتحدة الأمريكية بتاريخ 6 مارس2025، الساعة 4:15م.

الأهمية للحد من مخاطر الحروب السيبرانية، فنجد اللائحة العامة لحماية البيانات في الاتحاد الأوروبي تضع معايير صارمة لحماية البيانات مع حرية التعبير، علاوة على قانون إنقاذ الشبكة الذي تم تقديمه في إحدى الدول الأجنبية (ألمانيا) لمكافحة خطاب الكراهية والمعلومات المضللة عبر الإنترنت، الذي يفرض على منصات التواصل الاجتماعي إزالة المحتوى غير القانوني بسرعة أو مواجهة غرامات كبيرة، ويهدف القانون إلى جعل البيئة الرقمية أكثر أمانًا واحتراما مما قد يؤدي عن غير قصد إلى قمع حرية التعبير، علاوة على اتجاه الحكومات إلى تطوير قوانين الفضاء الإلكتروني للسيطرة على الهجمات التي تستهدف الأنشطة الإعلامية عبر الإنترنت، وقد تؤثر هذه القوانين على الإعلاميين ومنشوراتهم.

ويؤكد **محمود فرج**[31] أن هناك بعض الدول لم تشرع قوانين لضمان الأمن السيبراني رغم خطورتها مثل ماليزيا، إلا أن قلة تكاليف الحروب السيبرانية مقارنة بنظيرتها التقليدية يحتم ضرورة وضعها في أولويات الدول خاصة لإمكانية الهجوم في أي وقت، مع أهمية إبراز التوجه الدولي لتجديد المنظومة الأمنية وتكييفها مع المتطلبات العصرية بدلا من التمسك بالأساليب الكلاسيكية في العمل الأمني وخلق نظرة برجماتية فاعلة تستطيع تحقيق الأمن الوطني وتحصين المجتمعات من هذه التهديدات والاختراقات السيبرانية، والأدلة والشواهد على هذه الاختراقات لا تعد ولا تحصي منها في سبتمبر2023 ، حيث شن قراصنة إيرانيون هجوماً إلكترونياً على شبكة السكك الحديدية الإسرائيلية، واستخدم المتسللون حملة تصيد لاستهداف البنية التحتية الكهربائية للشبكة، كما ورد أن شركات برازيلية وإماراتية استهدفت في الهجوم نفسه.

وفي سبتمبر2023 حذَّر المسؤولون الأمريكيون واليابانيون من أن المتسللين الصينيين الذين ترعاهم الدولة وضعوا تعديل برامج داخل أجهزة التوجيه لاستهداف الصناعات والشركات الحكومية الموجودة في البلدين، واستخدم المتسللون ثغرات البرامج الثابتة للبقاء مختبئين والتحرك في شبكات استهدافهم ونفت الصين هذه المزاعم، وفي 2023

31) مقابلة مع محمود فرج.. مدرب دولي معتمد في الذكاء الاصطناعي شركة هواوي العالمية، بتاريخ 20 فبراير 2025، الساعة 8:00م.

أصاب هجوم إلكتروني ضخم برمودا لإدارة التخطيط والخدمات الحكومية مثل المستشفيات، والنقل، إلى أن توقفت هذه الخدمات لعدة أسابيع، وأعلنت برمودا أنها تحقق في الهجوم، ورفضت ذكر ما إذا كانت هناك أي بيانات حساسة تم اختراقها، وفي 2023 أيضًا استهدف مجرمو الإنترنت وزارة الكويت باستخدام هجوم الفدية "التصيد"، وفرضت الكويت أنظمة لحمايتها من هجمات أخرى محتملة، وفي سبتمبر2023 استطاع مجرمو الإنترنت الروس خرق أنظمة تكنولوجيا المعلومات في المحكمة الجنائية الدولية وسط تحقيق مستمر في الحرب الروسية وسط الجرائم المرتكبة في أوكرانيا، وتوضح هذه الأمثلة أهمية إعطاء الأولوية للأمن السيبراني وتطوير استراتيجية وطنية متماسكة للأمن السيبراني مع مجموعة من المبادرات، من بينها حماية البنية التحتية للبلاد، وتعبئة الاستجابة للحوادث السيبرانية، وتحديد معايير الأمن السيبراني، وتحسين الوعي السيبراني للمواطنين، وتطوير قدرات الأمن السيبراني للمهنيين.

ويبرهن على الكلام ذاته أ.د **عبد العزيز السيد**[32]، قائلًا بأنه في مايو 2017 تعرضت وكالة الأنباء القطرية (QNA) للاختراق، مما أدى إلى نشر تصريحات مُفبركة نُسبت إلى أمير قطر، وبدت هذه التصريحات وكأنها تُعبر عن دعم إيران وحماس، مما أثار ردود فعل دبلوماسية غاضبة من عدة دول خليجية، بما في ذلك المملكة العربية السعودية والإمارات العربية المتحدة والبحرين، وقطر، ومصر، ويُبرز اختراق وكالة الأنباء القطرية الحاجة المُلحة للمؤسسات الإخبارية للتحقق من صحة مصادرها بدقة، ونشرت وسائل الإعلام الإقليمية والدولية في البداية هذه البيانات المُلفقة، مُسلّطةً الضوء على تحديات تحديد المعلومات الكاذبة، ويُظهر الانتشار السريع للمعلومات الكاذبة إمكانية حدوث عواقب وخيمة عند نشر أخبار زائفة غير مُتحقق من صحتها، ويُبرز هذا الحادث دور الصحافة في تصعيد الصراعات الجيوسياسية المحتملة من خلال نشر المعلومات المضللة، وعقب الاختراق، واجهت وسائل الإعلام انتقادات مكثفة لدورها في نشر الأخبار الكاذبة.

---

32) مكالمة هاتفية مع أ.د / عبد العزيز السيد عبد العزيز.. أستاذ الصحافة، وعميد كلية الإعلام جامعة بني سويف، بتاريخ 2028 فبراير 2025، الساعة 10:00م.

وتُسلّط هذه القضية الضوء على المسئوليات الأخلاقية للصحفيين في منع نشر المعلومات المضللة وأهمية الحفاظ على ثقة الجمهور، وعقب الاختراق، وُجّهت دعوة دولية لإجراء تحقيق بمشاركة مكتب التحقيقات الفيدرالي (FBI) وهيئات دولية أخرى معنية بالأمن السيبراني، علاوة على الإجراءات القانونية التي اتخذتها قطر لمعالجة الاختراق، ودور التعاون الدولي لتعقب الجناة، والنقاشات الواسعة النطاق حول معايير وقوانين الأمن السيبراني على المستوى الدولي، وخاصةً فيما يتعلق بالأنشطة السيبرانية التي ترعاها الدول، مما يشير إلى أهمية التعاون الدولي في مجال الأمن السيبراني، وآثار قوانين الحرب السيبرانية، والاعتبارات الأخلاقية في التغطية الإعلامية في ظل الأوضاع الجيوسياسية شديدة الحساسية، إضافة إلى الخطوات التي ينبغي على وسائل الإعلام اتخاذها للتحقق من المعلومات في عصر يشهد تطوراً متزايداً في التلاعب الرقمي.

ثامنًا: الأطر القانونية والتشريعات السيبرانية المنظمة لطبيعة العمل الصحفي

تهدف الأطر القانونية والتشريعات السيبرانية المنظمة لطبيعة العمل الصحفي إلى حماية حرية الصحافة وضمان التوازن بينها وبين مسؤولياتها القانونية، وتحدد هذه التشريعات قواعد سلوك الصحفيين في المجال الرقمي، بما في ذلك نشر المعلومات، وقواعد التعامل مع المصادر، وحماية الخصوصية، وتجنب التشهير أو النشر الكاذب .

يؤكد **أ.م.د. عباس مصطفى**[33] ضرورة الحاجة إلى أطر قانونية مرنة تتماشي مع الطبيعة الديناميكية للبيئة الرقمية في مصر، وأهمية صياغة إطار قانوني لموائمة احتياجات المؤسسات الإعلامية من الأمن السيبراني مع الحفاظ على حرية التعبير والذي يعد تحد حتمي في العصر الرقمي لا سيما في المشهد الإعلامي الرقمي، فنجد المادة 31 من الدستور المصري تنص على أن " أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي.

وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون"، واستطاعت جمهورية مصر العربية الانتهاء من المحور الأول للهيكل التشريعي لقوانين

---

33) مقابلة مع أ.م.د/ عباس مصطفى.. استاذ القانون المساعد.. كلية الحقوق.. جامعة قنا، بتاريخ 7 فبراير 2025، الساعة 12 ظهراً بمكتب سيادته.

الأمن السيبراني (تجريم الجاني)، وقانون مكافحة جرائم تقنية المعلومات 175 لسنة 2018، والانتهاء من اللائحة التنفيذية (قانون مكافحة جرائم تقنية المعلومات)، والانتهاء من البند الأول للمحور الثاني قانون حماية البيانات الشخصية 151 لسنة 2020، وجاري اعتماد اللائحة التنفيذية للقانون، أما بالنسبة للبند الثاني للمحور الثاني، فجاري العمل على إعداد مسودة لقانون الأمن السيبراني، إضافة إلى الدور العظيم للهيئة الوطنية للأمن السيبراني وهي تتبع رئيس الوزراء وتختص بتنظيم العمل في مجال الأمن السيبراني والإشراف على تنفيذ القوانين والالتزامات في ذات المجال في قطاعات الدولة المختلفة، هذا ويحدد قانون الأمن السيبراني ولائحته التنفيذية صلاحيات ومسئوليات الهيئة والمراكز القطاعية التابعة كافة، وتهدف التشريعات السيبرانية إلى جعل بيئة الإعلام الرقمي أكثر أمانًا وأكثر احترامًا.

ويؤكد **محمود فرج**[34] على حادثة "الفلبين سنة 2000 م، المعروفة باسم "أحبك"، حيث تم إرسال دودة "أحبك" من خلال بريد إلكتروني في سطر الموضوع "أحبك"، الذي أغرى المستخدمين بفتح المستند، ثم انتشرت الدودة عبر الكمبيوتر ونسخت نفسها إلى جميع جهات الاتصال المدرجة في قائمة جهات اتصال المستلم، وفي غضون ساعات انتشرت بالفعل في آسيا وأوروبا وأمريكا الشمالية، وتسببت في زيادة التحميل على أنظمة خادم البريد الإلكتروني مما تسبب في خسائر مالية فادحة للمنظمات، وقد قُدِّر تأثيرها بنحو 10 مليارات دولار، وقد أبرز هذا الهجوم الإلكتروني ضرورة وجود أطر قانونية للأمن السيبراني والجرائم الافتراضية واستراتيجيات للأمن السيبراني على المستوى الدولي.

ويرى **أ.د حلمى محسب**[35] أن الأمن الرقمي للصحفيين ومصادرهم يتعرض للتهديد في مختلف أنحاء العالم، وقد أصبحت تهديدات الأمن السيبراني، على وجه الخصوص، أكثر أهمية من أي وقت مضى بالنسبة لوسائل الإعلام العالمية، حيث أصبح الصحفيون

---

[34]) مقابلة مع محمود فرج.. مدرب دولي معتمد في الذكاء الاصطناعي شركة هواوي العالمية، بتاريخ 20 فبراير 2025، الساعة 8:00م.

[35]) مقابلة مع أ.د حلمي محمود محسب.. عميد كية الإعلام وتكنولوجيا الاتصال، جامعة قنا، بتاريخ 5 مارس 2025، الساعة 10:00ص.

والناشرون أهدافًا بارزة للبرمجيات الخبيثة وبرامج التجسس والمراقبة الرقمية، مما يعرض معلوماتهم الشخصية ومعلومات مصادرهم للخطر ويهدد سلامتهم، ولقد حظي الأمن الرقمي والأمن السيبراني باهتمام صانعي السياسات عالمياً، حيث سنّت 156 دولة تشريعات لمكافحة الجرائم الإلكترونية اعتباراً من عام 2021.

وتؤكد **د.لامان محمد**[36] أن جميع أنواع الهجمات تشكل تهديدًا واضحًا على العملية التشريعية والملفات المحملة على المواقع الإعلامية بسبب تعطيل نقل المعلومات أو تزييفها، ويعد شكلًا من أشكال التضليل الإعلامي، لذلك من الضروري تطبيق جدار حماية موثوق به يمنع وصول أطراف غير مصرح به، مع أهمية قوانين الفضاء الإلكتروني ليست لمنتجي المعلومات ولكن أيضا لمستخدمي الإنترنت القادرين على الوصول لهذه المعلومات عبر الإنترنت، وتشديد العقوبات على المهاجمين خاصة وأن الفضاء السيبراني سيصبح مجال للهجمات والحروب وتصفية الحسابات، ومن هنا تأتي أهمية قوانين الفضاء الإلكتروني لحرية الصحافة وحقوق المواطنين العامة في حرية التعبير، مع ضرورة اعتماد مسودة قانونية للأمن السيبراني لحماية الإعلام الرقمي باعتباره جزء لا يتجزأ من مجالات الإعلام، وان يخضع الإعلام الزائف لقوانين الجريمة الإلكترونية، وتصميم وتطوير إطار قانوني للأمن السيبراني لمعالجة جميع لأنواع الجرائم السيبرانية.

وفقًا للنتائج السابقة استطاعت الباحثة أن تقدم مقترح مسودة قانون للتشريعات السيبرانية المنظمة لبيئة الإعلام الرقمى ومكافحة الأخبار الزائفة، ممثلة في الآتى:

- احترام سيادة الأراضي المصرية وسلامتها ووسائل إعلامها.
- حرية التعبير جزء مهم من المجتمع الديمقراطي الليبرالي.
- المساءلة الديمقراطية يمكن أن تصبح ممكنة من خلال حرية التعبير.
- حرية التعبير المدعومة بوسائل الإعلام يمكن أن تحمي الحقوق الأخرى للمواطن.
- لكل فرد الحق في الكرامة والخصوصية.

---

[36]) محادثة هاتفية مع د. لامان محمد.. رئيس قطاع الذكاء الاصطناعي والميتافيرس في big cloud والرئيس التنفيذي لمنصة bulls club في الولايات المتحدة الأمريكية بتاريخ 6 مارس2025، الساعة 4:15م.

- يعد تأمين البيانات والشبكات السيبرانية ذا أهمية قصوى للمؤسسات الإعلامية من الأفراد إلى الدول.
- يصبح المجلس الأعلى للإعلام السلطة الوطنية المختصة ونقطة الاتصال الفردية لأغراض شعبة الأمن السيبراني الوطنية مع مختلف المواقع الإعلامية، وتزويدها بفريق متخصص من وزارة الاتصالات متخصص في الفضاء الإلكتروني، وتخصيص مبالغ أمنية مناسبة من الموازنة العامة لتطوير الفريق إدارياً لإنشاء وحدات أمنية متخصصة بالمخاطر السيبرانية.
- يحدد المجلس الأعلى للإعلام معايير الأمن السيبراني، وإصدار إرشادات للحماية من التهديدات السيبرانية وتطوير سياسات الأمن السيبراني، التي تهدف إلى إحباط القرصنة والتصيد والبرمجيات الخبيثة بما لا ينتهك حقوق حرية التعبير والإعلام.
- معالجة البيانات الشخصية للإعلاميين والصحفيين بشكل قانوني وعادل وشفاف، وحمايتها من أي تهكير غير أخلاقي أو القضاء على التهديدات السيبرانية حال حدوثها، ويتم جمعها لأغراض محددة وصريحة ومشروع وليس أكثر من ذلك، وتقتصر على ما هو ضروري فيما يتعلق بالغرض من معالجة البيانات؛ وأن تكون هذه البيانات دقيقة وحديثة.
- احترام خصوصية الإعلامي بما فيها أسماء وعناوين ومراسلات وتنقلات الإعلاميين الإلكترونية، وهذه البيانات جزء من الخصوصية التي يجب ضمانها.
- حرية وسائل الإعلام وفتح الفضاء الإلكتروني ومنح الأفراد الحرية الكاملة في الوصول إلى محتوياته أو النشر من خلاله ومعاملته معاملة مساوية لوسائل الإعلام الأخرى.
- تقليل الرقابة الأمنية على وسائل الإعلام.
- إنشاء أدوات وتقنيات دفاعية وتدابير مضادة، توصي باتخاذ التدابير المضادة المناسبة والتقنيات الدفاعية للمحلل الأمني عند الاستعلام عن تقنية الهجوم، التي يمكن أن تساعد على تسريع عملية صنع القرار لإنتاج رد فعل سريع.

- تنفيذ ضوابط أمنية على منصات التواصل الاجتماعي للحد من المعلومات المضللة والحفاظ على حرية التعبير.
- اعتماد أطر متعددة الأبعاد على أن تجمع استراتيجيات الأمن السيبراني للمؤسسات الإعلامية بين المقاييس التكنولوجية والتحليلات النفسية من أجل خطط دفاع أكثر آلية.
- أن تمتلك المؤسسات الإعلامية أكثر من نموذج أمان مقترح للهجمات الإلكترونية المختلفة سواء (فدية – تجسس – الصفري – إلخ...)، حيث يمكن التنبؤ بطبيعة الهجمات بسهولة وبشكل أكثر سرعة.
- التعاون مع الشركاء الدوليين لجمع وتحليل معلومات التهديدات العالمية.
- إنشاء البروتوكولات الدولية للاستجابة المشتركة للهجمات الإلكترونية واسعة النطاق التي تستهدف البنية التحتية للمؤسسات الإعلامية.
- تتبع اتجاهات الجريمة الإلكترونية المتطورة قبل حدوثها.
- تطبيق لوائح ومعايير الأمن السيبراني داخل كل الأقسام بمختلف المؤسسات الإعلامية.
- مسائلة المؤسسات الإعلامية عن عدم الامتثال للأنظمة المعمول بها واتخاذ إجراءات لذلك.
- التحقيق في الحوادث والانتهاكات السيبرانية للفضاء الإعلامي، وجمع وتحليل معلومات التهديد.
- مراقبة التهديدات السيبرانية ونقاط الضعف واتجاهات الهجوم لتحذير المؤسسات الإعلامية وإعدادها بشكل استباقي.
- إنشاء منصات آمنة عبر مواقع التواصل الاجتماعي لتبادل المعلومات.
- تسهيل التبادل الأمن لمعلومات التهديدات بين الجهات الحكومية وكيانات القطاع الخاص والشركاء الدوليين .
- تنبيه المؤسسات الإعلامية بالتهديدات الناشئة ونقاط الضعف، وأطر مواجهتها.
- تطوير وتقييم الفضاء السيبراني للمواقع الإعلامية بصفة دورية .
- توفير بيئات آمنة لاختبار خدمات الأمن السيبراني والتحقق منها.

- تيسير التعاون الدولي رداً على الهجمات الإلكترونية واسعة النطاق والتهديدات العالمية .
- دمج (الذكاء الاصطناعي) في استراتيجيات الأمن السيبراني لحماية الأنظمة عبر الإنترنت من التهديدات السيبرانية.
- تدريب أنظمة الذكاء الاصطناعي لتمكين التشغيل التلقائي من الكشف عن التهديدات السيبرانية، وتوليد التنبيهات، وتحديد خيوط جديدة من البرامج الضارة، وحماية المؤسسات الإعلامية وحماية البيانات الحساسة.
- تسخير الذكاء الاصطناعي في الأمن السيبراني– مثل التعلم الآلي، وتمثيل المعرفة والاستدلال، واللغة الطبيعية المعالجة من أجل دفاع إلكتروني أكثر آلية وذكاء.
- ضمان المساءلة عن اختراقات البيانات والمعلومات الهامة والحساسة بالمؤسسات الإعلامية.
- تلتزم المؤسسات الإعلامية بالمتطلبات التنظيمية، ليس فقط لأنه التزام قانوني ولكن أيضاً لأنه يوفر إطارا أمن إلكتروني قوي.
- لا يجوز لمزودي خدمة تقديم المحتوى الإعلامي تقديم محتوى غير لائق أو فاحش أو كاذباً أو مهدداً أو قبيحاً لغرض ما، من خلال اختراق المواقع الإعلامية والصحفية بنية مضايقة أو إساءة أو تهديد شخص ما، وعديد من هذه الأنشطة مثل التنمر الإلكتروني أو المواد الإباحية أو نقل الفيروسات أو نشر الافتراء، أو حتى الأخبار المزيفة، تعتبر جريمة بموجب القانون وفي حالة مخالفة المادة، فقد تخضع لغرامة والسجن، وهي غرامة لا تتجاوز خمسين ألف جنيه أو السجن لمدة لا تتجاوز سنة واحدة.
- في حال انتهاك قواعد تقديم محتوى مزيف عبر منصات التواصل الاجتماعي أو التهديد بقصد مضايقة الآخرين قد يكون عرضة لغرامة مالية لا تتجاوز 50000 جنيه مصري أو السجن لمدة لا تتجاوز سنة واحدة أو كليهما .
- إدانة شخص ما يقدم معلومات خاطئة دليل على ارتكاب جريمة، بدفع غرامة مالية لا تتجاوز 50000 جنيه مصري أو السجن لمدة لا تتجاوز 10 سنوات أو كليهما .

- تعزيز السلطات الإشرافية بالمؤسسات الإعلامية إلى تشريعات الأمن السيبراني الخاصة بالمجلس الأعلى للإعلام، مع فرض عقوبات في حالة عدم الامتثال، ويتمثل الحد الأقصى للغرامة المالية المطبقة من 100 ألف إلى 200 ألف جنيه مصري من إجمالي المبيعات السنوية للمؤسسة الإعلامية.
- الكشف المبكر عن الهجمات في وقتها الحقيقي من خلال استخدام "حساسات Sensors" على الشبكات والبرامج والتطبيقات، إضافة إلى توظيف المعلومات الاستخباراتية لرصد أي نشاط غير طبيعي قد يصنف على أنه هجمات سيبرانية، وبداية مواجهتها واحتوائها قبل أن تبدأ نشاطها في الشبكة أو النظم المستهدفة في المؤسسات الإعلامية.
- توافر ظاهرة الهجوم السيبراني الاستباقية لدى كل مؤسسة إعلامية، من خلال استخدام ونشر "الديدان البيضاء Worms White"، وهي برامج قادرة على اكتشاف التطبيقات الضارة وتدميرها قبل توظيفها في إطلاق هجمات سيبرانية محتملة، وتدمير أدوات وبرمجيات القراصنة، مما يساعد على إحباط مخطط الهجمات نفسها، وتحديد هوية ومصدر الهجمة، بما يمكن من إطلاق هجمة إلكترونية مضادة فيما تعرف بـ" الاختراق العكسي back-Hack".

خاتمة الدراسة:

- تمثل الدراسة الراهنة محاولة لوضع مسودة قانون للتشريعات السيبرانية المنظمة لطبيعة العمل الصحفي، والحد من الجرائم الافتراضية التي تتعرض لها المؤسسات الإعلامية، والقضاء عليها، وأهمية التفطن الدائم والاستعداد المستمر لأي هجمة قد يتم التعرض لها، والتعاون الدائم مع الدول من أجل التصدي للهجمات السيبرانية وحماية مجالها، مع تشديد القوانين والعقوبات على المهاجمين، خاصة وأن الفضاء السيبراني أصبح مجال للهجمات والحروب وتصفية الحسابات.
- أصبح الأمن السيبراني مصدر قلق مجتمعي، خاصة في المؤسسات الإعلامية، نتيجة عديد من التهديدات ونقاط الضعف، مثل البريد المزعج والمتسللين، واختراق البيانات والتجسس وفيروسات الكمبيوتر وسرقة الهوية، وهجمات رفض الخدمة الموزعة،

والنقر على روابط احتيالية مرسلة عبر البريد الإلكتروني، والقرصنة عبر الإنترنت، والمراقبة الدولية الجماعية، والتسلط عبر الإنترنت، ونشر الأخبار الزائفة، كما تمثل الحرب الإلكترونية أمثلة حية للمخاوف الإلكترونية والمتصيدون عبر الإنترنت والإيذاء السيبراني.

- هناك عديد من المخاوف بالغة الأهمية بشأن إدارة معلومات المؤسسات الإعلامية، منها حماية الخصوصية بشأن الاتصالات المخزنة إلكترونياً؛ وضمان صحة المعلومات؛ وحماية حقوق الملكية أو الملكية المرتبطة بالمعلومات؛ وتسهيل الوصول إلى المعلومات، وقد تواجه المؤسسات الإعلامية مزيداً من التعقيدات بسبب إمكانية وجود أشكال عديدة متناقضة وغير متوافقة من التكنولوجيا تتعايش في وقت واحد، مما يجعل من الصعب على المنظمات تحديد نقطة دخول مخاطر الأمن السيبراني بسرعة.
- هناك عديد من التهديدات السيبرانية الموجودة على صفحات المواقع الإعلامية بمنصات التواصل الاجتماعي، مثل: فقدان الإنتاجية- التنمر الإلكتروني – المطاردة الإلكترونية – سرقة الهوية – العلامات التجارية- تلف السمعة الشخصية – خرق البيانات – البرامج الضارة – انقطاع الخدمة – الاختراق – الوصول غير المصرح به إلى حسابات القيادات الحكومية وحسابات الإعلاميين عبر وسائل التواصل الاجتماعي، وصولًا إلى حسابات الجمهور، علاوة على نشر الأخبار الزائفة التي تعد أحد أشكال الجرائم الافتراضية في الفضاء الإلكتروني، حيث أسست الحكومات في الأنظمة الاستبدادية، مثل روسيا وكمبوديا وفيتنام، الأخبار الزائفة كتهديد وجودي للأمن القومي بما يضاهي الإرهاب والحرب الإلكترونية، في حين سعت لتمرير قوانين تهتم بحرية وسائل الإعلام وحرية الرأي والتعبير.
- على الرغم من أهمية الأمن السيبراني في مكافحة الجرائم الافتراضية، فإنه يمكن أن يكون له تأثير مخيف على حرية التعبير واتاحة المعلومات، على سبيل المثال يمكن أن يؤدي الاستخدام المفرط لمراقبة المحتوى إلى الرقابة غير المقصودة على المحتوى الشرعي، الذي يزيل المحتوى المثير للجدل ولكنه غير قانوني، وهذه الرقابة غير

مقصودة، لا تقمع الأصوات الفردية فحسب، ولكن تقلل من تنوع وجهات النظر المتاحة على الإنترنت.

- تستطيع الدول أن تستخدم ذريعة الأمن السيبراني لتبرير مراقبة الاتصالات الرقمية بما ينتهك حقوق الخصوصية ويخنق حرية التعبير، وقد تنخفض حرية المواطن مع سعي الدول لتأمين أنظمتها سيبرانيًا، ويجب أن تكون جميع عمليات الأمن السيبراني شفافة وقائمة على مبادئ النزاهة، وأن تكون سياسات الأمن واضحة ومفهومة للجميع، ويجب تجنب أي ممارسات خادعة أو مخادعة، وينبغي تطبيق إجراءات صارمة لحماية هذه المعلومات من الوصول غير المصرح به، وتحمل المسئولية عن أي فشل أمني أو انتهاك للقواعد الأخلاقية والمهنية، ويجب أن تتضمن الإيديولوجية إجراءات واضحة لتحديد المسئولية اتخاذ الإجراءات الموضوعية، وحماية البنية التحتية الرقمية ودعم الحق في حرية التعبير، وإتاحة المعلومات وعدم تغييرها أو تزييفها.
- يساعد الأمن السيبراني على حماية الملكية الفكرية وحماية الأصول من السرقة والقرصنة، حيث تعتبر الملكية الفكرية، مثل المحتوى الأصلي والأخبار الحصرية، من أهم أصول المؤسسات الإعلامية، إضافة إلى الامتثال للقوانين واللوائح حيث تخضع المؤسسات الإعلامية لعديد من القوانين واللوائح المتعلقة بحماية البيانات والخصوصية، ويساعد الأمن السيبراني على ضمان الامتثال لمثل هذه القوانين، وتجنب العقوبات القانونية، وأيضًا زيادة الوعي الأمني.
- وفقًا لنظرية دافع الحماية (PMT)، ينبغي أن تحرص المؤسسات الإعلامية على تزويد الصحفيين بنظام معلومات مؤسساتهم الصحفية، وكيفية الحفاظ على معلوماتهم وأخبارهم وهويتهم الشخصية من الهجمات الإلكترونية، بما يُحفّز الالتزام بلوائح الأمن السيبراني، وعدم الوقوع ضحية لجريمة إلكترونية، واتباع الإجراءات الوقائية بما يخفف من حدة بعض هجمات الحاسوب، علاوة على استخدام دوافع حماية مناسبة لتشجيع الصحفيين بشكل كافٍ على اتخاذ تدابير الأمن السيبراني

المناسبة، ومساعدتهم على تطبيق أساليب أفضل للأمن السيبراني، مع زيادة توعيتهم بخطورة التهديد واحتمالية وقوعه وفعالية الاستجابة لأمن المعلومات.

- ضرورة اكتساب محللي الأمان للبصيرة السيبرانية في المواقع الإعلامية، وأن يتوفر لديه نظرة ثاقبة عن التهديدات السيبرانية وهجمات الأمن السيبراني والمخاطر السيبرانية مثل نقاط الضعف والاستغلال والحوادث الأمنية واختراق البيانات والجرائم الإلكترونية، خاصة تهديدات الأمن السيبراني في وسائل التواصل الاجتماعي، وهجمات الهندسة الاجتماعية، وعدم وجود سياسة وسائل التواصل الاجتماعي، وتتمثل الهندسة الاجتماعية في هجوم على أمن المعلومات للوصول إلى الأنظمة، ويتضمن هجوم الهندسة الاجتماعية على وسائل التواصل الاجتماعي عدة خطوات، وهي جمع المعلومات، وفحص وسائل التواصل الاجتماعي والمعلومات الداخلية الحساسة، وفي البيئة الرقمية سريعة التطور أحدثت التقنيات الناشئة مثل الذكاء الاصطناعي، والمركبات ذاتية القيادة، وإنترنت الأشياء، والتعلم الآلي، والبلوكتشين، والحوسبة السحابية ثورة في مختلف القطاعات.
- يجب أن تحرص المؤسسات الإعلامية على إدارة مخاطر الأمن السيبراني الجديدة بشكل فعال، فعلى سبيل المثال، يمكن لخوارزميات الذكاء الاصطناعي تحليل كميات هائلة من البيانات لتحديد الشذوذ والنشاط المشبوه الذي قد يشير إلى هجوم إلكتروني على المواقع الإعلامية، إضافة إلى تقنية البلوكتشين التي يمكن استخدامها لإنشاء سجل آمن وشفاف للمحتوى، مما يسهل عليها مشاركة البيانات الآمنة وإدارة الهوية، كما يساعد بلوكتشين على منع اختراق البيانات، ويجعل من الصعب على المهاجمين العبث بالبيانات والمعلومات الصحفية، أما إنترنت الأشياء فهو يقدم مخاطر تتعلق بخصوصية البيانات والوصول غير المصرح به، وإساءة استخدام المعلومات الحساسة.
- تأمين الفضاء الإلكتروني كونها مهمة شاقة تتطلب تقنية كبيرة مقترنة برؤى سلوكية، مع ضرورة وضع إطار أخلاقي شامل يوجه القرارات المتعلقة بالأمن السيبراني في المؤسسات الإعلامية، حيث تعد الأخلاق سلاحاً فعالًا لاتخاذ القرارات السليمة في

بيئة متغيرة، مع تحديد ممارسات الأمن السيبراني الموصى بها لمستخدمي وسائل التواصل الاجتماعي، وأهمية الامتثال للقوانين واللوائح الخاصة بالأمن السيبراني لضمان حماية البيانات وعدم إساءة استخدام الصلاحيات، مع أهمية حماية سرية وخصوصية البيانات ومراقبة التهديدات الداخلية والخارجية، وينبغي للمؤسسات الإعلامية التي تستفيد من وسائل التواصل الاجتماعي أن تجعل الأمن السيبراني أولوية قصوى لحماية بياناتها ومعلوماتها من التعرض للهجوم، أو إساءة الاستخدام، أو الاستيلاء عليها، والاستفادة من الأطراف غير المسئولة لمصلحتهم.

- أهمية التعاون الدولي لحماية الفضاء السيبراني للمؤسسات الإعلامية من الهجمات السيبرانية المتكررة، خاصة وأن مفتاح التغلب على التهديدات السيبرانية المتطورة يكمن في التكيف والابتكار المستمر في مجال الأمن السيبراني.
- اقتراح منهجية لإنشاء انطولوجيا خاصة بالمؤسسات الإعلامية لإنشاء سيناريوهات خاصة بالمجال تتعلق بالتهديدات السيبرانية ونقاط الضعف والهجمات والتدابير المضادة، وإثراء هذه الانطولوجيا برؤى محدثة من خلال تكاملها مع البرمجة اللغوية العصبية ومصادر البيانات المتنوعة، مع ضرورة استفادة المؤسسات الإعلامية من البرمجة اللغوية العصبية لاستخراج المعلومات ذات الصلة من مصادر متنوعة، مثل التقارير والمدونات ووسائل التواصل الاجتماعي، وإنشاء أدوات توصي باتخاذ التدابير المضادة المناسبة والتقنيات الدفاعية للمحلل الأمني عند الاستعلام عن تقنية الهجوم، وأتمتة العلاقة بين التقنيات الهجومية والدفاعية والتدابير المضادة باستخدام نماذج اللغة، وضرورة بناء نموذج لغوي لربط التدابير المضادة الدفاعية بالتقنيات الهجومية، حيث يمكن ان تدمر الهجمات الإلكترونية سمعة المؤسسة الإعلامية، ومن ثمَّ ستفقد ثقة الجمهور والرأي العام.
- يمكن حماية البنية التحتية للمؤسسات الإعلامية من الجماعات الإرهابية من خلال تعزيز تعزيز الأمن السيبراني، وتطبيق ضوابط أمنية مشددة، ومراقبة التهديدات الإرهابية على الإنترنت، وضرورة التعاون مع الجهات الأمنية، ووضع خطط للطوارئ، وإجراء تدريبات للطوارئ، مع أهمية التعاون مع المؤسسات الإعلامية الأخرى لتبادل

المعلومات والخبرات، ومواكبة أحدث التطورات في مجال الأمن السيبراني، مع أهمية الحصول على شهادات الاعتماد في مجال الأمن السيبراني.

- التعاون وتبادل المعلومات مع مختلف أصحاب المصلحة، بما في ذلك الحكومات والمنظمات الدولية والكيانات الخاصة، وتبادل المعلومات الاستخباراتية حول التهديدات وأفضل الممارسات وتنسيق الجهود لمنع الهجمات السيبرانية والاستجابة لها، وينبغي أن تشمل برامج تعزيز التعاون الدولي تطوير استراتيجية التعاون الدولي في مجال الأمن السيبراني، التي تختص بإرساء مبادئ واتجاهات الدبلوماسية السيبرانية المصرية وفتح آفاق التعاون عربيًا وأفريقيًا وعالميًا ورفع مستوي الابتكار بالتعاون مع الشركاء الدوليين على أن تكون وزارة الخارجية المصرية هي الجهة الوطنية المعنية بإدارة هذا الملف.
- تأتي أهمية قوانين الفضاء الإلكتروني لحرية الصحافة وحقوق المواطنين العامة في حرية التعبير، مع ضرورة اعتماد مسودة قانونية للأمن السيبراني لحماية الإعلام الرقمي باعتباره جزء لا يتجزأ من مجالات الإعلام، وان يخضع الإعلام الزائف لقوانين الجريمة الإلكترونية، وتصميم وتطوير إطار قانوني للأمن السيبراني لمعالجة جميع أنواع الجرائم السيبرانية.

التوصيات:

1- محاسبة الدول على الجرائم الإلكترونية المرتكبة داخل حدودها الوطنية.

2- إجراء دراسات تهتم بتأثير التشريعات الإلكترونية لتحديد فعالية وكفاءة مثل هذه السياسات كرادع للبرامج الضارة.

3- إجراء دراسات حالة حول جهود الدول القومية في ردع البرامج الضارة والجرائم الإلكترونية.

4- وضع معايير لاستخدام وسائل التواصل الاجتماعي، بما في ذلك تحديد المخاطر المحتملة، والالتزامات السياسية والقانونية الشاملة، واقتراح قائمة مرجعية لتقييم المخاطر قبل الاستخدام.

5- تعزيز الأمن السيبراني في المؤسسات الإعلامية والصحفية المصرية.

6- تعزيز الوعي بقوانين وأنظمة الأمن السيبراني.

7- النهوض بالتشريع السيبراني للوصول إلى درجة عالية من الاحتراف.

8- زيادة الوعي بالأمن السيبراني بين الإعلاميين والصحفيين.

9- عمل بحوث ودراسات مستقبلية تتناول دور الحملات السيبرانية في استهداف السياسة بشكل عام.

10- إنشاء قوانين سيبرانية جديدة.

11- إنشاء منصة مركزية للأمن السيبراني.

12- العمل على سد الفجوة الأمنية السيبرانية بالمؤسسات الإعلامية.

13- تطوير القدرات البشرية والمادية والتقنية في مجال الأمن السيبراني.

14- الاهتمام بالخطاب العالمي حول الحقوق الرقمية والأمن السيبراني.

15- حماية المواقع الإعلامية ومواقع التواصل الاجتماعي الناطقة باسمها من طيف الهجمات الإلكترونية.

16- بناء نظام رقمي أمن ضد التهديدات السيبرانية وتعزيز بيئة مواتية لخطاب حر ومفتوح واحترام القيم الديمقراطية.

17- تسخير الذكاء الاصطناعي والتعلم الآلي العدائي لتقوية الدفاعات الرقمية وحماية الأصول الرقمية على سلامة الأنظمة عبر الإنترنت.

18- التدفق المستمر للمعلومات والشفافية التامة لضمان تأمين الفضاء الرقمي وحماية الديمقراطية.

19- تطوير استراتيجية وطنية متماسكة للأمن السيبراني مع مجموعة من المبادرات من بينها حماية البنية التحتية الحيوية للبلاد، وتحديد معايير الأمن السيبراني، وتحسين الوعي السيبراني للإعلاميين، وتطوير قدرات الأمن السيبراني للمتخصصين.

20- اقتراح نظام برامجي خاص بالمؤسسات الإعلامية يمكنه اكتشاف الهجمات السيبرانية في الوقت المناسب.

21- تصميم انطولوجيا إدارة الثغرات الأمنية لإعلام المستخدمين بشكل أفضل عن نقاط الضعف والتدابير المضادة.

22- بناء نظام رقمي ليس أمنا فحسب ضد التهديدات السيبرانية بل يعزز أيضا بيئة مواتية لخطاب حر ومفتوح واحترام القيم الديمقراطية.

23- تطوير مبادرات الأمن السيبراني بطرق تحترم وتعزز مبادئ الحرية والخصوصية والخطاب المفتوح.

24- الحاجة الماسة إلى معاهدات دولية تحظي بتأييد واسع لمكافحة الجرائم الإلكترونية.

25- تمويل مبادرات أبحاث الأمن السيبراني.

26- تشريع قانون حرية المعلومات وحماية الخصوصية لتنظيم قضايا الخصوصية والأمن السيبراني.

المراجع:

1) Guerrero, V. L. (2024). Cyber Threats, Cyber Risks, and Cybersecurity Responses: Modeling Whole-Of-Nation Strategy Implementation for American Organizations and Citizens (Doctoral dissertation, Clemson University).

[2](Ebot, A. (2024). Technology Acceptance Model for Adopting Cybersecurity Technology in Small and Medium Business/Enterprise: A Generic Qualitative Study (Doctoral dissertation, Capella University).

3(Gualtier, K. A. (2015). Information operations under international law: A Delphi study into the legal standing of cyber warfare (Doctoral dissertation, Walden University).

4) Moore, M. C. (2014). Development and implementation of government cybersecurity policies and practices for national security and cybercrime (Doctoral dissertation, Walden University).

5(Griffiths, J. L. (2016). Cyber security as an emerging challenge to South African national security (Master's thesis, University of Pretoria (South Africa)).

6) Miranda, R. M. D. F. C. (2016). Cyber Warfare in the Context of International Criminal Law (Master's thesis, Universidade Catolica Portuguesa (Portugal)).

7) Sithole, T. (2024). Impact of Brics cybersecurity regulation on the South African cybersecurity legal landscape (Master's thesis, University of Johannesburg (South Africa)).

8) Shawe, R. (2024). Exploring the Global Impact of Domestic Cyberterrorism on Cybersecurity (Doctoral dissertation, Capitol Technology University).pp 25-26.

9) Smith, A. M. (2024). Federal Organizations Mitigation of Cybersecurity Risks Due to Employees' Use of Social Media During Work Hours: A Systematic Review (Doctoral dissertation, University of Maryland University College).
10(Parra, W. (2022). Deterring Ransomware Through Cyber Legislation (Master's thesis, Utica University).
[11]) Chundu, B., Masamha, T., & Sifile, O. (2025). Cyber-security governance framework pillars for Zimbabwean local authorities. Cogent Social Sciences, 11(1), 2453094.
12) Clanton, E. L. (2024). Least Developed Countries' Digital Access: A Survey of Sustainable Development Goal 9 and Cyber Diplomacy (Doctoral dissertation, Marymount University).
13(Ifeanyi-Ajufo, N. (2023). Cyber governance in Africa: at the crossroads of politics, sovereignty and cooperation. Policy Design and Practice, 6(2), 146–159. https://doi.org/10.1080/25741292.2023.2199960.
14) Barber, I. A., & Kumar, S. (2023). Learning from the ground up: lessons from civil society engagement in addressing the human rights implications of cybercrime legislation. Journal of Cyber Policy, 1–18. https://doi.org/10.1080/23738871.2023.2240331
15(Yan, Z. (2022). The Dual Foundation of Cybersecurity Legislation. Social Sciences in China, 43(3), 4-20.
[16](Broeders, D., De Busser, E., Cristiano, F., & Tropina, T. (2022). Revisiting past cyber operations in light of new cyber norms and interpretations of international law: inching towards lines in the sand?. Journal of Cyber Policy, 7(1), 97-135.
[17](Mačák, K. (2021). Unblurring the lines: military cyber operations and international law. Journal of Cyber Policy, 6(3), 411-428.
18(Akoto, W. (2022). Accountability and cyber conflict: examining institutional constraints on the use of cyber proxies. Conflict Management and Peace Science, 39(3), 311-332.
19) Ebert, H. (2020). Hacked IT superpower: how India secures its cyberspace as a rising digital democracy. India Review, 19(4), 376–413. https://doi.org/10.1080/14736489.2020.1797317
20) Adams, J. (2020). Legal Boundaries of The Cyberspace: Privacy of E-Commerce Transactions in The International Law (Doctoral dissertation, University of Essex).
21) Dunn Cavelty, M. (2018). Europe's cyber-power. European politics and society, 19(3), 304-320.
22) Shawe, R. (2024). Exploring the Global Impact of Domestic Cyberterrorism on Cybersecurity (Doctoral dissertation, Capitol Technology University).
23) قـادري & ,نـور الهـدى. (2023) الجريمـة السـيبرانية وآليـات مكافحتهـا–مواجهـة تحـديات الأمـن السيبراني .المجلة الجزائرية للحقوق والعلوم السياسية.337-321 ,(1)8 .
24بن خليف سارة. (2023). مكافحة الجرائم السيبرانية في التشريع الجزائري & ,) دايرى لبنى.
25) Abbas, Z., Khan, R., Khan, M. Z., & Imran, M. (2023). Cyber Laws and Media Censorship in Pakistan: An Investigation of Governmental Tactics to Curtail

Freedom of Expression and Right to Privacy. Journal of Creative Communications, 09732586231206913.
[26]) Barber, I. A., & Kumar, S. (2023). Learning from the ground up: lessons from civil society engagement in addressing the human rights implications of cybercrime legislation. Journal of Cyber Policy, 1-18.
[27]) Masduki. (2022). Cyber-troops, digital attacks, and media freedom in Indonesia. Asian Journal of Communication, 32(3), 218-233.
28) زناتي, محمد السعيد, جواج & ,يمينة .(2022) أثر الجرائم السبرانية على الحريات الفردية (الجزائر نموذجا .(المجلة الافريقية للدراسات القانونية والسياسية.62-43 ,(1)6 ,
[29](Shandler, R., Gross, M. L., & Canetti, D. (2021). A fragile public preference for cyber strikes: Evidence from survey experiments in the United States, United Kingdom, and Israel. Contemporary Security Policy, 42(2), 135-162.
30(McCurdy, M. (2020). The evolution and legislative response to Nigerian cybercrime (Master's thesis, Utica College).
31) Masood, U. H. B. (2017). Countering Cyber Attacks in Malaysian Law: Assessing the Concept of Cyber Attacks and the Countermeasures (Doctoral dissertation, University of Leeds).
32) Barclay, C. (2017). Cybercrime and legislation: a critical reflection on the Cybercrimes Act, 2015 of Jamaica. Commonwealth Law Bulletin, 43(1), 77-107.
33) White, J. K. (2017). Impact of protection motivation theory and general deterrence theory on the behavioral intention to implement and misuse active cyber defense (Order No. 10622990). Available from ProQuest Dissertations & Theses Global. (1957432791). Retrieved from https://www.proquest.com/dissertations-theses/impact-protection-motivation-theory-general/docview/1957432791/se-2
34(ing Li, Li Xu, Wu He (2022) he effects of antecedents and mediating factors on cybersecurity protection behavior,Computers in Human Behavior Reports, Volume 5, https://doi.org/10.1016/j.chbr.2021.100165.
35) Towbin, R. S. (2019). A protection motivation theory approach to healthcare cybersecurity: A multiple case study (Order No. 13809084). Available from ProQuest Dissertations & Theses Global; Publicly Available Content Database. (2207492982). Retrieved from https://www.proquest.com/dissertations-theses/protection-motivation-theory-approach-healthcare/docview/2207492982/se-2
36(Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks. Information, 13(9), 413. https://doi.org/10.3390/info13090413
37) Shawe, R. (2024) op. cit, p15.
38) Sithole, T. (2024). Impact of Brics cybersecurity regulation on the South African cybersecurity legal landscape (Master's thesis, University of Johannesburg (South Africa)).
39) MacInnes, J., (2020). Exploratory Data Analysis, In P. Atkinson, S. Delamont, A. Cernat, J.W. Sakshaug, & R.A. Williams (Eds.), SAGE Research Methods Foundations. https://doi.org/10.4135/9781526421036889602

40(Atatsi, E. K. (2024). Exploring the use of internships to build practical experience for emerging cybersecurity professionals in order to meet industry work experience requirements (Order No. 31146741). Available from ProQuest Dissertations & Theses Global. (3037345737). Retrieved from https://www.proquest.com/dissertations-theses/exploring-use-internships-build-practical/docview/3037345737/se-2

[41]) أجرت الباحثة مقابلات متعمقة مع عدد من الخبراء، ممثلين في:

أولًا: الخبراء الأكاديميون:

1- أ.د / أحمد حلمي.. أستاذ تكنولوجيا المعلومات.. كلية التربية النوعية.. جامعة قنا.
2- أ.د حلمي محمود محسب.. عميد كية الإعلام وتكنولوجيا الاتصال، جامعة قنا.
3- أ..د / عبد العزيز السيد عبد العزيز.. أستاذ الصحافة ، وعميد كلية الإعلام جامعة بني سويف.
3- أ.د عماد على.. عميد كلية الحاسبات والمعلومات – جامعة قنا.
4- أ.د/ نجلاء فارس.. أستاذ تكنولوجيا المعلومات ، كلية التربية النوعية ، جامعة قنا.
5- أ.م.د/ أحمد أبو ذكير.. أستاذ القانون المساعد.. كلية الحقوق.. جامعة قنا.
6- أ.م.د/ عباس مصطفي.. استاذ القانون المساعد.. كلية الحقوق. جامعة قنا.
7- أ.م.د / هاني فوزي عبد الغني.. أستاذ العلاقات العامة المساعد، ورئيس قسم العلاقات العامة ، كلية الإعلام ، جامعة قنا.
8- محمود فرج.. مدرب دولي معتمد في لذكاء الاصطناعي شركة هواوي العالمية.
9- لامان محمد.. رئيس قطاع الذكاء الاصطناعي والميتافيرس في big cloud والرئيس التنفيذي لمنصة bulls club في الولايات المتحدة الأمريكية.

ثانيًا: ممارسو العمل الصحفي:

1- محمود المملوك.. رئيس تحرير موقع القاهرة 24.
2- إسلام مصطفى.. مدير تحرير الـ Social Media بموقع القاهرة 24.
3- مقابلة مع جمعة حمد الله، رئيس تحرير جريدة المصري اليوم.
4- هشام أبو حديد.. رئيس تحرير جريدة المصري اليوم.
5- حجاج سلامة.. مدير تحرير جريدة الوفد.
6- بسام رجب.. مدير تحرير جريدة الفجر.
7- محمد حمدي.. مدير تحرير جريدة المصري اليوم.
8- أبو المعارف الحفناوي.. مدير تحرير جريدة أخبار اليوم.
9- محمد عصام.. نائب رئيس القسم الاقتصادي، القاهرة 24.

[42](Reality Winner, Former N.S.A. Translator, Gets More Than 5 Years in Leak of Russian Hacking Report - The New York Times

[43]) https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea

[44]) CrowdStrike’s work with the Democratic National Committee: Setting the record straight

References

Guerrero, V. L. (2024). Cyber Threats, Cyber Risks, and Cybersecurity Responses: Modeling Whole-Of-Nation Strategy Implementation for American Organizations and Citizens (Doctoral dissertation, Clemson University).

(Ebot, A. (2024). Technology Acceptance Model for Adopting Cybersecurity Technology in Small and Medium Business/Enterprise: A Generic Qualitative Study (Doctoral dissertation, Capella University).

(Gualtier, K. A. (2015). Information operations under international law: A Delphi study into the legal standing of cyber warfare (Doctoral dissertation, Walden University).

Moore, M. C. (2014). Development and implementation of government cybersecurity policies and practices for national security and cybercrime (Doctoral dissertation, Walden University).

(Griffiths, J. L. (2016). Cyber security as an emerging challenge to South African national security (Master's thesis, University of Pretoria (South Africa)).

Miranda, R. M. D. F. C. (2016). Cyber Warfare in the Context of International Criminal Law (Master's thesis, Universidade Catolica Portuguesa (Portugal)).

Sithole, T. (2024). Impact of Brics cybersecurity regulation on the South African cybersecurity legal landscape (Master's thesis, University of Johannesburg (South Africa)).

Shawe, R. (2024). Exploring the Global Impact of Domestic Cyberterrorism on Cybersecurity (Doctoral dissertation, Capitol Technology University).pp 25-26.

Smith, A. M. (2024). Federal Organizations Mitigation of Cybersecurity Risks Due to Employees' Use of Social Media During Work Hours: A Systematic Review (Doctoral dissertation, University of Maryland University College).

(Parra, W. (2022). Deterring Ransomware Through Cyber Legislation (Master's thesis, Utica University).

Chundu, B., Masamha, T., & Sifile, O. (2025). Cyber-security governance framework pillars for Zimbabwean local authorities. Cogent Social Sciences, 11(1), 2453094.

Clanton, E. L. (2024). Least Developed Countries' Digital Access: A Survey of Sustainable Development Goal 9 and Cyber Diplomacy (Doctoral dissertation, Marymount University).

(Ifeanyi-Ajufo, N. (2023). Cyber governance in Africa: at the crossroads of politics, sovereignty and cooperation. Policy Design and Practice, 6(2), 146–159. https://doi.org/10.1080/25741292.2023.2199960.

Barber, I. A., & Kumar, S. (2023). Learning from the ground up: lessons from civil society engagement in addressing the human rights implications of cybercrime legislation. Journal of Cyber Policy, 1–18. https://doi.org/10.1080/23738871.2023.2240331

(Yan, Z. (2022). The Dual Foundation of Cybersecurity Legislation. Social Sciences in China, 43(3), 4-20.

(Broeders, D., De Busser, E., Cristiano, F., & Tropina, T. (2022). Revisiting past cyber operations in light of new cyber norms and interpretations of international law: inching towards lines in the sand?. Journal of Cyber Policy, 7(1), 97-135.
(Mačák, K. (2021). Unblurring the lines: military cyber operations and international law. Journal of Cyber Policy, 6(3), 411-428.
(Akoto, W. (2022). Accountability and cyber conflict: examining institutional constraints on the use of cyber proxies. Conflict Management and Peace Science, 39(3), 311-332.
Ebert, H. (2020). Hacked IT superpower: how India secures its cyberspace as a rising digital democracy. India Review, 19(4), 376–413. https://doi.org/10.1080/14736489.2020.1797317
Adams, J. (2020). Legal Boundaries of The Cyberspace: Privacy of E-Commerce Transactions in The International Law (Doctoral dissertation, University of Essex).
Dunn Cavelty, M. (2018). Europe's cyber-power. European politics and society, 19(3), 304-320.
Shawe, R. (2024). Exploring the Global Impact of Domestic Cyberterrorism on Cybersecurity (Doctoral dissertation, Capitol Technology University).
-Qadri, Nour El-Hoda. (2023) aljarimat alsiybiraniat waliat mukafahatiha-muajahat tahadiyat al'amn alsiybirani. almajalat aljazayiriat lilhuquq waleulum alsiyasiat 8(1), 321-337..
Abbas, Z., Khan, R., Khan, M. Z., & Imran, M. (2023). Cyber Laws and Media Censorship in Pakistan: An Investigation of Governmental Tactics to Curtail Freedom of Expression and Right to Privacy. Journal of Creative Communications, 09732586231206913.
Barber, I. A., & Kumar, S. (2023). Learning from the ground up: lessons from civil society engagement in addressing the human rights implications of cybercrime legislation. Journal of Cyber Policy, 1-18.
Masduki. (2022). Cyber-troops, digital attacks, and media freedom in Indonesia. Asian Journal of Communication, 32(3), 218-233.
-Zenati, Mohamed. (2022). 'athar aljarayim alsubraniat ealaa alhuriyaat alfardia (aljazayir namudhaja). almajalat alafriqiat lildirasat alqanuniat walsiyasiati, 6(1), 43-62.
(Shandler, R., Gross, M. L., & Canetti, D. (2021). A fragile public preference for cyber strikes: Evidence from survey experiments in the United States, United Kingdom, and Israel. Contemporary Security Policy, 42(2), 135-162.
(McCurdy, M. (2020). The evolution and legislative response to Nigerian cybercrime (Master's thesis, Utica College).
Masood, U. H. B. (2017). Countering Cyber Attacks in Malaysian Law: Assessing the Concept of Cyber Attacks and the Countermeasures (Doctoral dissertation, University of Leeds).
Barclay, C. (2017). Cybercrime and legislation: a critical reflection on the Cybercrimes Act, 2015 of Jamaica. Commonwealth Law Bulletin, 43(1), 77-107.

White, J. K. (2017). Impact of protection motivation theory and general deterrence theory on the behavioral intention to implement and misuse active cyber defense (Order No. 10622990). Available from ProQuest Dissertations & Theses Global. (1957432791). Retrieved from https://www.proquest.com/dissertations-theses/impact-protection-motivation-theory-general/docview/1957432791/se-2

(ing Li, Li Xu, Wu He (2022) he effects of antecedents and mediating factors on cybersecurity protection behavior,Computers in Human Behavior Reports, Volume 5, https://doi.org/10.1016/j.chbr.2021.100165.

Towbin, R. S. (2019). A protection motivation theory approach to healthcare cybersecurity: A multiple case study (Order No. 13809084). Available from ProQuest Dissertations & Theses Global; Publicly Available Content Database. (2207492982). Retrieved from https://www.proquest.com/dissertations-theses/protection-motivation-theory-approach-healthcare/docview/2207492982/se-2

(Sulaiman, N. S., Fauzi, M. A., Hussain, S., & Wider, W. (2022). Cybersecurity Behavior among Government Employees: The Role of Protection Motivation Theory and Responsibility in Mitigating Cyberattacks. Information, 13(9), 413. https://doi.org/10.3390/info13090413

Shawe, R. (2024) op. cit, p15.

Sithole, T. (2024). Impact of Brics cybersecurity regulation on the South African cybersecurity legal landscape (Master's thesis, University of Johannesburg (South Africa)).

MacInnes, J., (2020). Exploratory Data Analysis, In P. Atkinson, S. Delamont, A. Cernat, J.W. Sakshaug, & R.A. Williams (Eds.), SAGE Research Methods Foundations. https://doi.org/10.4135/9781526421036889602

(Atatsi, E. K. (2024). Exploring the use of internships to build practical experience for emerging cybersecurity professionals in order to meet industry work experience requirements (Order No. 31146741). Available from ProQuest Dissertations & Theses Global. (3037345737). Retrieved from https://www.proquest.com/dissertations-theses/exploring-use-internships-build-practical/docview/3037345737/se-2

(Reality Winner, Former N.S.A. Translator, Gets More Than 5 Years in Leak of Russian Hacking Report - The New York Times

https://www.vox.com/2015/1/20/18089084/sony-hack-north-korea

CrowdStrike’s work with the Democratic National Committee: Setting the record straight

Journal of Mass Communication Research «J M C R»

A scientific journal issued by Al-Azhar University, Faculty of Mass Communication

Correspondences

- Al-Azhar University- Faculty of Mass Communication.
- Telephone Number: 0225108256
- Our website: http://jsb.journals.ekb.eg
- E-mail: mediajournal2020@azhar.edu.eg

Issue 75 July 2025 - part 2

Deposit - registration number at Darelkotob almasrya /6555

International Standard Book Number "Electronic Edition" 2682- 292X

International Standard Book Number «Paper Edition»9297- 1110

Rules of Publishing

Our Journal Publishes Researches, Studies, Book Reviews, Reports, and Translations according to these rules:

- Publication is subject to approval by two specialized referees.
- The Journal accepts only original work; it shouldn't be previously published before in a refereed scientific journal or a scientific conference.
- The length of submitted papers shouldn't be less than 5000 words and shouldn't exceed 10000 words. In the case of excess the researcher should pay the cost of publishing.
- Research Title whether main or major, shouldn't exceed 20 words.
- Submitted papers should be accompanied by two abstracts in Arabic and English. Abstract shouldn't exceed 250 words.
- Authors should provide our journal with 3 copies of their papers together with the computer diskette. The Name of the author and the title of his paper should be written on a separate page. Footnotes and references should be numbered and included in the end of the text.
- Manuscripts which are accepted for publication are not returned to authors. It is a condition of publication in the journal the authors assign copyrights to the journal. It is prohibited to republish any material included in the journal without prior written permission from the editor.
- Papers are published according to the priority of their acceptance.
- Manuscripts which are not accepted for publication are returned to authors.