دور مواقع الإعلام الرقمي في حماية الأمن السيبراني

دراسة تحليلية لعينة من المواقع الخاصة بالأمن السيبراني

د. أماني حمدي قرني*

د. إيمان عبد المنعم خطاب**

مقدمة:

تعد الحروب والصراعات وسيلة لتحقيق أهداف وغايات وأجندات سياسية واقتصادية وأمنية وغيرها تتمثل في إرغام العدو والخصوم للامتثال والخضوع لإرادة القوة، ولا شك ان أدوات ووسائل الحروب العسكرية اختلفت وتغيرت بشكل كبير وتغير معها التغطيات الإعلامية وطرق المعالجة، إلى أن استمر التغيير في الشكل والطريقة والمواجهة وبات مع التطور التكنولوجي الإعلام جزءً أساسياً من أدوات الحروب.. وذلك حين دخلنا عالم الفضاء الإلكتروني والحروب السيبرانية .

تستخدم تلك التقنيات للتغلب على الطرف الأخر، فمع تزايد اعتماد الدول على الاتصالات والشبكات الإلكترونية والتحول الرقمي لإدارة البنية التحتية ومفاصل ومؤسسات الدولة، بدأ يتزايد الخطر المحدق الجديد الذي يهدد أوجه الدولة المختلفة وعلى رأسها الأمن القومي.. حيث كانت الهجمات السيبرانية ولا زالت تلحق الضرر والأذى بالاقتصاد الدولي والسياج المجتمعي للدولة.. وكذلك تتحكم في نتائج معارك حقيقية وحسم قرارات دول لصالح المتحكم الأقوى إلكترونيًا.

وغيرت تلك الحروب مفاهيم القوى وعمليات الإرغام، غير أن العدو متخفيًا ويدير المعركة بشكل غير مباشر والهجمات غير معلومة المصدر والرد عليها معقداً جدا وتوقعها أكثر تعقيدًا.. وكذلك سلاحها أخطر ما يكون لإنه بات في يد كل مواطن في مختلف دول العالم متصل بشبكة الإنترنت ومرتبط بإعلام المواطن أو التواصل الإجتماعي.

هذا التطور فرض على الدول البحث في استراتيجيات مختلفة للمواجهة ليس فقط تطوير التقنيات الدفاعية العسكرية، إنما ايضًا وجود انذار مبكر ضد الهجمات الالكترونية وتطوير برامج الحماية والتصدي ، ولجأت بعض الدول لتجنيد محترفي القرصنة والبرمجيات وضمها لقواتها المسلحة، ومن أمثلة ذلك القيادة السيبرانية الامريكية، وقراصنة الظل التابعين للحكومة الروسية، وكذلك قيام عدد من الدول بتأسيس مراكز متخصصة للدفاع السيبراني مثل قيام بريطانيا بتأسيس مركز وطني للتصدي للهجمات الالكترونية المرتبط بشكل مباشر بالاستخبارات البريطانية.

---

* مدرس بقسم الصحافة بكلية الإعلام جامعة بني سويف

** مدرس بقسم الصحافة بكلية الإعلام – جامعة سيناء– فرع قنطرة شرق

كذلك تبنت أمريكا استراتيجية الردع[1].مفادها الهجوم المضاد حال التعرض لأي هجوم، وجاء ذلك على لسان جون بولتون مستشار الأمن القومي للرئيس الامريكي دونالد ترامب حين أعلن عن أول وثيقة رسمية أمريكية للدفاع الإلكترونية في 2018م.

مشكلة الدراسة

تمثلت مشكلة الدراسة في الوقوف على النمط الأكثر إشغالًا لميدان الحروب الداخلية والخارجية الهجمات والحروب السيبرانية بأنواعها المختلفة خاصة المهددة للأمن القومي للدولة المصرية ومن هنا تتبلور مشكلة الدراسة في هذا التساؤل الرئيس: ما دور وسائل الإعلام الرقمي في الحد من الجرائم السيبرانية في مصر؟ وإلي أي مدى يستطيع الإعلام الرقمي مواجهتها؟

أهداف الدراسة

1. التعرف على قضايا الأمن السيبراني التي حظيت باهتمام وسائل الإعلام الرقمية عينة الدراسة.
2. رصد أبرز الهجمات السيبرانية ومخاطرها.
3. معرفة تداعيات الهجمات السيبرانية على الامن القومي
4. التعرف على السبل والإمكانيات المتاحة لمواجهة تلك الحروب.
5. رصد الآليات الإعلامية في مكافحة تلك الجرائم .

أهمية الدراسة

الأهمية العلمية

تأتي الأهمية العملية من خلال تركيزها على التطور التكنولوجي والإعلامي ما بين التحديات الذي تم معالجته في دراسات مختلفة، ومحاولة تقديم حقل جديد لتلك الدراسات المختصة بالحروب السيبرانية وأساليب مواجهتها من الإعلام الرقمي.

الأهمية العملية

إن التركيز على دراسة الحروب السيبرانية ومحاولة تعميق فهمًا خصوصًا في ظل تسارع الاعتماد على الهجمات الالكتروبية وتطور استراتيجياتها، مهم للباحثين وصناع القرار من أجل تطوير استراتيجيات مختلفة تتبنى التصدي لأي هجمة متوقعة مستقبليًا، خاصة وإنالجرائم السيبرانية من الجرائم المستحدثة التي تمثل خطرًا وتهديدًا كبيرًا على الفرد والمجتمع.

تساؤلات الدراسة

1. ماهي صور الجرائم السيبرانية قانونيًا؟
2. ما هي سبل الدول مواجهة الجرائم السيبرانية؟

3. ما هو موقف القانون الدولي من الرائم السيبرانية؟

4. كيفية مواجهة الإعلام الرقي للجرائم السيبرانية ؟

الدراسات السابقة:

انقسمت على النحو التالي:

المحور الأول: الإعلام فى مواجهة المخاطر السيبرانية:

- **دراسة ثيليني هراث وآخرون (2022)**[2] هدفت الدراسة إلي تحديد العوامل التي تؤثر على وعي المستخدمين بالميزات المتعلقة بالأمان في منصات التواصل الاجتماعي وتأثير وعي مستخدمي وسائل التواصل الاجتماعي على سلوكهم في منصات التواصل الاجتماعي، أظهرت نتائج الدراسة أن هناك العديد من التهديدات السيبرانية الموجودة داخل منصة وسائل التواصل الاجتماعي مثل فقدان الإنتاجية ، والتنمر الإلكتروني ، والمطاردة عبر الإنترنت والحمل الزائد على المعلومات الاجتماعية، ضرر بالسمعة الشخصية ، خرق للبيانات ، برامج ضارة ، خدمة المقاطعات والاختراقات والوصول غير المصرح به إلى حسابات وسائل التواصل الاجتماعي. من بين النتائج الأخرى، فكشفت الدراسة أيضًا أن العوامل الديموغرافية، مثل العمر والجنس والمستوى التعليمي، قد لا تكون كذلك بالضرورة عوامل مؤثرة تؤثر على الوعي السيبراني لمستخدمي الإنترنت.

- **دراسة أسماء أحمد أبوزيد (2021)**[3] هدفت رصد وتحليل وتفسير استراتيجيات خطاب صحافة التكنولوجيا العربية في كل من مصر والسعودية تجاه الآمن السيبراني، من خلال تحليل آليات خطابات أبواب التكنولوجيا في الموقع الإلكتروني لصحيفتي "اليوم السابع" المصرية و"عكاظ" السعودية، ومحددات تشكيل تلك الآليات، وكذلك العوامل والمتغيرات المؤثرة في إنتاج هذا الخطاب الصحفي سواء عوامل ومتغيرات مجتمعية، أو عوامل ومتغيرات لها علاقة بالمناخ الصحفي والإعلامي المنتج له، وأشارت نتائج الدراسة إلى توظيف صفحة "علوم وتكنولوجيا" بموقع جريدة اليوم السابع محل الدراسة أسلوب وضوح الأهداف للتأكيد على سعي مصر لإيقاف أي محاولات واختراقات سيبرانية مهما تعاظم اسلوبها وتقنياتها، وتأمين البنى التحتية للاتصالات وتكنولوجيا المعلومات في مختلف القطاعات وخاصة القطاعات الحيوية؛ بالإضافة إلى أهمية الاستعداد اللازم لمواجهة الأخطار السيبرانية المختلفة خاصة هجمات إعاقة الخدمات الحيوية وتخريب البني التحتية، ونشر الفيروسات الخبيثة والهجمات المركزة، وسرقة البيانات الخاصة والهوية الرقمية.

- **هدفت دراسة بشائر حامد قطب (2021)**[4]إلى قياس وعي الصحفيين بمفهوم الأمن السيبراني، والتعرف على أبعاد الآمن السيبراني من وجهة نظر الصحفيين، والتعرف على الأنظمة والتشريعات في مواجهة التهديدات الخارجية والداخلية لتحقيق الأهداف الطموحة التي تنص عليها رؤية 2030، وتوصلت الدراسة إلى عدة نتائج من أهمها أن (84.3%) من عينة الدراسة على معرفة سابقة بمصطلح الأمن السيبراني، أظهرت الدراسة فروق بين

المبحوثين في مدي معرفتهم بمهام ووظائف الهيئة الوطنية للأمن السيبراني، كما ظهر فروق بين المبحوثين في مدي معرفتهم بالأنظمة والتشريعات المتعلقة بالأمن السيبراني.

- **هدفت دراسة شريهان أبو الحسن وسمية عبد الراضي (2021)**[5]إلى تحليل المخاطر السيبرانية للألعاب الإلكترونية القتالية سيمولوجيًا وانعكاسها على التجنيد الإلكتروني للشباب، بالاعتماد على منهج التحليل السيمولوجي؛ لتوصيف وتحليل المخاطر السيبرانية للألعاب الإلكترونية سيمولوجيًا، ومعرفة الدلالات السيمولوجية وانعكاسها على التجنيد الإلكتروني للشباب، و فضلًا عن منهج دراسة الحالة بالتطبيق على لعبة بابجي، باستخدام مجموعات النقاش البؤرية على عدد (50)مفردة من الشباب من عمر (18 /35 سنة) من مستخدمي لعبة بابجي بصورة منتظمة؛ لمعرفة مدى إلمامهم بالمخاطر السيبرانية للعبة، وتوصلت نتائج الدراسة إلى وجود بعض الثغرات السيبرانية في الألعاب الإلكترونية القتالية وفقًا لنظرية اللعبة للأمن السيبراني، والتي تستغلها بعض المنظمات الإرهابية المتطرفة في استقطاب الشباب وتجنيدهم، ومحاولة التأثير عليهم وإقناعهم بمناهجهم ومبادئهم، ومن ثم الانضمام إلى صفوفهم.

- **هدفت دراسة هاني إبراهيم السمان(2021)**[6] إلى الكشف عن دور اليوتيوب في توعية الشباب الجامعي بمخاطر الإرهاب الإلكتروني، ورصد اتجاهات الشباب الجامعي في صعيد مصر نحو معاجلة اليوتيوب لظاهرة الإرهاب الإلكتروني، ومدى متابعته للمضامين المتعلقة به، ودوافع تعرضهم لها، ورصد التأثيرات الناجمة عن تعرضهم للموضوعات المتعلقة بالإرهاب الإلكتروني على موقع اليوتيوب، وتوصلت إلى عدة نتائج أهمها أن فيديوهات الإرهاب الإلكتروني تسهم في توعية الجمهور بخطورة الإرهاب الإلكتروني، وأن اليوتيوب يقدم حلولًا واقعية لكيفية النجاة من هجمات القراصنة الإلكترونية، كما أن اختراق معلومات الأمن السيبراني مرتبط دائمًا منظمات إرهابية هدفها الحصول على المعلومات، وجاءت أهم أسباب التعرض للفيديوهات المتعلقة بمعلومات حول الإرهاب الإلكتروني لحماية أنفسهم وحساباتهم من هجمات الهاكرز المختلفة.

- **دراسة ولاء محمد الطاهر(2021)**[7]هدفت الدراسة التعرف على آليات تنفيذ الاستراتيجية الوطنية للأمن السيبراني في التوعية بأخطار الهجمات السيبرانية والجرائم الإلكترونية ، وذلك من خلال تحليل المواد الإعلامية عبر منصات التواصل الاجتماعي لمركز الأمن الإلكتروني بحكومة دبى الذكية ، حيث أكدت الدراسة أهمية مواجهة التكنولوجيا بوعي كامل ومهارة عالية، وكانت استراتيجية اطلاق البوابات الإلكترونية لتدعيم الوعي بأخطار التقنية الرقمية من أهم استراتيجيات الوعى السيبراني 20.7%، كما أوصت الدراسة بعدد من التوصيات على كافة الأصعدة الدولية والإقليمية والمحلية والمؤسساتية والتي من شأنها تفعيل آليات الوعي السيبراني لدى الجمهور، والعمل على وجود مجتمع أمن معلوماتيًا بحماية الهياكل الأساسية للمعلومات من تلك الهجمات السيبرانية التي تضر بالأمن القومي والعالمي.

المحور الثانى : دور الإعلام الرقمى فى مواجهة الجرائم الإلكترونية:

• **دراسة إردال أوزكايا (2022)**[8] استهدفت الدراسة الطرق التي تضع بها منصات التواصل الاجتماعي المستخدمين بطبيعتها في طريق تهديدات الأمان والخصوصية، وقد افترضت أن منصات التواصل الاجتماعي هي الجناة في زيادة تهديدات الأمن والخصوصية التي يواجهها المستخدمون أظهرت نتائج الدراسة أن المستخدمين أصبحوا حذرين بشكل متزايد من أمنهم عبر الإنترنت بسبب منصات التواصل الاجتماعي، وجد أيضًا أن هناك العديد من مستخدمي وسائل التواصل الاجتماعي الذين يتعرضون لمخاطر الأمان والخصوصية ولكنهم غير مدركين.

• **دراسة أميرة محمد محمد (2021)**[9] سعت الدراسة لوضع رؤية استراتيجية نموذجية متكاملة لمكافحة الجرائم الإلكترونية من زوايا مختلفة يمكن تطبيقها على كافة المستويات، والتي من شأنها حماية المجتمع من الشائعات والأخبار المضللة المثارة على مواقع التواصل الاجتماعي، وتأمين سلامة عمل قطاعات الدولة المختلفة من خلال تحقيق الأمن لها من أي اختراقات وتعزيز الحفاظ على الأمن القومي -من خلال استطلاع آراء الخبراء والمتخصصين عبر ثلاث جولات مختلفة بتطبيق أسلوب دليفي، وأسلوب التخطيط الاستراتيجي، وتوصلت الدراسة إلى تعدد أسباب وأساليب انتشار تلك الجرائم، وتنوع تهديداتها على الأصعدة الاجتماعية والسياسية والأمنية والاقتصادية، كما تعددت الآليات المقترحة ما بين الآليات القانونية والأمنية والتقنية والإعلامية والتربوية والتعليمية، والفنية والدولية للحد من مخاطر وانتشار تلك الجرائم والحفاظ على الأمن السيبراني، وسلامة المجتمع وشبكات البنية الحيوية التحتية وتدعيمها بكل وسائل الأمن والحماية.

• **هدفت دراسة رشا عادل لطفي** (2021)[10] إلى رصد أبرز الاتجاهات البحثية والنظرية، وتقييم نتائجها، وكشف نواحي الضعف فيها، واقتراح اتجاهات جديدة للبحث، اعتمادًا على التحليل الكيفي وتحليل المستوي الثاني لعينة متاحة من الإنتاج العلمي المنشور في دوريات علمية عالمية محكَّمة تتعلق ببحوث جرائم الاتصال عبر الإنترنت وأخلاقياته، كما تهتم الدراسة الحالية برصد مسار تطور الأطر المعرفية والنظرية والمنهجية في تلك البحوث، وهو ما يساعد في وضع خريطة أولية لأجندة الاهتمامات البحثية في هذا المجال. اعتمدت الباحثة على عدد من المناهج البحثية منها: منهج المسح بالعينة، والمنهج المقارن، وتمثلت أداة جمع البيانات في استمارة تحليل، وتوصلت الدراسة إلى أهمية سن القوانين التي تتيح وتكفل حرية التعبير عن الرأي، والقوانين التي تحد من الجرائم الإلكترونية.

• **هدفت دراسة مجدي داغر (2021)**[11]إلى رصد اتجاهات النخبة نحو تطبيقات الذكاء الاصطناعي في انتاج المحتوى الإعلامي، وتقتصر هذه الدراسة على معرفة اتجاهات النخبة المصرية نحو توظيف الإعلام الأمني لتطبيقات الذكاء الاصطناعي في موضوعات الجرائم الإلكترونية وانعكاساتها على دعم وتعزيز الأمن السيبراني في

مصر، توصلت الدراسة إلى عدد من النتائج حيث جاءت النخبة الأمنية أكثر اهتمامًا بمتابعة تطبيقات الذكاء الاصطناعي وتأثيراتها الأمنية على قضايا المجتمع يليها النخبة الإعلامية والأكاديمية، وهو ما يعني اهتمام النخبة المصرية عامة بكل جديد في مجال تكنولوجيا الاتصال وتقنية المعلومات، فيما جاءت النخبة الأمنية هي الفئة الأكثر متابعة لتطبيقات الإعلام الأمني، وهو ما يشير إلى إدراك النخبة المصرية التام لتأثيرات تطبيقات الذكاء الاصطناعي على مكافحة الجرائم الإلكترونية ودعم وتعزيز الأمن السيبراني، ويعزو الباحث ذلك إلى ارتباط الذكاء الاصطناعي بالعلوم الأمنية في تحليل التهديدات والمخاطر ومواجهة البرامج الضارة التي قد تتعرض لها الأنظمة الإلكترونية بالمؤسسات العامة والأمنية ومكافحة الجرائم الإلكترونية بأنواعها، كما توقعت النخبة وجود تهديدات ومخاطر قد تصاحب تطبيقات الإعلام الأمني والتي قد تتمثل في المعالجة السطحية للأحداث بعيدًا عن رؤية وتوجهات المؤسسة الأمنية.

- **هدفت دراسة نرمين نبيل الأزرق (2021)**[12]إلى رصد وتوصيف محددات المسئولية الجنائية لجرائم الاختراق والاعتراض والانتحال وتحليلها كما وردت بالنصوص التشريعية في البلاد العربية، وكيفية مواجهة القوانين لتلك الجرائم، وتقييم الأطر التشريعية الضابطة في الدول العربية والمقارنة بينها من حيث شمول النصوص ووضوحها وآليات الردع ونوعية العقوبة، وما إذا كانت التشريعات تضع ظروفًا استثنائية، وماهية أوجه الشبه والاختلاف بين البلاد العربية محل الدراسة(مصر والإمارات والسودان والأردن) في هذه الأمور القانونية، ومن أهم النتائج التي توصلت إليها الدراسة تميز القانون المصري بتوضيح حالات ارتكاب الجريمة الإلكترونية التي يترتب عليها المسئولية الجنائية لفاعلها بشكل أكبر من القوانين الأخرى، وبشكل عام فلقد خرجت التشريعات العربية محل الدراسة الخاصة بمكافحة جرائم تقنيةش المعلومات من عباءة الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، وجاءت نصوصها القانونية لتتسق إلى حد كبير مع أهداف هذه الاتفاقية.

عينة الدراسة:

تم إجراء دراسة استطلاعية على عينة من صفحات ومواقع الإعلام الرقمي التي تناولت القضايا المتعلقة بالأمن والجرائم السيبرانية وذلك لتحديد عينة الدراسة التحليلية وكانت متمثلة في:

جدول رقم (1) يوضح عينة الدراسة الاستطلاعية

م	الصفحات	عدد المتابعين	ملحوظة
1	صفحة تكنولوجيا المعلومات	213 متابع	
2	الأمن السيبراني العربي	2300 متابع	ليست صفحة ولكنها جروب تفاعلي -يضع المنشورات كل يومين.
3	مركز المعلومات ودعم اتخاذ القرار مجلس الوزراء	4901 متابع	كن موضوعاتها متعلقة بكل الشئون داخل وخارج الدولة المصرية - واقتصرت الموضوعات المتعلقة بالأمن السيبراني على تحركات وقرارات الدولة كإنشاء مجلس أعلى للأمن السيبراني.

4	محترفي أمن المعلومات والأمن السيبراني	5400 متابع	والأغلبية مصري الجنسية اتضح ذلك من خلال التعليقات والتساؤلات المطروحة – وكانت الصفحة تحتوي على عدد كبير من المنشورات.
5	صفحة أم ن المعلومات	741 متابع	وعدد المنشورات المطروحة على الصفحة تحتوي على 20 منشور فقط.
6	أمن المعلومات والشبكات	3300 متابع	هو عبارة عن جروب خاص عدد منشوراته قليلة للغاية.
7	أمن المعلومات) I-Secutiry	29ألف متابع	لأن 90% من المنشورات عبارة عن تفاعلات وتساؤلات من الجمهور العام فقط" أي نشرت بواسطة المتابعين وليس الأدمن"
8	arab_security_cyber_wargames	207 متابع	21 منشور فقط .
9	صفحةEG-CERT	14 ألف متابع	وهي صفحةالخاصة بمجلس الأمنالسيبراني "المصري" فهي متخصصة والتفاعل جيد.

وخرجت الدراسة الاستطلاعية بمجموعة من المؤشرات ومنها:

1. عدم وجود صفحات رسمية متعددة للأمن السيبراني سواء متعلقة بالتوعية بالجرائم أو المواجهة .

2. زيادة عدد الصفحات والمجموعات الخاصة حول الأمن السيبراني مما يؤكد زيع صيته وانتشار معلومات عنه في مختلف المحافظات داخل الدولة المصرية.

3. تفاعل الجمهور مع المنشورات الموجودة في تلك الصفحات وتوجيه أسئلة عديدة لمسؤولي الصفحة.

4. جاءت صفحةEG-CERTالصفحة الرسمية الوحيدة الأكثر تفاعل ونشر وتخصص في موضوع الامن السيبراني.

5. جاءت صفحة محترفي أمن المعلومات والأمن السيبراني ضمن الصفحات المصرية المهتمة بالأمن السيبراني، كما جاءت من أكثر الصفحات تفاعلًا وطرح الموضوعات المتعلقة بالأمن السيبراني على صفحاتها وذلك؛ مختلفة التوجهات حول الأمن السيبراني.

6. اختلفت موضوعًا صفحةEG-CERTبين توعية وإخبار وإشادة بدور الدولة ومشاركة لبرامج حديثة، كذلك شاركتها في نفس التوجه صفحة محترف أمن المعلومات.

7. اعتمدت صفحتي EG-CERT ومحترفي أمن المعلومات على وجود (صور/ فيديوهات /منشورات)

8. فيما جاءت الصفحات العامة الأخرى السابق ذكرها في الجدول أعلى، أقل نشر ودورية التحديث متباعدة وحجم التفاعل بين متوسط وضعيف.

لذا تم اختيار عينة عمدية متمثلة في EG-CERT حيث أنها صفحة رسمية ثرية بالمنشورات مختلفة التوجهات والتفاعل جيد كذلك تم اختيار محترفي والأمن السيبراني لنفس الأسباب عدا كونها تابعة للدولة.

الإطار المنهجي

نوع الدراسة

تعد هذه الدراسة من الدراسات الوصفية التحليلية التي توصف ماهية الإعلام الرقمي والأمن السيبراني وكيفيه مواجهه الاعلام الرقمي للمخاطر السيبرانية .

منهجية الدراسة

للتثبت من صحة فرضية التي انطلقت منها الدراسة، فإنه تم الاعتماد على المناهج التالية:

المنهج الوصفي التحليلي

ينطلق هذا المنهج من توصيف الظاهرة موضع الدراسة، من خلال عرض ما تتميز به من خصائص ومحددات، كما يبحث في أسباب تشكل الظاهرة وتحديد خصائصها المميزة والمختلفة عن غيرها.

وقد تم توظيف هذا المنهج في الدراسة من خلال دراسة واستعراض خصائص الحروب السيبرانية وأنواعها وابعادها على مختلف سياسات واستراتيجيات الدول، ومعالجة وتصدي الإعلام الرقمي لها.

المنهج المقارن

يعتمد هذا المنهج على المقارنة بين ظاهرتين؛ وإبراز أوجه الإختلاف والتشابه للظاهرة محل الدراسة.

وقد تم توظيف هذا المنهج في الدراسة من خلال المقارنة بين معالجة وسائل الإعلام الرقمية المختلفة للحروب السيبرانية.

أدوات جمع البيانات

اعتمدت الدراسة التحليلية على أداتي:

أداة التحليل الاستراتيجي: لرصد نقاط القوة والضعف للمحتوي المقدم في المواقع الخاصة بالأمن السيبراني(EG-CERT صفحة رسمية / صفحة محترفي والأمن السيبراني غير رسمية).

أداة تحليل المضمون: وذلك لتحليل المضمون المواقع الخاصة بالأمن السيبراني للتعرف على المعالجة المطروحة للقضية وتم وضع فئات هذه الاستمارة بعد الرجوع للدراسات في هذا الإطار.

الإطار الزمني:

تم إجراء عينة الدراسة الزمنية خلال 6 شهور فقط.

الإطار المعرفي

الفصل الأول: ماهية الحروب السيبرانية وتطور هجماتها

1- تعريف الحروب السيبرانية وانواعها وخصائصها

- **اصطلاحًا:**

عرفها جون أركويلا وديفيد رونفيلدت بأنها: "تنفيذ العمليات العسكرية، والاستعداد لتنفيذها، وفقًا للمبادئ المعلوماتية، من خلال تعطيل، أو تدمير، نظم المعلومات والاتصالات على أوسع نطاق[13].

وتشمل أيضًا: تدمير العقيدة العسكرية للعدو، التي يعتمد عليها لتحديد هويته، وخططه، وتصرفاته، وأهدافه، والتحديات التي يواجهها، وذلك عبر معرفة كل شيء عن العدو، ومنعه في الوقت نفسه من معرفة أي شيء عن الطرف الآخر، وتحويل ميزان المعرفة ليكون في مصلحة هذا الطرف".

وعرفها جوزيف ناي بأنها: "الأعمال العدائية في الفضاء السيبراني التي لها آثار تعادل أو تفوق العنف الحركي التقليدي.

وعرفها كينيث جيرز بأنها: "القدرة على الدفاع عن والهجوم على المعلومات، من خلال شبكات الحاسب الآلي عبر الفضاء الإلكتروني، بالإضافة إلى شل قدرة الخصم على القيام بهذه الهجمات نفسها. وتشمل هذه الحرب خمسة عناصر رئيس ية، هي: التجسس، والدعاية، والحرمان من خدمة الإنترنت، وتعديل البيانات والتلاعب بها، والتلاعب أيضا بالبنية التحتية.

فيما عرفتها وزارة الدفاع الأمريكية بأنها: (توظيف القدرات السيبرانية بهدف تحقيق غرض أساسي، يتمثل في تحقيق الأهداف أو الآثار العسكرية في الفضاء السيبراني أو من خلاله).

أما مجلس الأمن الدولي أكد انها (استخدام أجهزة الحاسوب، أو الوسائل الرقمية، من قبل حكومة، أو بمعرفة، أو موافقة صريحة من تلك الحكومة ضد دولة أخرى، أو مُلكية خاصة داخل دولة أخرى، بما في ذلك: الوصول المتعمد أو اعتراض البيانات، أو تدمير البنية التحتية الرقمية، وانتاج وتوزيع الأجهزة التي يمكن استخدامها لتخريب النشاط المحلي).

وعرفها عبد القادر محمد فهمي بأنها: هجمات تستخدم فيها المنظومة الشبكية والأجهزة الحاسوبية للدولة، أو الفاعلين من غير الدول، لتعطيل كفاءة السيطرة والقدرة على التحكم في منظومة أجهزة أو شبكات الحاسوب وما تتضمنه من بيانات ومعلومات للفاعلين الآخرين من الدول وغير الدول، أو تقليلها، أو حتى تدميرها، سواء كان ذلك على مستوى البنية التحتية الوطنية للدولة، أو على مستوى منظومات قوتها العسكرية، وبالشكل الذي يعرض الأمن القومي للدولة إلى تهديد جسيم[14].

• **إجرائيًا:**

هي الهجمات التي شنتها بعض الدول مثل روسيا والولايات المتحدة الأمريكية والصين واسرائيل وايران، وكان مسرحها هو الفضاء الالكتروني، بغرض إلحاق الضرر بالمنشآت والبنية التحتية والأهداف العسكرية للدولة التي تعرضت للهجوم[15].

أنواع الهجمات السيبرانية وخصائصها :

شهدت الهجمات السيبرانية تنوع وتطور في اشكالها وأنواعها وكذلك الأدوات والوسائل المستخدمة كبث الفيروسات والبرامج التخريبية والمدمرة للأنظمة والشبكات الحاسوبية، أو اختراق حسابات والوصول إلى معلومات سرية وتسريبها أو الاستفادة منها لأغراض متعددة منها العسكري والأمني والعدائي والسياسي والإقتصادي، حيث عززت تلك الهجمات من مستويات وفرص الحروب اللامتماثلة ، ومن أبرز انواع الهجمات السيبرانية[16] :-

- الاعتداء على معطيات الحاسب الآلي وحرمة الحياة الخاصة
- الاعتداء على حقوق الملكية الفكرية
- الاستيلاء والنصب والاحتيال السيبراني
- الانتحال والتغرير السيبراني
- الابتزاز والتهديد
- التنصت والتجسس
- السطر على اموال البنوك
- الاعتداء على الاخلاق والاتجار بالبشر
- الاعتداء السيبراني على الامن والبنية التحتية للدول
- عمليات الاستقطاب والتجنيد والعمليات الإرهابية

وامتازت الحروب الإلكتروني بخصائص عديدة كانت الدافع وراء اعتماد العديد من الفاعلين الدوليين عليها، ويأتي في مقدمة هذه الخصائص انخفاض تكلفتها بالمقارنة مع أدوات الحرب التقليدية، حيث لا تحتاج لمعدات وجيوش، ومقارنة بما تحققه من نتائج وكذلك الضحايا والخسائر البشرية .

اعتماد الهجمات السيبرانية على مبدأ إخلاء المسئولية، لصعوبة تحديد الجهة الفاعلة أو مكان الهجوم وهذا يصعب تطبيق فكرة الردع، كما أن تلك الهجمات تؤثر على كافة الجوانب والمجالات وليس فقط العسكري، بل يسود خلالها أيضا عمليات التجسس والاستطلاع وجمع المعلومات وتجنيد المخترقين[17]

لا تعرف الحدود المكانية والجغرافية ، وطبيعة الاسلحة والأدوات تعتمد بصفة أساسية على الأجهزة والبرامج ووحدات المعالجة والأقمار الصناعية وغيرها من محددات وتطورات التكنولوجيا.

أي إنها جرائم تتم من خلال اجهزة الحاسوب وشبكات الإنترنت ، وهي جرائم خفية سريعة التنفيذ عابرة للقارات ، وصعبة الإثبات الأدوات السيبرانية وممتلكيها.

أفضل من أشار إلى الفاعلين الحقيقيين في عالم الفضاء والأمن السيبراني، يعد البروفيسور الأميركي جوزيف. اس. ناي، المفكر الأمريكي صاحب رؤية "القوة الناعمة"، وعنده أن هناك عدة قوى حول العالم تمثل العناصر المحركة الرئيسة في هذا المجال:

1) الدول بمختلف أحجامها، كبرى أو صغرى، غير أن الهجومات السيبرانية ربما هي التي تحتاج إلى دول كبرى فاعلة تمتلك بنى تحتية سيبرانية لإحداث خسائر في أعدائها على المستوى الدولي[18].

2) قوى غير دولية "الكيانات الأممية"، وعادة ما يكون لهولاء أهدافًا تخريبية، إلا أن قدرتهم على القيام بعمليات واسعة النطاق تعوزها مساعدة أجهزة استخبارات دولية.

3) وسائط التواصل الاجتماعي العالمية الكبرى مثل "فيسبوك" و"جوجول" وتويتر" وما شابه، وهذه تمتلك قدر من المعلومات يسر لها قدرات تفوق في واقع الحال قدرات بعض الدول.

4) الجماعات الإرهابية، وهنا تتضح المخاطر الحقيقية للعالم السيبراني، إذ تستخدم العصابات الإجرامية هذا الفضاء لسرقة المعلومات وتسهيل كل ما هو غير مشروع من عينة تجارة البشر والسلاح[19] .

5) الأشخاص الاعتياديين، مثل ما رأيناه في ظاهرة ويكليكس، حيث استطاع مخترق للأمن المعلوماتي الأميركي أن يهدد أكبر دولة في العالم، الولايات المتحدة الأميركية، ويكشف أوراقها وتحالفاتها حول الكرة الأرضية.

2- بداية وتطور الهجمات السيبرانية

جاء التطبيق الأول للهجمات السيبرانية مع حرب الخليج الثانية عام 1991م، حين قامت القوات الأمريكية باختراق وتعطيل منظومة الدفاع الجوي العراقي، وتدمير كابلات الألياف الضوئية وشبكة الاتصالات العسكرية الممتدة من بغداد حتى البصرة.

ومع نهاية عقد التسعينات من القرن الماضي برزت الهجمات الإلكترونية المتبادلة بين الهند وباكستان، وذلك على خلفية النزاع بشأن كشمير، حيث زادت عدد الهجمات الإلكترونية سنويًا بين البلدين تصاعاديًا من 45 هجمة عام 1999 إلى 133 هجمة عام 2000 إلى 275 عام 2001م.

في عامي 2009 و2010 م ، برزت الهجمات التي نفذتها الوحدة (8200) الإسرائلية بالتعاون

مع "وكالة الأمن القومي" الأمريكية، على المنشأة النووية الإيرانية، عبر نشر فيروس حاسوبي يطلق عليه اسم "ستوكسنت، الذي استهدف نظام التشغيل لأجهزة الطرد المركزي المستخدمة في تخصيب اليورانيوم، ما أدى إلى جعلها تتحرك بوتيرة خارجة عن السيطرة وأدى بالنهاية إلى تكسرها[20].

وفي عام 2010م، تجددت الهجمات الإلكترونية المتبادلة بين الهنود والباكستانيين، حيث قام

"الجيش السيبراني الهندي"، بشن هجوم استهدف (36) لقاعدة بيانات حكومية باكستانية. وفي عام 2103 م اخترق ذلك الجيش الموقع الرسمي للجنة الانتخابات في باكستان. وردًا على ذلك، قام "جيش السايبر الحقيقي" التابع لباكستان ، باختراق وتشويه مواقع الويب التابعة لهيئات الانتخابات الهندية.

ومع اندلاع النزاع في شبه جزيرة القرم وتدخل روسيا عسكريًا فيه عام 2014م، أعلنت شركة روستك العسكرية الروسية استيلائها على طيارة أمريكية بدون طيار بعد هجمة من التشويش المغناطيسي.

واعلنت وزارة الطاقة الأوكرانية عام 2015 أن متسللين استخدموا شركة إنترنت مقرها روسيا وشنوا هجومًا إلكترونيا منسقًا على شبكة الكهرباء الأوكرانية ، ما تسبب في انقطاعات بالكهرباء في حينه، واعتبرت هذه الحادثة على نطاق واسع أول انقطاع للكهرباء ناجم عن هجوم إلكتروني ، وهذه الهجمات أثر توتر العلاقة بين أوكرايا وروسيا[21].

وفي عام 2017 م أصدر مكتب مدير الإستخبارات الوطنية الأمريكية جيمس كلابر تقريرًا يوضح خلاله الهجمات السيبرانية الروسية ضد أمريكا جراء الانتخابات الرئاسية عام 2016م .

وواجهت بريطانيا في العام ذاته هجوم إلكتروني كبير عرف باسم هجوم ""واناكراي"" الإلكتروني، واستهدف منظومة المعلومات التابعة لوزارة الصحة، ما أدى إلى تعطل في السجلات الطبية لدى مجموعة من المستشفيات، وتوقف بعض المنشآت الصحية عن العمل جراء الأعطال التي تسببت بها هذه الهجمات على أجهزة الحاسوب المتعلقة بالنظام الصحي الإلكتروني وتلف في جزء من بيانات المرضى.

كما تعرضت روسيا خلال استضافتها لبطولة كأس العالم عام 2108 م، لحوالي خمسة وعشرين مليون هجوم إلكتروني على البنية التحتية لتكنولوجيا المعلومات، وفي العام ذاته ذكرت شركة "آريا 1 سيكيوريتي" الأميركية المتخصصة في أمن المعلومات، أن وحدة إلكترونية تابعة لجيش التحرير الشعبي الصيني، اخترقت شبكة اتصالات يستخدمها الاتحاد الأوروبي لتنسيق السياسات الخارجية، حيث تمكن القراصنة من الوصول إلى آلاف البرقيات الدبلوماسية، - بحسب صحيفة نيويورك تايمز – وضمنها تحليلات لتوجهات السياسات العالمية والتجارة، وخصوصا دور الصين وتحولات سياساتها تحت حكم الرئيس شي جينبينغ، وكذلك علاقات الاتحاد الأوروبي مع كل من روسيا والولايات المتحدة الأمريكية.

وفي عام 2019م أعلن نائب مدير المركز التنسيقي الروسي لمواجهة حوادث الحاسوب، نيقولاي موراشوف، أن هجوما سيبرانيًا موسعًا وقع ضد روسيا من الخارج، وذلك في يوم الانتخابات الرئاسية في مارس 2108 م. وبين أن المركز بدأ برصد هجمات سيبرانية اعتبارًا من يونيو 2103 م، وبلغت الهجمات ذروتها يوم فعالية "الخط المباشر" مع الرئيس فلاديمير بوتين في يونيو 2103 م. ومن ثم تجددت الهجمات وتكثفت في مارس 2108م، يوم الانتخابات الرئاسية، واستهدفت تحديدًا تعطيل عمل مراقبة عمليات التصويت عبر الفيديو.

وفي تطور لاحق،كانت إسرائيل من اكثر الدول التي تعلن عن وقفها لهجمات سيبرانية، ففي عام 2020 أعلن جهاز الأمن الإلكتروني الوطني الإسرائيلي، عن إحباط هجوم إلكتروني على منظومة المياه ، تضمن الهجوم على الأنظمة الحاسوبية لست منشآت مياه ومجارٍ في إسرائيل بواسطة قراصنة ، مع الترجيح بوقوف إيران وراء الهجوم، وقد اخترق القراصنة البرمجيات المسؤولة عن التحكم في عمليات تشغيل المحطات، ما أدى إلى توقف أجهزة التحكم الرئيسية فيها. وقد تبين بأن المهاجمين استخدموا خوادم أمريكية لشن الهجوم، وذلك بهدف التمويه[22].

وفي عام 2020 إثرتعرض أمريكا لعمليات قرصنة إلكترونية واسعة النطاق، استهدفت وكالات حكومية أميركية، من بينها إدارة الأمن النووي، ووزارات الدفاع والخارجية والطاقة والخزانة، وشركات خاصة مرتبطة بالحكومة الفيدرالية ، توعد الرئيس جو بايدن الروس، باعتبار أنهم يقفون وراء هذا الهجوم ، وأكد أن الأمن السيبراني سيكون من بين أولويات إدارته.

وفي عام 2022 ظهرت الهجمات السيبرانية خلال الحرب الروسية الأوكرانية، حيث تعرضت شركة تويوتا إلى هجوم سيبراني أوقف كل عملياتها في اليابان .. وذلك جاء فور انضمام اليابان إلى الغرب في فرض عقوبات على روسيا ... ولم تقتصر الهجمات على الشركات فقط بل استهدفت مسئولين أوكرانيين " أعضاء برلمان وسياسيين وممثلي الصحافة والمجتمع المدني"، كما رصد نشر بعض مقاطع الفيديو التي تصور أوكرانيا ضعيفة ومستسلمة لروسيا ، وجنود أوكرانيين يرفعون رايات الاستسلام البيضاء – وذلك وفقاً لبيان صادر عن ميتا بلاتفورمز[23].

3- تداعيات الحروب السيبرانية على الامن القومي

تعددت المخاطر العسكرية وغير العسكرية التي تهدد الأمن القومي وتمثل تحديًا كبيرًا ، وعلى رأسه الحروب والهجمات السيبرانية التي تؤثر على تفاعلات السياسة الدولية[24] ، حيث :-

– تصاعد مخاطر استهداف المنشأت الحيوية (المدنية والعسكرية) مما يؤثر على وظائف تلك المؤسسات.

– الفضاء السيبراني إعادة تشكيل قدرة الأطراف المؤثرة ، ولم يعد هناك قوة أحادية .. بل بات فاعلين متعددين.

– تصاعد القدرات في سباق التسليح السيبراني وتبني سياسات دفاعية سيبرانية لدى الاجهزة المختلفة للدولة .. وتزايد الاستثمار في عسكرة الفضاء السيبراني وليس في الجيوش الحقيقية.

– تشكيل اعباء مؤسسات جديد خاصة بوحدات متخصصة في الحروب السيبرانية وتدريبات على الدفاع السيبراني، وإجراء مناورات لتعزيز الدفاع السيبراني.

– تتبنى معظم الدول المتقدمة استراتيجية حرب المعلومات باعتبارها حرب المستقبل.

وهذا يؤكد أن هناك تغييرًا طرأ على مفهوم الأمن القومي على مستوى التهديدات والفاعلين ، حيث أصبح أخطرها الفضاء السيبراني وعسكرته .

4- الردع الدولي قانونيًا للهجمات السيبرانية[25]

فرض التطور التكنيكي والتكنولوجي لطرق الحروب وظهور الحروب والهجمات السيبرانية تحدي قوي في مبدأ القانون الدولي حول تنظيم أو تأطير قانوني لهذه الهجمات من حيث الإدانة والمسئولية الدولية ، حيث الصعوبة في وجود إثبات مادي حول الهجمة أو فاعلها .

ويذكر في ذلك المحور المبدأ القانوني الأول " مبدأ الإمتناع " : أي الامتناع عن استخدام القوة عموما من قبل أي دولة ضد أي دولة أخرى، والذي جاء النص عليه في الفقرة الرابعة من المادة الثانية من ميثاق الأمم المتحدة، ونصها: (يمتنع أعضاء الهيئة جميعًا في علاقاتهم الدولية عن التهديد باستعمال القوة أو استخدامها ضد سلامة الأراضي أو الاستقلال السياسي لأية دولة أو على أي وجه آخر لا يتفق ومقاصد الأمم المتحدة).

واجته الباحثين في تفسير هذا النص ومن بينهم شين وروسيني الذان أكدا انه من الممكن أن تعد الهجمات الإلكترونية بمثابة خرق واضح لأحكام الفقرة شريطة أن تتسبب بتعطيل أو دمار واسع للبنى التحتية الضرورية في حياة الناس.

ووفقا لهذا الاجتهاد فإن للدولة الحق في الدفاع عن نفسها إيزاء أي هجوم، بغض النظر عن شكله ووسيلته. وقد جاء إعلان وزارة الدفاع الأمريكية عام2011 ليؤكد على هذا الاعتبار، إذ جاء فيه بأن توجيه هجمات إلكترونية ضد الولايات المتحدة الأمريكية، وما ينجم عنها من أضرار، يعني تبرير استخدام القوة العسكرية اللازمة، للرد على هذا الاعتداء، باعتبار ذلك حربًا مبررة وعادلة.

أما المبدأ القانوني الثاني الذي بالإمكان تكييف الهجمات الإلكترونية وفقا له فهو مبدأ وجوب التمييز بين المدنيين والمقاتلين، وخصوصا إن جانب كبير من الهجمات الإلكترونية يستهدف القطاعات الاقتصادية، والأمنية، والزراعية، والصناعية وغيرها من القطاعات المدنية التي لا غنى عنها لبقاء السكان المدنيين على قيد الحياة، ولا تقتصر في أهدافها على المنشآت والأهداف العسكرية.

وقد جاء في المادة 48 من البروتوكول الإضافي الأول لعام 1977 م الملحق باتفاقيات جنيف: (تعمل أطراف النزاع على التمييز بين السكان المدنيين والمقاتلين وبين الأعيان المدنية والأهداف العسكرية، ومن ثم توجه عملياتها ضد الاهداف العسكرية دون غيرها، وذلك من أجل تأمين احترام وحماية السكان المدنيين والأعيان المدنية).

وبالتالي، فإنه ووفقًا لهذا المبدأ (التمييز بين المدنيين والعسكريين) يتوجب على أطراف النزاع المسلح التمييز بين المقاتلين والمدنيين في الهجمات، وهو ما لا يتحقق في جانب كبير من الهجمات الإلكترونية، والتي تؤدي إلى تدمير منشآت حيوية مدنية محمية وفقا للقانون الدولي. وبالتالي يمكن اعتبار بأن هذه الهجمات محظورة ومُدانة وفقا لما تقرره المبادئ الدولية التي تحظر ذلك[26].

هكذا، ويُلاحظ بأن التكييف القانوني للهجمات الإلكترونية لازال ضمن مستوى القياس والاجتهاد، ولم يصل بعد إلى مرحلة إبرام اتفاقيات دولية صريحة خاصة به، وهذا ما يُعزى إلى أسباب عدة، يأتي في مقدمتها وجود عقبات تضعها الدول المهيمنة في مجال حروب الفضاء الإلكتروني، مثل الولايات المتحدة الأمريكية، وروسيا، والصين، إذ أن هذه الدول لا تفضل طرح موضوع التنظيم على المنابر الدولية حتى لا يضر بأمنها القومي فإبقاء الأمر خارج حدود القضايا القانونية يتيح للدول مساحة واسعة لكي تتحرك في توظيف أسلحتها الإلكترونية لتحقيق أهدافها.

بالرغم من ذلك، فقد برزت بعض المحاولات لبلورة اتفاقيات دولية بهذا الشأن، إلا أنها لم ترقَ إلى مستوى تنظيم الحروب والهجمات الإلكترونية، بقدر ما كانت أقرب لإقرار أطُر للهجمات السيبرانية ومن أبرزها :-

– اتفاقية مجلس أوروبا المتعلقة بالجريمة السيبرانية، في اكتوبر 2001 والتي تعرف أيضًا باسم "معاهدة بودابست لمكافحة جرائم الفضاء المعلوماتي".

– القرار الصادر عن الجمعية العامة للأمم المتحدة رقم (56/121) والموسوم ب "مكافحة إساءة استعمال تكنولوجيا المعلومات.

– وفي عام 2103 م، صدر دليل تالين، والذي وسم أنه دليل "بشأن القانون الدولي المطبق على الحروب السيبرانية"، والذي أعد من قبل مجموعة من الخبراء الدوليين، وبدعوة من "مركز التميز التابع لحلف الناتو".

– وضعت الدول العربية عام 2010 اتفاقية متعلقة بجرائم تقنية المعلومات والتي تضمنت تلبية طلبات الدول بخصوص تسليم المجرمين وحفظ الأدلة وحفظ وتسليم البيانات والمعلومات .

– ركزت بعض الدول على حماية الداخل أولًا : منها الدولة المصرية حيث أنشأت وزارة الداخلية عام 2002 "إدارة لمكافحة جرائم الحاسب الآلي وشبكة المعلومات" " وحدة شبكات

البيانات والجرائم السيبرانية" لتتولى رصد جرائم تكنولوجيا المعلومات وتعقب مرتكبيها ...كذلك أنشأت الدولة المصرية عام 2010 مركز الاستعداد لطوارئ الحاسبات والشبكات[27].

يجد البحث أن التحدي الأكبر الذي يواجه تنظيم الهجمات في الفضاء الإلكتروني قانونيًا هو عدم وجود إرادة دولية على صعيد المفاوضات أو على صعيد قرارات مجلس الأمن، حيث تغيب الإدارة الدولية اللازمة للدفع باتجاه ذلك، وخصوصا من قبل الدول المهيمنة في هذا المجال، كما أن القانون الدولي الإنساني يذهب إلى تنظيم استخدام الأسلحة بصورتها التقليدية وغير التقليدية، في حين لا يبدو أن الهجمات الإلكترونية، حتى الآن، تصنف على هذا النحو، باعتبارها أسلحة مادية، وذلك باعتبار بقاء النظر لها باعتبارها تعمل في الحيز الافتراضي غير المادي، كما في عمليات الاستحواذ على ملفات رقمية أو تعطيل مواقع إلكترونية[28].

الفصل الثاني : تصدي الإعلام الأمني والرقمي للهجمات السيبرانية

إن الإعلام الأمني يساهم بنصيب وافر في الوقاية ومكافحة الجرائم ، وذلك من خلال تحصين أفراد المجتمع من السلوك الإجرامي ودعوتهم للتعاون مع رجال الأمن على اختلافها لمكافحة كل أشكال الجرائم والحد من آثارها السلبية، لذا يعد للإعلام الأمني دورًا قويًا ومؤثرا في مجال الأمن، حيث تؤثر وسائل الإعلام بدرجات متباينة على مجريات الأمن وفعالية أجهزته، لذلك يجب استغلال التأثير الإيجابي لوسائل الإعلام من خلال دعم قدرات الأجهزة الأمنية والتنويه بإنجازاتها وقدرتها على مواجهة الجريمة، وذلك قصد حشد الرأي العام الذي يدعم ويساند أجهزة الأمن ويحث أفراد المجتمع على التعاون مع رجال الأمن، إلا أنه بالمقابل ذلك توجد بعض العراقيل التي تحد من فعالية الإعلام الأمني في مكافحة الجريمة[29].

1 : مفهوم الإعلام الأمني :

الإعلام الأمني مفهوم قائم على تحقيق التماسك الاجتماعي في مواجهة المواقف الأمنية، وهو مفهوم إعلام متخصص وجديد فرضته المستجدات الأمنية الطارئة على المجتمع، وله العديد من التعريفات منهم :-

- تلك المعلومات التي تصدر عن جهاز الشرطة، وتبث عن طريق وسائل الإعلام المختلفة بهدف التوعية والإرشاد وتحسين صورة المؤسسة الشرطية في أذهان الجماهير لتحقيق التفاعل الإيجابي بين الشرطة و الجماهير[30].

- مختلف الرسائل الإعلامية المدروسة التي تصدر بهدف توجيه الرأي العام لتحقيق الخطة الشاملة والتصدي للأسباب الدافعة لارتكاب الجريمة والتوعية بأخطار ومخاطر الجرائم، وإرشاد المواطنين بأسلوب يضمن عدم وقوعهم فريسة للجريمة، وكذا تبصير الجمهور بأساليب الوقاية من جريمة من خلال تدابير مختلفة وتنمية حسهم الأمني[31].

- لا يقتصر دور الإعلام الأمني في ترسيخ الأمن والاستقرار في المجتمع، خاصة مع اتساع مفهوم الأمن الشامل، كما لا يقتصر على الدور الإرشادي والوقائي الذي يضمن تحصين الفكر، بل لهو هدف علاجي من خلال مكافحة الظواهر الإجرامية والمخالفات

وعالج الإنحرافات الفكرية، والأهم قدرته على ترسيخ القيم النبيلة وتنمية الحس الأمني، ونشر المعرفة الأمنية بين المواطنين للتعاون مع القطاع الأمني المختص في مكافحة الجرائم المختلفة[32].

2 : الإعلام الرقمي

الإعلام الجديد أو الإعلام الرقمي هو مجموعة تكنولوجيات الاتصال الرقمي التي تولدت من التزاوج بين تقنيات الحاسب والأجهزة الذكية والوسائل التقنية للإعلام مثل الطباعة والتصوير الفوتوغرافي والصوت والصورة والفيديو.

حقق الإعلام الرقمي الاكتساح الكبير، وفرض السيادة المطلقة من حيث الانتشار، واختراق كافة الحواجز سواءً كانت حواجز مكانية أو زمنيه إضافة إلى التنوع اللامتناهي في رسائله ومحتواه نظرًا لما يملكه من قدرات ومقومات تمكنه من الوصول للجميع ، والإعلام بمعناه البسيط هو : نقل المعارف والمعلومات والثقافات الفكرية والسلوكية ، بطريقة محددة من خلال أدوات ووسائل الإعلام والنشر، بقصد التأثير والتوجيه في سلوكيات و أفكار المتلقين سواءً بالإيجاب أو السلب[33].

ومع تطور التكنولوجيا باتت وسائل التواصل الاجتماعي لا توفر الرفاهية والتواصل فقط إنما توفر بيئة مثالية للحملات الإعلامية العدائية، فلقد فقد العديد من المتابعين الثقة في وسائل الإعلام القائمة حيث يميل كل شخص إلى المعلومات التي تؤكد وجهة نظره، ولم تكن روسيا بحاجة إلى خلق انقسامات جديدة في المجتمعات المستهدفة حيث إنها تقوم باستغلال الانقسامات الموجودة بالفعل، الدول الغربية تعتمد على الشركات متعددة الجنسية لتقييد عمليات الحرب الإعلامية فبعد الانتخابات مباشرة في كل من جوجل وفيسبوك وتويتر وشركات أخرى استخدامها في حملات التضليل ونشر الأخبار الزائفة.

- الإعلام والجرائم السيبرانية:

بات الأمن السيبراني هو المسئول الأوحد عن أمان تكنولوجيا المعلومات، وخط الدفاع الأول ضد أذرع الجيوش الحديثة التي تلعب داخل الفضاء السيبراني، لدرجة جعلت الردع السيبراني مقياسًا لنجاح قدرة الدولة على منع اختراقها، ولأنه أصبح سلاحًا استراتيجيًا يوجد في أيدى الحكومات والأفراد، تستغل من خلاله الدول المعادية نقاط الضعف لاستهداف عمق مجتمعات الدول الراسخة، بألاعيب التكنولوجيا عن بعد وأصبحت عناصر مؤشرات الأمن السيبراني على مستوى العالم تقاس بـ100 درجة ضمن خمسة معايير أهمها التشريعات والإطار المؤسسى في الدولة، وبناء القدرات البشرية، وتوافر القدرات والتقنيات اللازمة، والتوعية بمخاطر الحرب السيبرانية، ولهذا أوصى الرئيس عبدالفتاح السيسي، بإنشاء المجلس الأعلى للأمن السيبراني المصرى عام 2014، وصفحته الرسمية على موقع التواصل الإجتماعي "EG-CERT" ،و لم تغفل وزارة الاتصالات وتكنولوجيا المعلومات ذلك ووضعت قانونًا جديدًا يؤسس جهازًا قوميًا لأمن المعلومات، مهامه صياغة استراتيجية أمن المعلومات المصرى، وتشجيع انتشار ثقافة أمن المعلومات وتسجيل ومنح تراخيص حقيقية لهذه الخدمة، ووضع الاحتياط والتدابير لمنع المتسللين والمخترقين والقراصنة

وتعول الدولة على دور الإعلام في وضع استراتيجيات ما قبل الهجوم أو الاختراق والتي تسمى باستراتيجيات المنع، منها على سبيل المثال تطبيق الثقافة المعلوماتية والإعلامية في المناهج، ودور الإعلام في توعية المواطن يبدأ من توعية المواطن بأهمية الأمن الفضائي، وبتعليمه كيفية حماية أجهزته التكنولوجية ابتداء من تأمين تليفونه الشخصي من اختراقات الهاكرز، وبتوعيته بأهمية اتباع الإجراءات الخاصة بالأمان والسلامة عند استخدام أى موقع إلكتروني، وبأهمية الضغط على زر امزيد من القراءةب وعدم تجاهله ، فاختراقات المواقع الإلكترونية تستغل بياناته بشكل أو بآخر إما بجعله هدف لمبيعاتها وإما ببيعه لجهات استخباراتية تضر ببلده وتهدد أمنه القومي[35]وأشارت إلى ضرورة وجود جهد مخطط من خلال مؤسسات التنشئة الاجتماعية وسائل الإعلام كإحداها سواء بشكل مباشر أو بشكل غير مباشر عن طريق الدراما على سبيل المثال، وفي زمن قديم تم معالجة هذه الأمور في السينما كما شاهدنا في فيلم بطولة فؤاد المهندس الذي تحدث عن المطارات السرية، فهو كان شخص ليس لديه وعى أن هذه المعلومات تهدد الأمن القومي لبلده، مؤكدة أن دور الإعلام من جهة ومن جهة أخرى مؤسسات التعليم تشكل جزءًا هامًا من وعى الطالب على قدر مرحلته لذلك، فإنّ إشكالية الأمن المعلوماتي باتت تشكل رهاب قوي وتحدي خطير لمختلف الدول، وباتت أهمية الإعلام الرقمي والأمني تتزايد يوم تلو الأخر لتحقيق أمان واستقرار الدولة، فأصبح الإعلام بمثابة جيش ودرع للدولة تتزايد قوته كلما زادت التقنية والتطبيقات وقدرته على مواجهه وتحدي الجرائم الإلكترونية والوقاية منها ..

4- قوة مصر في مجال الأمن السيبراني

احتلت مصر المرتبة 23 في مؤشر الأمن السيبراني العالمي[36]2021 من قبل الاتحاد الدولي للاتصالات حيث تصدرت الولايات المتحدة القائمة تليها المملكة المتحدة والسعودية في المرتبة الثانية وأستونيا في المرتبة الثالثة في المؤشر .

ويعتبر مؤشر الأمن السيبراني العالمي اجى سى آب مرجع موثوق فيه يقيس التزام الدول بالأمن السيبراني على المستوى العالمي، ويتم تقييم مستوى التنمية أو المشاركة لكل بلد على أساس خمس ركائز وهى :التدابير القانونية والفنية والتنظيمية وبناء القدرات والتعاون ثم تجميعها في النتيجة الإجمالية، لافتًا إلى أن المؤشر ضرورة حتمية لتنتقل المؤسسات بشكل متزايد إلى المنصات الرقمية ويعد الأمن السيبراني تحديًا متعدد الأبعاد وعابرًا للحدود، مصر لديها مركز وطني لحالات الطوارئ للحاسبات والشبكات تم إنشاؤه بواسطة المعهد القومي للاتصالات عام 2019 ويقدم الدعم الفني اللازم لحماية البنية التحتية الوطنية للمعلومات ومراقبة الأمن السيبراني وتحليل البرامج الضارة والتعاون مع الدول الأخرى في تبادل المعلومات ويشمل المركز الوطني عددًا من الأنشطة وتشمل الخدمات الاستباقية

الإطار النظري

نظرية المسؤولية الاجتماعية

نظرية المسؤولية الاجتماعية والأخلاقية لوسائل الإعلام تتركز على ثلاث أبعاد رئيسية يتصل البعد الأول بالوظائف التي ينبغي أن يؤديها الإعلام المعاصر ويتصل البعد الثاني

بمعايير الأداء بينما يتصل البعد الثالث بالقيم المهنية التي ينبغي مراعاتها في العمل الإعلامي ففي ما يخص الأداء الإعلامي فإن نظرية المسؤولية الاجتماعية تهتم بوضع المعايير التي تشمل المعايير الأخلاقية للأفراد إضافة إلى معايير الوسائل الإعلامية ومواثيقها الأخلاقية سواء كانت مكتوبة أو غير مكتوبة والمعايير المهنية التي تضعها الهيئات الإعلامية المختلفة إضافة إلى مجموعة التشريعات والقوانين التي تحكم وتنظم وسائل الإعلام، وتشكل معايير الأداء الإعلامي في مجملها العام الضوابط الأخلاقية والقانونية التي تحكم ممارسة العمل الإعلامي في إطار المسؤولية الاجتماعية والأخلاقية التي تحتم على الإعلام أن يقوم بواجبه تجاه المجتمع كما ينعم بحقه في الحرية وكذلك عرض الحقائق والمعلومات التي تدعم الديمقراطية وتضمن مشاركة الرأي العام في الأحداث الجارية[37].

ومن هنا فان نظرية المسئولية الاجتماعية تشير إلى أهم العناصر التي يجب الالتزام بها حتى تحقق وسائل الإعلام دورها المسئول في المجتمع، ومن ثم تفيد النظرية في مناقشة نتائج الدراسة فيما يتصل بدور وسائل الإعلام الرقمي بكافة أشكالها المتعددة بمعالجة والتصدي لقضايا الجرائم الإلكترونية وقضايا الأمن السيبراني الذي صار لها أولوية كبيرة لدرء والتصدي للتهديدات الإلكترونية بكافة أشكالها، وذلك في إطار تعزيز الجهود العالمية لمكافحة الهجمات السيبرانية، خاصة أنها باتت تطال الدول الكبيرة والصغيرة على حد سواء في ضوء تسارع التطورات التكنولوجية والتقنيات المستخدمة في هذا المجال.

مدخل تحليل النُظُم

يعتمد هذا المدخل على فكرة أن هناك عوامل خارجية يطلق عليها "المدخلات" تتفاعل مع وسط نظامي وتسمى التفاعلات ب "العمليات"، ويترتب عليها نتائج تسمى "مخرجات"، وهي عبارة عن قرارات تتخذها مراكز صنع القرار لمواجهة ظاهرة ما ولاتخاذ السياسات وتحديدها، كما أن هذه العملية يرافقها تغذية راجعة، تتمثل في آثار وعواقب هذه القرارات، وأبرز من كتب في هذا المدخل هما "ديفيدايستون"، و"مورتن كابلان."

وقد تم توظيف هذا المدخل من خلال دراسة العوامل والمسببات التي أدت إلى تغير أو تطور التعامل الإعلامي مع معالجات السيبرانية ومن ثم تتبع الأثر الذي أحدثته هذه المعالجات الإعلامية في طبيعة التصدي وتفادي هذه الهجمات.

نتائج الدراسة التحليلية:

جدول رقم (1) يوضح أهم القضايا الفرعية في مواقع الإعلام الرقمي عينة الدراسة في مكافحة الجرائم السيبرانية

صفحة / الموضوعات	صفحةEG-CERT		محترفي أمن المعلومات والأمن السيبراني - TECHVORTEX		المجموع	
	ك	%	ك	%	ك	%
اختراق الحسابات	17	%45.9	26	%26.8	43	%32.1
جرائم إلكترونية دولية	4	%10.8	12	%12.4	16	%11.9
الإجراءات الوقائية	7	%18.9	6	%6.2	13	%9.7
مخاطر الجرائم على الأمن القومي	2	%5.4	4	%4.1	6	%4.5
دور مصر في التصدي للجرائم الإلكترونية	3	%8.1	1	%1	4	%3
الاستخدامات الإيجابية	1	%2.7	42	%43.3	43	%32.1
المصطلحات الجديدة	3	%8.1	6	%6.2	9	%6.7
المجموع	**37**	**%100**	**97**	**%100**	**134**	**%100**

يتضح من الجدول السابق أهم القضايا الفرعية في وسائل الإعلام الرقمي عينة الدراسة في مكافحة الجرائم السيبرانية حيث جاءت قضيتي **اختراق الحسابات و الاستخدامات الإيجابية** في الترتيب الأول بنسبة 32.1% موزعة ما بين صفحة EG-CERTبنسبة 45.9% في موضوع اختراق الحسابات **ويرجع ذلك إلى** خطة اعتماد صفحة EG-CERT خطة الدولة إلى زيادة وعي وثقافة المواطن لمواجهة كافة الجرائم بأشكالها وأنواعها المختلفة وفي مقابلة لأحد المسؤولين عن الصفحة أن تأمين معلومات الدولة يبدأ من تأمين المعلومات الشخصية لكل مواطن لذا تتعمد الصفحة بنشر منشورات توعية لتأمين حسابات المواطنين داخل الدولة، بينما صفحة محترفي أمن المعلومات والأمن السيبرانيTECHVORTEXجاءت بنسبة 26.8%، أما موضوع الاستخدامات الايجابية جاءت في صفحة EG-CERT بنسبة 2.7% بينما تفوقت عليها صفحة محترفي أمن المعلومات والأمن السيبرانيTECHVORTEX فجاءت بنسبة 43.3%**ويرجع ذلك** عمدت نشر طرق الاستخدامات الإيجابية وطرق تأمين الحساب أما بفيديوهات شرح أو روابط لبعض الخبراء والمتخصصين في الأمن السيبراني، وجاء في الترتيب الثانية موضوع **جرائم إلكترونية دولية** بنسبة 11.9% موزعة ما بين صفحة EG-CERT بنسبة 10.8%، وتفوقت عليها صفحة محترفي أمن المعلومات والأمن السيبرانيTECHVORTEX 12.4%، أما موضوع **الإجراءات الوقائية** جاءت في الترتيب الثالث بنسبة 9.7% ، والتي كانت تهدف إلى اتخاذ الإجراءات الوقائية لشركات الموبايل واللاب والتاب والنت، وجاءت هذه النتيجة موزعة ما بين صفحة EG-CERT 18.9% التي تفوقت على صفحة محترفي أمن المعلومات والأمن السيبرانيTECHVORTEX 6.2%، جاء موضوع **المصطلحات الجديدة** في الترتيب الرابعبنسبة 6.7% تمثلت في بعض المصطلحات الآتية (برنامج الجدار الناري/ شبكة البرمجيات الخبيثة /بوت نت / حصان طروادة/ الوشم الالكتروني الذكي / لغة بايسون/ أداةRoutersploit/ جدار الحماية برمجيات خبيثة/ **nmap**) وذلك موزعة ما بين

صفحة EG-CERT بنسبة 8.1% بينما صفحة محترفي أمن المعلومات والأمن السيبرانيTECHVORTEX بنسبة 6.2%، وفي الترتيب الخامس **مخاطر الجرائم على الأمن القومي** بنسبة 4.5% موزعة ما بين صفحة EG-CERT بنسبة 5.4% التي تقاربت نفس النسبة مع صفحة محترفي أمن المعلومات والأمن السيبرانيTECHVORTEX بنسبة 4.1%**ويرجع ذلك إلى** اعتبار الصفحات عينة الدراسة أن تهديد الجرائم السيبرانية للأمن القومي متمثلة في المواطن حتي إلى الآن وليس يتعدى ذلك المؤسسات أو البنية التحتية للدولة ولأن الدولة ما زالت تنهي خطة التحول الرقمي لكل المؤسسات فبالتالي تعمل التوعية بشكل الأمن للمواطن أولًا، وبالتالي ترتب عليها أن الاهتمام بالتصدي للجرائم الإلكترونية كانت ضئيلة بالنسبة لباقي الموضوعات الآخرى، وفي الترتيب الأخير جاء دور مصر في **التصدي للجرائم الإلكترونية** بنسبة 3% موزعة ما بين صفحة-EG CERTبنسبة8.1%، في حين صفحة محترفي أمن المعلومات والأمن السيبرانيTECHVORTEX كانت بنسبة ضئيلة 1%.

جدول رقم (2)يوضح أهم العناصر المرافقة للمضمون في مواقع الإعلام الرقمي عينة الدراسة في مكافحة الجرائم السيبرانية

صفحة / العناصر المرافقة للمضمون	صفحة EG-CERT		محترفي أمن المعلومات والأمن السيبراني - TECHVORTEX		المجموع	
	ك	%	ك	%	ك	%
متعددة	20	%22.2	16	%20.7	26	%20.3
صور إخبارية	24	%26.7	0	0	24	%18.7
روابط	23	%25.6	27	%35.1	20	%15.6
رسوم كتابية	4	%4.4	12	%15.6	16	%12.5
رسوم تعبيرية	5	%5.6	6	%7.8	12	%9.4
نص فقط	3	%3.3	9	%11.7	12	%9.4
انفوجراف	8	%8.9	2	%2.6	10	%7.8
ملفات فيديو	2	%2.2	4	%5.2	6	%4.7
صور شخصية	1	%1.1	1	%1.3	2	%1.6
المجموع	**90**	**%100**	**77**	**%100**	**128**	**%100**

• ملحوظة زيادة عدد المجموع يرجع إلى تعدد الصور والفيديوهات المطروحة على الصفحة داخل المنشور الواحد.

يتضح من الجدول السابق أن **متعددة** جاءت في المرتبة الأولى بنسبة 20.3% موزعة ما بين صفحة EG-CERT التي جاءت بنسبة 22.2% بينما صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEX بنسبة 20.7% **ويرجع ذلك إلى** محاولة الصفحات

لجذب الجمهور المتلقي بإضافة أكبر عدد من الفيديوهات والروابط، وفي المرتبة الثانية جاءت **صور إخبارية** بنسبة 18.7% موزعة ما بين صفحة EG-CERT فقط التي جاءت بنسبة 26.7% ، أما **روابط** جاءت في المرتبة الثالثة بنسبة 15.6% موزعة ما بين صفحة EG-CERT التي جاءت بنسبة 25.6% بينما صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEX تفوقت على الصفحة الآخرى بنسبة 35.1%، بينما **رسوم كتابية** جاءت في المرتبة الرابعة بنسبة 12.5% موزعة ما بين صفحة EG-CERT التي جاءت بنسبة 4.4% بينما صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEX بنسبة 15.6%، أما في المرتبة الخامسة جاءت **رسوم تعبيرية ونص فقط** بنسبة 9.4% موزعة ما بين صفحة EG-CERT التي جاءت بنسبة 5.6% بينما صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEX بنسبة 7.8% في الرسوم التعبيرية ،أما في نص فقط موزعة ما بين صفحة EG-CERT التي جاءت بنسبة 3.3% بينما صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEX بنسبة 11.7% ، وفي المرتبة السادسة جاءت **أنفوجراف** بنسبة 7.8% موزعة ما بين صفحة EG-CERT التي جاءت بنسبة 8.9% بينما صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEX بنسبة 2.6%، وفي المرتبة السابعة جاءت **ملفات فيديو** بنسبة 4.7% موزعة

ما بين صفحة EG-CERT التي جاءت بنسبة 2.2% بينما صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEX بنسبة 5.2%، وفي المرتبة الأخيرة جاءت **صور شخصية** بنسبة 1.6% موزعة ما بين صفحة EG-CERT التي جاءت بنسبة 1.1% بينما صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEX بنسبة 1.3%.

جدول رقم (3) يوضح أهم مصادر المعلومات في مواقع الإعلام الرقمي عينة الدراسة في مكافحة الجرائم السيبرانية

صفحة / مصادر المعلومات	صفحة EG-CERT		محترفي أمن المعلومات والأمن السيبراني - TECHVORTEX		المجموع	
	ك	%	ك	%	ك	%
مواقع إلكترونية إخبارية	6	%13	18	%45	24	%27.9
صفحات رسمية	20	%43.6	0	0	20	%23.3
جمهور عام	0	0	18	%45	18	%20.9
منظمات دولية_ شركات دولية	16	%34.8	0	0	16	%18.6
خبراء ومثقفين	0	0	3	%7.5	3	%3.5
مجلس وزراء	2	%4.3	0	0	2	%2.3

متحدثين رسميين	2	%4.3	0	0	2	%2.3
أخرى	0	0	1	%2.5	1	%1.2
المجموع	**46**	**%100**	**40**	**%100**	**68**	**%100**

*ملحوظة زيادة عدد المصادر يرجع إلى أن صفحة EG-CERT كانت متعددة المصادر في المنشور الواحد ، بينما قلة عدد المصادر في صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEX كانت ليست معلومات ولكنها كانت مجرد تساؤلات.

يتضح من الجدول السابق أن **مواقع إلكترونية إخبارية** جاءت في المرتبة الأولى بنسبة 27.9% ، موزعة ما بين صفحة EG-CERT بنسبة 13% في حين تفوقت صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEX بنسبة 45% وجاءت مصادر المعلومات متمثلة في (يوتيوب – صفحات فيس بوك أخرى)، وجاءت في المرتبة الثانية **صفحات رسمية** بنسبة 23.3%وجاءت هذه النسبة بصفحة EG-CERT فقط وعلى سبيل المثال على المصادر الرسمية (هيئة الاتصالات وتكنولوجيا المعلومات)**ويرجع ذلك إلى** أن صفحة هي صفحة رسمية تابعة للدولة المصرية وبالتالي يتم الاعتماد على مصادر من الصفحات رسمية أو تصريحات لمسؤولين وهذا ما افتقدته صفحة أمن المعلومات والأمن السيبراني، وجاء **جمهور عام** في المرتبة الثالثة بنسبة 20.9% وكانت متمثلة فقط في صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEX**ويرجع ذلك** لأنها صفحة عامة مفتوحة معتمدة على الجمهور العام وبالتالي يسمح للجمهور نشر المنشورات، أما **منظمات دولية – شركات دولية** جاءت في المرتبة الرابعة بنسبة 18.6% وكانت متمثلة في صفحة EG-CERT بنسبة 34.8% وكانت متمثلة (شركةApple– شركة Dell – شركةGoogle – شركةMicrosoft)، بينما جاءت **خبراء ومثقفين** في المرتبة الخامسة بنسبة 3.5% وكانت متمثلة في صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEX، وجاءت **مجلس الوزراء- متحدثين رسميين** في نفس المرتبة بنسبة 2.3% ، وفي المركز الأخير جاءت أخرى بنسبة 1.2%.

جدول رقم (4) يوضح دورية التحديث في مواقع الإعلام الرقمي عينة الدراسة في مكافحة الجرائم السيبرانية

صفحة / دورية التحديث	صفحة EG-CERT		محترفي أمن المعلومات والأمن السيبراني - TECHVORTEX		المجموع	
	ك	%	ك	%	ك	%
متعددة في اليوم	4	%10.8	47	%48.5	51	%38.1
يوميًا	9	%24.3	24	%24.7	33	%24.6

فترات متقاربة	6	%16.2	15	%15.5	21	%15.7
فترات متباعدة	18	%48.6	11	%11.3	29	%21.6
المجموع	37	%100	97	%100	134	%100

يتضح من الجدول السابق أن **متعددة في اليوم** جاءت في المرتبة الأولى بنسبة 38.1% ، موزعة ما بين صفحة EG-CERT بنسبة 10.8% في حين تفوقت صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEX بنسبة 48.5%وبالمقارنة بين الصفحتي نجد أن دورية التحديث بصفة سريعة وذلك لأن المنشورات على صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEX قد تصل إلى أكبر من متابعين الصفحة وبالتالي تتعدد المنشورات في اليوم الواحد، وجاءت في المرتبة الثانية يوميًا بنسبة 24.6% موزعة ما بين صفحة EG-CERT بنسبة 24.3% في حين تفوقت صفحة محترفي أمن المعلومات والأمن السيبرانيTECHVORTEXبنسبة 24.7% وكانت النسب متقاربة بين الصفحتين، وجاء **فترات متباعدة** في المرتبة الثالثة بنسبة 21.6% موزعة ما بين صفحة EG-CERT بنسبة 48.6%،بينما صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEXبنسبة 11.3% الفرق الواضح بين النسبتين يرجع إلى أن صفحة EG-CERTتعتمد على المصادر الرسمية دون السماح بالجمهور العام بالنشر على الصفحة وذلك لأنها تنتمي لوزارة الاتصالات وتكنولوجيا المعلومات، أما **فترات متقاربة** جاءت في المرتبة الرابعة **والأخيرة** بنسبة 15.7% موزعة ما بين صفحة EG-CERT بنسبة 16.2% في حين تفوقت صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEXبنسبة 15.5%، وتتقارب النسب بين الصفحتين بما يؤكد تكريس جهود الدولة بجميع أنشطتها وأجهزتها الذي يهدف إلى تحسين معايير وممارسات أمن المعلومات، وحماية البنى التحتية لقطاع الاتصالات وتقنية المعلومات من مخاطر واختراقات الإنترنت.

جدول رقم (5) يوضح أسلوب المعالجة في مواقع الإعلام الرقمي عينة الدراسة في مكافحة الجرائم السيبرانية

صفحة / أسلوب المعالجة		صفحة EG-CERT		محترفي أمن المعلومات والأمن السيبراني - TECHVORTEX		المجموع	
		ك	%	ك	%	ك	%
إطار الإيجابيات	إبراز	34	%91.9	81	%83.5	115	%85.8
إطار السلبيات	إبراز	3	%8.1	16	%16.5	19	%14.2
المجموع		37	%100	97	%100	134	%100

يتبين من الجدول السابق أن **إطار إبراز الإيجابيات** جاء في الترتيب الأول بنسبة 85.8% موزعة ما بين صفحة EG-CERT بنسبة 91.9% وكانت أبرز المنشورات المطروحة على تلك الصفحات عينة الدراسة متمثلة في (إبراز دور مصر في التعاون الخارجي للتصدي للهجمات السيبرانية-تحذير وتوعية من الهاكرز وطرق سرقة الحسابات- طرق عمل التحديثات اللازمة للحسابلات-الاستخدامات الإيجابية للتكنولوجيا -توعية بأساسيات الأمن السيبراني وكيفية حماية الحسابات - طرق الحفاظ على جهاز العمل- نصائح وارشادات لحماية نفسك وهويتك)، أما صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEX بنسبة 83.5% كانت المنشورات إطار إبراز الإيجابيات متمثلة في (نشر صورة للمتورطين في اختراقات- التعريف بمخاطر الهجمات السيبرانية على الأمن القومي- معلومات عن الوشم الذكي - والذكاء الاصطناعي- نشر بعض الدورات عن الأمن السيبراني) **ويرجع ذلك** إلى الهدف الأساسي من هذه الصفحات نشر التوعية ووتوعية الجمهور لتأمين المواطنين ورفع نسبة الإدراك بخطورة الهجمات السيبرانية على الأمن القومي، أما في الترتيب الثاني جاء إطار **إبراز السلبيات** بنسبة 14.2% موزعة ما بين صفحة EG-CERT بنسبة 8.1% **ويرجع ذلك** إلى طريقة معالجة الهجمات الإلكترونية التي تعرضت لها بعض الدول الغربية، أما صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEX بنسبة 16.5%،**ويرجع ذلك** إلي تزايدت في هذه الصفحة لوجود بعد المنشورات التي تنوه على صفحات لمخترقين كما روجت لبعض المصطلحات مثل الهاكر الأخلاقي، وكانت المنشورات السلبية المطروحة على صفحتها متمثلة في التعريفات بالثغرات الموجودة في الاجهزة وكيفية اختراقها -التأكيد ونشر فيديوهات عن خوارزميات الاختراق-الحديث عن الاختراق الاخلاقي!!- نشر صفحات فيس بوك والتنويه والاعلان عن هاكر ، تحت مسمى هاكر اخلاقي) وبمقارنة نتائج الجدول السابق يتضح أن النسبة بين إطار إبراز الايجابيات كبير ويمكن تفسير ذلك إلى أن صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEX يوجد بها عدد كبير من المنشورات التي كانت تتضمن منشورات الصفحة بالاضافة إلى منشورات المتابعين متتضمن استفساراتهم الخاصة، كما أن عدد الموضوعات التي كانت يتم نشرها تتضمن موضوعات متنوعة عن صفحة EG-CERT فكانت صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEX تركز على حماية الأمن الشخصي وحماية الأشخاص اهتمام بنشر ثقافة التوعية بالامن السيبراني ، حيث تم نشر العديد من اللينكات التي تنقل فيديوهات حول تأمين الجهاز الشخصي والكروت البنكية وغيرها.

جدول رقم (6) يوضح التقاعلية في مواقع الإعلام الرقمي عينة الدراسة في مكافحة الجرائم السيبرانية

التفاعل - التعليقات	صفحة EG-CERT		محترفي أمن المعلومات والأمن السيبراني - TECHVORTEX		المجموع	
	ك	%	ك	%	ك	%
مؤيد	19	%82.6	77	%71.3	96	%73.3
محايد	2	%8.7	31	%28.7	33	%25.2
معارض	2	%8.7	صفر	صفر	2	%1.5
المجموع	23	%100	108	%100	131	%100

- ملحوظة زيادة عدد التفاعلات كانت زيادة في صفحة أمن المعلومات وذلك لأن التفاعل كانت هناك مساحة للجمهور لنشر منشورات تفاعلية بتأييد موضوع أو استفسار عن موضوع

يتضح من الجدول السابق أن **مؤيد** جاءت في المرتبة الأولى بنسبة 73.3% ، موزعة ما بين صفحة EG-CERT بنسبة 82.6% في حين تفوقت صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEX بنسبة 71.3%،يرجع ذلك اختلفت التفاعلات المؤيدة جاءت بالإشادة بأدمن الصفحة أو ببعض العبارات الوطنية مثل (تحيا مصر)، **محايد** جاءت في المرتبة الثانية بنسبة 25.2% ، موزعة ما بين صفحة EG-CERT بنسبة 8.7% في حين تفوقت صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEX بنسبة 28.7%ويرجع الفرق الواضح بين النسبتين يرجع إلى أن صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEX كانت التساؤلات بنسبة أعلى من صفحة EG-CERT،وهنا ترابط قوي بين جدول رقم (3) وجدول رقم (6) ويؤكد أن نسبة كبيرة من المنشورات على صفحة أمن المعلومات جاءت منشورات تفاعلية وليست معلومات أي أنها كتبت بواسطة الجمهور وليس أدمن الصفحة وكان خلالها الجمهور أما يؤيد قضية معينة أو منشور معين ـو يطرح بعض التساؤلات، كما أن بعض التعليقات كانت تطرح بعض التساؤلات المحايدة للتعرف عن المزيد من التساؤلات لشرح الموضوع بصورة أكبر.

معارض جاءت في المرتبة الأولى بنسبة 1.5%، وكانت تلك النسبة في صفحة EG-CERTفقط بنسبة 8.7% وكانت تتمثل في وتمثلت في (الهجمات الالكترونية ل اوكرانيا وكوريا -التشكيك في وجود نت في كوريا - التشكيك في مصداقة الخبر المنشور على الصفحة).

جدول رقم (7) يوضح آليات المعالجة في مواقع الإعلام الرقمي عينة الدراسة في مكافحة الجرائم السيبرانية

صفحة / آليات المعالجة	صفحة EG-CERT		محترفي أمن المعلومات والأمن السيبراني - TECHVORTEX		المجموع	
	ك	%	ك	%	ك	%
إخباري	2	%5.4	4	%4.1	6	%4.4
توعوي	18	%48.6	18	%18.6	36	%26.9
تحذيري	8	%21.6	13	%13.4	21	%15.7
تثقيفي	5	%13.5	23	%23.7	28	%20.9
خدمي	4	%10.8	39	%40.2	43	%32.1
المجموع	37	%100	97	%100	134	%100

يتضح من الجدول السابق أن من أهم الآليات المعالجة التي اعتمدت عليها عينة الدراسة تمثلت في الخدمات التي تطرحها الصفحات جاءت **خدمي** في المرتبة الأولى بنسبة 32.1% ، موزعة ما بين صفحة EG-CERT بنسبة 10.8% في حين تفوقت صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEX بنسبة 40.2% وهذا يفسر الدور الذي يهدف إليه الصفحة في المرتبة الأولى وهو مساعدة المتابعين في قضايا الاختراق ومعلومات عن الهجمات الإلكترونية والإجابة عن استفساراتهم، **توعوي** جاءت في المرتبة الثانية بنسبة 26.9% ، موزعة ما بين صفحة EG-CERT بنسبة 48.6% التي تفوقت بنسبة كثير وذلك تأكيدًا لوقائع أثبتت الحاجة الملحة للتوعية بمخاطر الهجمات السيبرانية فتولي لها الدولة عناية استثنائية ؛وذلك لحماية الدولة حصانة الأمن الرقمي للمواطنين صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEX فجاءت بنسبة 18.6%، وفي المرتبة الثالثة جاءت **تثقيفي** بنسبة 20.9%موزعة ما بين صفحة EG-CERT بنسبة 13.5% ، بينما صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEX جاءت بنسبة 23.7%، وفي الترتيب الرابع جاءت **تحذيري** بنسبة 15.7% موزعة ما بين صفحة EG-CERT بنسبة 21.6%، بينما صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEXجاءت بنسبة 13.4%، وفي الترتيب الأخير جاءت إخباري 4.4% موزعة ما بين صفحة EG-CERT بنسبة 5.4%، بينما صفحة محترفي أمن المعلومات والأمن السيبراني TECHVORTEX جاءت بنسبة 4.1%.

توصيات الدراسة

– صياغة مجموعة من الخطط لتحصيل المعلومات والبيانات والحفاظ عليها، وتصنيفها حسب درجات السرية

– إعادة النظر في مفهوم الأمن القومي في ظل التطورات التكنولوجية والمعلوماتية التي يشهدها العالم، لتحديد المخاطر والتهديدات وتصنيفها ووضع خطط للتعامل معها .. أو محاولة بناء حدود سيادية داخل هذا المجال بوجود تطبيقات محلية.

– تشريع قوانين داخلية حاكمة لمجال الفضاء السيبراني ، عن طريق الاستعانة بخبراء في ها المجال .

– بات المجال الإعلامي والتكنولوجي مهم جدً للقطاعات والمؤسسات الأمنية وجزء من تسليحها.. خاصة بعد تحول الحروب من تقليدية لـ لا متماثلة وسيبرانية .

– اعتماد منظومة سلم كعادة الدولة المصرية.. كيفية استغلال وتطبيق التكنولوجيا في كل ما يفيد الأفراد المؤسسات ونبذ استخدامها في الحروب، ونشر ذلك الوعي من خلال دورات تثقيفية ومواد إعلامية إعلانية.

– المشاركة في الإستراتيجيات العربية لمواجهة مخاطر الإنترنت، والتنسيق مع المراكز والمؤسسات المختلفة للاطلاع على استراتيجيات القوة والردع والاستفادة منها.

– تطوير برامج الحماية وزيادة الدورات التوعوية حول الأمن السيبراني .. خاصة لدى القائمين على الصفحات الرسمية للدولة والمؤسسات المختلفة.

– التعاون داخل الدولة بين جميع الهيئات المعنية والقطاعين العام والخاص والشركات العاملة في مجال تكنولوجيا الاتصال والمعلومات من أجل وضع استراتيجية موحدة للأمن الإلكتروني.

– زيادة العقوبات حول جرائم الأمن السيبراني واختراق الحسابات الشخصية أو المؤسسية، وجود مركز متخصص لإستقبال الشكاوي أو الإبلاغ عن الجرائم السيبرانية ، وإنشاء محاكم متخصصة في الجرائم السيبرانية .

– على مختلف مؤسسات الدولة إعداد كوادر من الفنيين والتقنيين يمتلكون الخبرة والمهارة العالية في المجال السيبراني .

– إستحداث مادة داخل كليات الإعلام متعلقة بالأمن السيبراني وعلاقته وتأثيره على الأمن القومي للدولة ... كذلك دورات للعاملين بالمجال الإعلامي ..وأيضاً المتحدثين الرسميين لمؤسسات الدولة والقائمين على مراكزها الإعلامية .

– تأمين البنية التحتية وكل موارد الدولة، والمعلومات الخاصة بكل الجهات ، خاصة بعد تفعيل منظومة التحول الرقمي .

المراجع:

1) A Trump Doctrine for the Middle East . By Martin Indyk , atlantic magazine , APRIL 14, 2018 , link: https://www.theatlantic.com/international/archive/2018/04/trump-syria-middle-east/558053/ visited: 28-3-2022

2) Thilini B. G. Herath *, Prashant Khanna and Monjur Ahmed.(2022). Cybersecurity Practices for Social Media Users: A Systematic Literature Review. Journal of Cybersecurity and Privacy.

3) علام، أسماء أبو زيد. (2021). "استراتيجيات خطاب صحافة التكنولوجيا العربية تجاه الأمن السيبراني: دراسة تحليلية مقارنة". المجلة المصرية لبحوث الرأي العام: مج. ع2.

4) قطب، بشائر.(2021). دور الصحف السعودية في تنمية الوعي بالأمن السيبراني: دراسة على القائم بالاتصال". المجلة العربية للإعلام والاتصال. ع25.

5) أبو الحسن، شريهان و أبو راضي، سمية(2021). " المخاطر السيبرانية للألعاب الإلكترونية القتالية وانعكاسها على التجنيد الإلكتروني للشباب: لعبة بابجي نموذجًا". مجلة البحوث الإعلامية. ع 57.ج3.

6) السمان، هاني.(2021)." دور اليوتيوب في التوعية بمخاطر الإرهاب الإلكتروني- دراسة ميدانية على عينة من شباب جامعات جنوب الصعيد". مجلة البحوث الإعلامية 57 . ج4.

7) الطاهر، ولاء.(2021)." آليات مركز دبى للأمن الإلكتروني للتوعية بالاستراتيجية الوطنية للأمن السيبراني للحكومات الذكية عبر منصات التواصل الاجتماعي " أنستجرام نموذجًا ". مجلة اتحاد الجامعات العربية لبحوث الإعلام وتكنولوجيا الاتصال. ع 6.

8) Erdal Ozkaya.(2022) Cybersecurity Challenges in social media, School of Computing and Mathematics, Charles Sturt Universit.

9) محمد، أميرة. (2021)." استراتيجيات مكافحة الجرائم الإلكترونية في العصر المعلوماتي تعزيزًا لرؤية مصر 2030: دراسة استشرافية". مجلة البحوث الإعلامية 58 .ج4.

10) لطفي، رشا. (2021)."جرائم الاتصال عبر الانترنت وضبط أخلاقياته في ضوء الاتجاهات البحثية الحديثة". مجلة البحوث الإعلامية. ع58.ج2.

11) الداغر، مجدي. (2021)" اتجاهات النخبة نحو توظيف الإعلام الأمني لتطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وانعكاساته على دعم وتعزيز الأمن السيبراني في مصر". المجلة العربية لبحوث الإعلام والاتصال. ع ٣٣ ابريل- يونيو .

12) نبيل، نرمين. " محددات المسئولية الجنائية لجرائم الاختراق والاعتراض والانتحال وآليات الضبط والردع في التشريعات العربية في العصر الرقمي: دراسة تحليلية مقارنة". مجلة البحوث الإعلامية. ع 56.ج3.

13) طالة ،لامية.(2020)."التهديدات والجرائم السيبرانية: تأثيرها على الأمي القومي للدول واستراتيجيات مكافحتها ". مجلة معالم للدراسات القانونية والسياسية. مج 4 .ع 2 .صـ56- 69.

14) لطفي، خالد حسن أحمد . الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية. دار الفكر الجامعي : الإسكندرية . الطبعة الأولى . 2020 م ، ص 13.

15) حسين، حياة .(2021)." الفضاء الإلكتروني وتحديات الأمن العالمي ".مجلة العلوم السياسية والقانونية، مجلد 12 عدد 1 صـ 1066 .

16) الروضان، وليد أحمد . مالفرق بين أمن المعلومات والأمن السيبراني صحيفة الجزيرة الالكترونية ، مؤسسة الجزيرة للصحافة . والطباعة والنشر ، 1431 ه . ع 16631.

17) مكتب الأمم المتحدة المعني بالمخدرات و الجريمة. (2013) استخدام الإنترنيت في أيراض إرهابية. نيويورك: الأمم المتحدة.
18) عبد الصادق، عادل. (2013)." الفضاء الإلكتروني والرأي العام". المركز العربي لأبحاث الفضاء الإلكتروني: قضايا استيراتيجية.
19) عبد الحليم، سهير عثمان. (2008). الإرهاب والإنترنت: دراسة حالة فى ضوء التجربة المصرية، ورقة مقدمة للمؤتمر الدولى الأول حماية أمن المعلومات والخصوصية فى قانون الإنترنت.القاهرة: مركز الأبحاث والدراسات القانونية،) .
20) العبودي، علي عبد الرحيم. (2019). هاجس الحروب السيبرانية وتداعياتها على الأمن والسلم الدوليين . رسالة دكتوراة منشورة ، كلية الاقتصاد والعلوم السياسية و جامعة بغداد .
21) سامانثا رافيش ، الحروب السيبرانية وأمريكا (موقع اتجاهات البيان ، تاريخ النشر 24 إبريل 2018 ، الرابط **https://www.albayan.ae/opinions/articles/2018-04-24-:** تمت الزيارة 3-3-2022.
22) محمد الدوراني ، قتال غير مرئي : الحرب السيبرانية في الأزمة الخليجية (تقرير : مركز الجزيرة للدراسات ، تاريخ النشر 13 مايو 2018 ، الرابط:**http://studies.aljazeera.net/ar/reports/2018/05/180513101447007.html** ، **تمت الزيارة 24- 3- 2022**.
23) سامانتا .. مرجع سابق
24) منى الاشقر جبور ، الأمن السيبراني : التحديات مستلزمات المواجهة (اللقاء السنوي الأول للمختصين في أمن وسلامة الفضاء السيبراني ، بيروت 27-28 أغسطس 2012 صـ 8 - الرابط **https://carjj.org/sites/default/files/wrq_ml_lmrkz_-_d._mn_lshqr.docx. تمت الزيارة 21-2-2022.**
25) عبد الصادق، عادل . أنماط الحرب السيبرانية وتداعياتها على الأمن العالمي (مجلة السياسة الدولية : ملحق اتجاهات نظرية العدد 208 ، 2017) صـ34 .
26) اسماعيل، قادير . إدارة الحروب النفسية في الفضاء الإلكتروني : الاستراتيجية الأمريكية الجديدة في الشرق الأوسط (ندوة بعنوان : عولمة الإعلام السياسي وتحديات الأمن القومي للدولة النامية ، الجزائر ، 2017) صـ 8 ، الرابط https://manifest.univ-ouargla تمت الزيارة 5-3-2022
27) الأمان في الفضاء السيبراني ومكافحة الجرائم السيبرانية في المنطقة العربية توصيات سياساتية ، الامم المتحدة ESCWA ، 9فبراير 2015م .
28) Secretariat of the Security and Defense Committee, Finland´s Cyber security Strategy. ttp://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf, p. 10.
29) عبد اللطيف، والي. كمال، بوبعاية . تفعيل دور الإعلام الأمني في مكافحة الجريمة ،مجلة الفكر القانوني والسياسي (ISSN :2588-1620 المجلد الخامس العدد الأول)2021 (ص ص : 26 ،35).
30) السراني، عبد الله بن سعود.(2012). دور الإعلام الأمني في الوقاية من الجريمة، الإعلام الأمني بين الواقع والتطلعات، مركز الدراسات والبحوث، جامعة نايف العربية للعلوم الأمنية، الرياض، 2012 ،ص 45.
31) شعبان، حمدي محمد ، الإعلام الأمني وإدارة الأزمات والكوارث، د ط، الشركة العربية المتحدة للتسويق والتوريدات، مصر، 2005 ،ص 4
32) أبو عامود، محمد سعد. الإعلام الأمني: المفهوم ، الوظائف، والإشكالات، ط1، مركز الكتاب، مصر،.92 -91 ص ص، 2006.
33) أميمة سيد أحمد ، الإعلام الرقمي .. تطورات متلاحقة وتواصل بلا حدود ، دراسة متاحة على الرابط : https://www.sis.gov.eg/Story/135966/%D8%A7%D9%84%D8%A5%D8%B9%D9%84%D8%A7%D9%85-

%D8%A7%D9%84%D8%B1%D9%82%D9%85%D9%89-..-
%D8%AA%D8%B7%D9%88%D8%B1%D8%A7%D8%AA-
%D9%85%D8%AA%D9%84%D8%A7%D8%AD%D9%82%D8%A9-
%D9%88%D8%AA%D9%88%D8%A7%D8%B5%D9%84-
%D8%A8%D9%84%D8%A7-%D8%AD%D8%AF%D9%88%D8%AF?lang=ar ،
تاريخ الزيارة 29 مارس2022.

34) علو، أحمد.(2018). " الحروب السيبرانية والعنف الرقمي واقع عالمي جديد". مجلة الجيش . ع 402 - نوفمبر 2018م .

35) سعود، باسل العنزي و عبد القادر ، فايز.(2020)" دور الإعلام الأمني في مواجهة الجرائم الإلكترونية والحد منها من وجهة نظر العاملين في الأجهزة الأمنية في دولة الكويت" . كلية التربية ،جامعة الأزهر .

36) تقرير مؤشر الأمن السيبراني لعام 2021، available at: 2022/1/ 22
https://www.rowadalaamal.com/tag/%D8%A7%D9%84%D9%85%D8%A4%D8%B4%D8%B1-%D8%A7%D9%84%D8%B9%D8%A7%D9%84%D9%85%D9%8A-%D9%84%D9%84%D8%A3%D9%85%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%A8%D8%B1%D8%A7%D9%86%D9%8A-2021/.

37) التهامي، نجية حسين. (2021). نقد التغطية الإعلامية لنشر أخبار الجريمة الأخلاقية في وسائل الإعلام الليبية: دراسة وصفية في ضوء أبعاد نظرية المسؤولية الاجتماعية، ومحددات نشر أخبار الجريمة. مجلة جامعة الزيتونة .ع 40. ص233.