دور الإعلام الرقمي في تعزيز الامن السيبراني ومكافحة التهديدات والجرائم السيبرانية

د. شيرين البحيري*

ملخص الدراسة:

تهدف الدارسة الحالية للتعرف على دور الإعلام الرقمي في تعزيز الامن السيبراني. بجانب استكشاف دوره فى مقامة التهديدات والجرائم السيبرانية. وقد تم اختيار عينة الدراسة بالطريقة العمدية من مجتمع الاعلاميين بالمؤسسات الإعلامية المصرية والتى تكونت من (٦٤) مفردة من الإعلاميين المتخصصين في تخصصات مختلفة (الصحافة ,الإذاعة والتليفزيون) بالمؤسسات الإعلامية (مؤسسة الاهرام وأخبار اليوم , الجمهورية والإذاعة والتليفزيون).

وقامت الباحثة بتصميم أداة الدراسة التى تمثلت فى استمارة الاستبيان (Questionnaire) لجمع البيانات التي تضمنت محورين اساسين للدراسة أحدهما يمثل مقياس دور الاعلام الرقمي في تعزيز الامن السيبراني. والمحور الاخر يمثل مقياس دور الاعلام الرقمي في مكافحة التهديدات والجرائم السيبرانية. وقد استخدمت الباحثة برنامج الحزم الإحصائية للدراسات الاجتماعية (spss) لتحليل نتائج الدراسة وقد توصلت الدراسة من خلال النتائج الى ان الاعلام الرقمي له دور كبير في تعزيز الامن السيبراني بدرجة مرتفعة وقد بلغ الوزن المرجح على مقياس ليكرت الخماسي لهذا المحور (٣,٥٧٢) كما بلغ الانحراف المعياري (١,٢٣٤). كما توصلت نتائج الدراسة الى ان الاعلام الرقمي يلعب دور كبير في مقاومة التهديدات والجرائم السيبرانية بدرجة مرتفعة وقد بلغ الوزن المرجح على مقياس ليكرت الخماسي (٣,٧٦٣٤) و الانحراف المعياري (١,٣٥٩٦) لمحور مقياس دور الاعلام الرقمي في مكافحة التهديدات والجرائم السيبرانية.وقد أوصت الدراسة بضرورة وضع استراتيجية متكاملة لمكافحة التهديدات والجرائم السيبرانية و قيام المستخدمين بالفهم العميق للطرق والأساسيات اللازمة لأمان البيانات والمعلومات وتنفيذ خطوات الأمان وفي مقدمتها اختيار كلمات مرور قوية. كما أوصت الدراسة بضرورة القيام بتأهيل كوادر مدربة تكون متخصصة في الأمن السيبراني ومتعمقة في مجال الفضاء السيبراني. لتمثل حائط صد قوى للتهديدات والجرائم السيبرانية.

الكلمات المفتاحية: الإعلام الرقمي، الأمن السيبراني، مكافحة التهديدات، الجرائم السيبرانية.

* الأستاذ المساعد بقسم الصحافة بكلية الإعلام- جامعة المنوفية

The Role of Digital Media in Strengthening Cyber security and Combating Cyber Threats and Crime

Abstract:

The current study aims to identify the role of digital media in enhancing cyber security. In addition to exploring his role in combating cyber threats and crimes. The study sample was selected in a deliberate way from the media community in the Egyptian media institutions, which consisted of (64) individual media professionals in different specializations (journalism, radio and television) in media institutions (Al-Ahram and Akhbar Al-Youm Foundation, Al-Gomhoria, Radio and Television). And the researcher designed the study tool, which was represented in the questionnaire (Questionnaire) to collect data, which included two main axes of the study, one of which represents a measure of the role of digital media in enhancing cyber security. The other axis represents a measure of the role of digital media in combating threats and crimes. The researcher used the statistical packages for social studies program (spss) to analyze the results of the study. The study concluded through the results that digital media has a significant role in enhancing cybersecurity to a high degree, and the weighted weight on the five-point Likert scale for this axis reached (3.572) and the standard deviation reached. The results also concluded that digital media plays a significant role in combating Cyber Threats and Crime: to a high degree, and the weighted weight on the five-point Likert scale reached (3.7634) and the standard deviation (1.3596) for the axis of the scale of the role of digital media in combating Cyber Threats and Crime:. The study recommended the need to develop an integrated strategy to combat threats and crimes and for users to have a deep understanding of the methods and basics necessary for data and information security and implement security steps, foremost of which is the selection of strong passwords. The study also recommended the necessity of rehabilitating trained cadres that are specialized in cybersecurity and in-depth in the field of cyberspace.

Keywords: Digital Media, Cyber security, Cyber Threats.

مقدمة

ان التكنولوجيا الرقمية الحديثة انتشرت بطريقة واسعة وغير مسبوقة خاصة في مجال الصحافة والإعلام فقد ساهمت فى ايجاد واقعاً فضائياً وافتراضياً ملموساً ومحسوساً يطلق عليه بالفضاء الافتراضي (السيبراني) والذي توغل وانتشر عقب الثورة الرقمية والتكنولوجية المعاصرة، والتي أدت إلى التدفق الهائل للمعلومات بشكل غزير وغير مسبوق، في ظل تعدد وسائل الاتصال التكنولوجية النافذة إلى مصادر المعلومات. وقد بات تأثير هذا الواقع الافتراضي (السيبراني) واضحاً وملموساً على حياة الأفراد والمجتمعات وقد نتج عن ذلك بعض الظواهر السلبية مثل ما يعرف بجرائم الإنترنت أو التهديدات والجرائم الإلكترونية التي يطلق عليها أيضاً التهديدات والجرائم المعلوماتية (طالة وسلام، ٢٠٢٠)[١].

ولقد انتشرت التهديدات والجرائم الالكترونية انتشاراً واسعاً في الآونة الأخيرة. تلك التهديدات والجرائم التي ارتبطت بالهجمات السيبرانية وانتهكت الامن السيبراني وتمثلت في أشكال متعددة مثل القرصنة الالكترونية وسرقة الهوية مرورًا بمحاولات الابتزاز ووصولًا إلى فقدان البيانات المهمة مثل الصور الشخصية أو العائلية. إضافة الى سرقات أرقام حسابات سواء للأشخاص أو الشركات أو المستخدمين من خلال e-mail, IP, accounts... الخ. وكذلك الهجوم عبر الأجهزة الذكية والهواتف الذكية وأجهزة الكمبيوتر واللاب توب , Virus Attack. هذه التهديدات والجرائم التي تنطلق بدوافع متنوعة من قبل مرتكبيها. تلك الدوافع قد تكون لأغراض سياسية , اقتصادية , مالية , اجتماعية أو لتحقيق أغراض اجتماعية وثقافية من خلال توسيع انتشار مفاهيم ومضامين ذات طابع إجرامي وكذلك نشر تفافة الصراعات بين الدول والمجتمعات. فالدول المتقدمة تتنافس في المصارعة نحو تحقيق أعلى مستويات من الامن السيبراني والذي يمثل حائط الصد الأول والأقوى نحو حماية المعلومات ذات الأهمية الكبرى للدول. هذا الامن السيبراني عندما يكون عند مستويات عالية من الأمان فإن المعلومات ذات الأهمية تكون بعيدة كل البعد عن المنال من قبل القراصنة أو الهاكرز أو غيرها وذلك لأنها مؤمنة بدرجة كبيرة من السرية والحماية.

لذا فإن الحروب الالكترونية أصبحت واحدة من أقوى الحروب الشرسة التي تقع بين الدول وبعضها وتزداد حدة الصراع في حالات المنازعات والمشاحنات وعدم الاستقرار وتنامى المتغيرات السريعة سواء كانت متغيرات سياسية أو اجتماعية أو اقتصادية.

لذا من الأهمية بمكان التأمين ضد الوقوع في هذه الحروب الالكترونية من خلال الارتقاء بمستوى الامن السيبراني الى اقصى درجة ممكنة حيث أنها تمثل ميدان في غاية الأهمية من ميادين المنافسة القوية بين الدول وبعضها البعض.

وتعد الدول التي تحقق تقدماً كبيراً فى الامن السيبراني من الدول القوية التي تستطيع حماية معلوماتها الحيوية التي تقيس مدى قوتها وتقدمها ومن ثم تحديد طريقة التعامل المثلى مع البنية التحتية الرقمية للاتصالات والمعلومات التي تعتبر كأمن قومي استراتيجي بالغ الأهمية.

اضافة الى الوضع في الاعتبار أن قضية الأمن السيبراني أصبحت ذات أولوية وتمثل أخطر التحديات الأمنية والاقتصادية الوطنية التي تواجه الدول. بينما الدول التي عندها ضعف في مستوى الامن السيبراني تكون عرضة للجرائم الالكترونية وسرعان ما تنال الخسارة واعلان راية الهزيمة في ميدان المنافسة في تلك الحروب الضروس التي مازالت تتنامى وتزداد حدة في صراعها يوماً بعد يوم.

وقد سارعت الدول المتقدمة في تطبيق استراتيجيات صارمة وقوية تهدف الى الارتقاء بمستوى درجات الأمن السيبراني وتقديم كافة الدعم وتوفير كل التسهيلات للشركات والمؤسسات ذات الصلة بالعمل في مجال الاتصالات والمعلومات والقيام بتطوير وتفعيل منظومات وبرامج حماية جديدة وانشاء بيئة الالكترونية رقمية قوية مناسبة تقبل كافة التغيرات المعلوماتية الحديثة. فالأمن السيبراني يتضمن عمليات متعددة مثل حماية الأنظمة والشبكات والبرمجيات المتنوعة لدى الحكومات والشركات والمؤسسات ضد تلك الهجمات الالكترونية الرقمية التي تهدف للوصول إلى المعلومات الحساسة أو القيام بتغييرها أو تدميرها بالكلية. ولتحقيق فعالية الامن السيبراني في مواجهة الهجمات السيبرانية لابد ان يشتمل على طبقات متعددة من الحماية تنتشر عبر الشبكات , أجهزة الكمبيوتر , الموبايلات , البرامج أو البيانات الحساسة المرغوب في الحفاظ عليها.

إن الالمام بالمبادئ الأساسية لتحقيق أمن البيانات والمعلومات والامتثال إليها من قبل المستخدمين مثل اختيار كلمات مرور قوية جداً متضمنة حروف وأرقام وعلامات ترقيم وتوخي الحذر من متابعة المرفقات الموجودة ضمن خدمات البريد الإلكتروني والنسخ الاحتياطي للبيانات ضرورة لابد من التوعية بها ونشر ثقافتها بين المستخدمين. وقد بلغت أهمية الاعلام الرقمي مبلغاً كبيراً في سياق مستحدثات تكنولوجيا الاتصال والمعلومات كما لعبت جهود الإعلام الرقمي عبر فضاء الامن السيبراني دور في غاية الأهمية خاصة في رسم معالم الاستراتيجيات والأمن القومي وذلك في ظل تنامي التهديدات والجرائم والتهديدات والجرائم الإلكترونية الجديدة (فرحات,٢٠١٩)[٢].

وأصبحت كافة القطاعات والهيئات والمؤسسات بشكل أساسي تعتمد اعتماداً كلياً على البنية التحتية الرقمية لتكنولوجيا المعلومات والاتصالات. وباتت تلك القطاعات والهيئات والمؤسسات تخضع لسيطرة ورقابة أنظمة إشرافية من القطاعات الأمنية وفقاً لحساسية المعلومات والبيانات المتداولة ومتطلبات الحصول على المعلومات وطبيعة العمليات التكنولوجية المعقدة الأخرى المرتبطة بها. وصارت الحكومات والمجتمعات تعتمد اعتماداً كلياً على تكنولوجيا الاتصالات والمعلومات في تقديم كافة الاشتراكات والخدمات وتعمل على إدارة العمليات عبر مناطق جغرافية مختلفة.

ان الامن السيبراني يتضمن وجود بيئة الكترونية رقمية متطورة ومتغيرة ومرتبطة بالمهارات اللازمة لعملية تطبيق وتقييم معتمدة على التقنيات الحديثة والأنظمة الأمنية الذكية. كما يتضمن القيام بعملية حماية المعلومات والأصول ذات الأهمية القصوى للمنظمة وذلك من خلال المتابعة المتصلة بإدارة مخاطر الأمن السيبراني، فضلاً عن المتابعة المستمرة للممارسات والأعمال في جميع أنحاء المؤسسة. ويساعد ذلك في تنفيذ وتحقيق المراقبة

المستمرة للشبكة والقيام بتوفير الحلول الأمنية المناسبة في الأوقات المناسبة. فالأمن السيبراني الفعال أصبح ضرورة ووسيلة لا يمكن الاستغناء عنها لضمان الحماية ومنع الانحرافات وتحقيق الأهداف التنموية والأمنية. (هيام محمد الهادي، ٢٠٢٠)[٣].

مشكلة الدراسة: -

تشهد تكنولوجيا الاتصال والمعلومات تطورًا مذهلاً وغير مسبوق في معالجة الكم الهائل من البيانات التي يتم تداولها عبر الشبكات بالهيئات والمؤسسات الحكومية والغير الحكومية. وتتمتع تكنولوجيا الاتصال والمعلومات باعتبارها الداعم الرئيسي لتطوير البرمجيات الحديثة خاصة المتعلقة بالأمن المعلوماتي كما أنها ترتبط ارتباطاً وثيقــاً بالوسائل التكنولوجية الحديثة التي يتم ابتكارها وتحديثها بصورة مستمرة مثل صناعة أجهزة الموبايل الذكية، واللاب توب والأجهزة اللوحية الذكية والتي تمثل أبرز أذرع أدوات الاعلام الرقمي. فضلاً عن كون الاعلام الرقمي يلعب دوراً محورياً في المحافظة على مستوى الأمن المعلوماتي من خلال التوعية المستمرة والارتقاء بالمستوى الثقافي لدى الافراد نحو التنمية المستدامة. لذا تسعى الدراسة الحالية للكشف عن طبيعة العلاقة بين الاعلام الرقمي والأمن السيبراني وطبيعة العلاقة بين الاعلام الرقمي والتنمية المستدامة. إضافة الى التطلع لمعرفة الدور الفعال الذي يقوم به الاعلام الرقمي في تعزيز فرص الامن السيبراني مقاومة التهديدات والجرائم السيبرانية وكذلك تحقيق فرص حقيقية نحو التنمية المستدامة. ويمكن صياغة مشكلة الدارسة في التساؤلات التالية: -

❖ **ما هو دور الاعلام الرقمي في تعزيز الأمن السيبراني؟ وما هو دوره في مكافحة التهديدات والجرائم السيبرانية؟**

أهمية الدراسة

❖ تنبع أهمية هذه الدراسة من خلال ارتباطها بموضوع في غاية الأهمية والحيوية وهو الإعلام الرقمي ودوره في تعزيز الامن السيبراني ومكافحة التهديدات والجرائم السيبرانية (الالكترونية) من وجهة نظر الإعلاميين بالمؤسسات الإعلامية المصرية.

❖ تتزايد أهمية الدراسة الحالية نظراً لتعلقها بالإعلام الرقمي وارتباطه بالأمن السيبراني الذي يؤثر بدوره بطريق مباشر نحو الاستقرار وإيجاد حلول إيجابية لتوفير بيئة خصبة تتحلى بالأمن والسلام وتتجه نحو تحقيق التنمية المستدامة.

❖ تسهم الدراسة الحالية في تقديم رؤية الإعلاميين المصريين بالمؤسسات الإعلامية المصرية عن أثر الإعلام الرقمي على الامن السيبراني وكذلك أثره فى مكافحة التهديدات والجرائم السيبرانية.

❖ تكمن أهمية هذه الدراسة في تناولها موضوع جديد يربط بين الاعلام الرقمى والامن السيبراني خاصة مع قلة الدراسات والبحوث التي تتعرض للأمن السيبراني ومكافحة التهديدات والجرائم السيبرانية.

أهـــداف الدراسة:

١)تسعى الباحثة من خلال الدراسة الحالية للتعرف على العلاقة بين الإعلام الرقمي والامن السيبراني والدور الفعال الذي يقوم به الإعلام الرقمي في دعم وتعزيز الامن السيبراني.

٢)تهدف الدراسة الحاليـــة للكشف عن طبيعة الأمن السيبراني وأهم المفاهيم المرتبطة به وكذلك التعرف على التهديدات والجرائم السيبرانية التي يتم يمكن التعرض لها.

٣)رصد وتحليل التهديدات والجرائم السيبرانية التي تهدد الامن السيبراني والوقوف على طرق مكافحة تلك التهديدات والجرائم التي تؤثر بالسلب على الاستقرار والتقدم نحو التنمية المستدامة.

٤)التعرف على الإعـــلام الرقمي والأدوات التي يتم استخدامها نحو تعزيز الامن السيبراني وحماية الأنظمة المرتبطة به.

الدراســـات السابقة:

لا شك ان الإعلام الرقمي تزداد أهميته يوماً بعد يوم خاصة في ظل التقدم التكنولوجى الهائل والذي حقق طفرة قوية وغير مسبوقة في مجالات متعددة. ويعد الامن السيبراني واحد من أهم تلك المجالات التي ليست بمنأى عن هذا التقدم. وقد تعرضت بعض الدراسات للامن السيبراني. هذه الدراسات تم تقسيمها إلى محورين، هما:

المحور الأول: الدراسات التي تناولت التوعية بالأمن السيبراني:

١-دراسة (اية عمر فرج ,٢٠٢٢)[٤] عن: دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي – جامعة الأمير سطام بن عبد العزيز نموذجاً

سعت هذه الدراسة للتعرف على دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي بجامعة الأمير سطام بن عبد العزيز، وقد استخدمت الباحثة المنهج الوصفي للدراسة، وقامت بتصميم استبان تكون من (٢٦) فقرة مقسمة على ثلاثة محاور وقد طُبقت الدراسة على عينة تمثلت من أعضاء هيئة التدريس وقد بلغت (١٢٥) عضواً من أعضا هيئة التدريس بجامعة الأمير سطام بن عبد العزيز، و اعتمدت على متغيرات: (الكلية، التخصص، سنوات الخبرة)، وتوصلت نتائج الدراسة الى أن دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي بجامعة الأمير سطام بن عبد العزيز من وجهة نظر عينة الدراسة كانت بدرجة متوسطة بالنسبة للاستبيان ؛بينما حصل محور الدواعي المجتمعية لتعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي للجامعة على متوسط (٣,٧٠)، ثم جاء محور الدواعي المعرفية لتعزيز ثقافة الأمن السيبراني بالجامعة متوسط عام (٣,٥١)، وجاء فى المرتبة الأخيرة محور الدواعي التقنية وجاء بتقدير متوسط (٣,٤٦)، كما توصلت النتائج لعدم وجود فروق ذات دلالة إحصائية لمتغير الكلية والرتبة العلمية، بينما كانت هناك فروق تعزى لمتغير سنوات الخبرة وقد أوصت الدراسة بضرورة إدراك منافع البرمجيات المتاحة لمكافحة المخاطر السيبرانية.

٢-دراسة (أسماء أحمد أبو زيد علام, 2021)[٥] عن: استراتيجيات خطاب صحافة التكنولوجيا العربية تجاه الأمن السيبراني

هدفت هذه الدراسة للتطلع والتعرف على إطار استراتيجيات خطاب صحافة التكنولوجيا العربية تجاه الأمن السيبراني في مصر والسعودية من خلال القيام بعمل الرصد والتحليل بموقع صحيفتي (اليوم السابع المصرية وعكاظ السعودية) في الفترة الزمنية بداية من العام 2018وإلى بداية العام ٢٠١٩ وقد اعتمدت الدراسة على المنهج الوصفي جبناً الى جنب مع منهجي التحليلي المقارن والمنهج المسحي وكان من أبرز نتائج الدراسة تأكيدها على ضرورة الاحتياج للأمن السيبراني فهو ضرورة دفاعية في غاية الأهمية. كما توصلت الدراسة إلى أن المخاطر السيبرانية لا يمكن مواجهتها إلا بالترابط والتكاتف بين الجميع سواء أفراد أو مجتمعات.

٣-دراسة (منال حسن محمد بن إبراهيم, 2021) [٦] عن: الوعي بجوانب الأمن السيبراني في التعليم عن بعد

هدفت هذه الدراسة للكشف عن الفاعلية لبرنامج تدريبي مقترح لتنمية الوعي بجوانب الأمن السيبراني في التعليم عن بعد لدى معلمات العلوم بالمرحلة الابتدائية بالمملكة العربية السعودية، وقد استخدمت الدراسة المنهج التجريبي. وقد اعتمدت الدراسة على أداة الدراسة التي تمثلت في مقياس تم تصميمه من قبل الباحثة لمعرفة الوعي بجوانب الأمن السيبراني في التعليم عن بعد، وقد بلغت عينة الدراسة (٣٠) معلمة من مجتمع الدراسة الممثل في المعلمات لمادة العلوم لدى المرحلة الابتدائية، وقد تم تطبيق مقياس الوعي بجوانب الأمن السيبراني في التعليم عن بعد قبليا وبعدياً بعد تدريب المعلمات على البرنامج المقترح خلال الفصل الدراسي الأول من العام 1442/1441هـ، بواقع (١٠) جلسات تدريبية. وتوصلت نتائج الدراسة الى وجود فرق ذي دلالة إحصائية عند مستوى$0,05 \geq \alpha$) (بين متوسطي درجات المعلمات في التطبيقين القبلي والبعدي لمقياس الوعي لصالح التطبيق البعدي مما يؤكد على فاعلية البرنامج التدريبي المقترح.

٤-دراسة (Ameen et al., 2021) [٧]

هدفت هذه الدراسة الى معرفة مدى امتثال الموظفين للأمن السيبراني وسياساته. وقد طبقت الدراسة على عينة من مجتمع الموظفين متعددة الثقافات و الجنسيات مثل الولايات المتحدة والمملكة المتحدة،، والإمارات العربية المتحدة هذه العينة بلغ قوامها ١٧٣٥ مفردة وقد بلغت أعمارهم ما بين (٣٥ الى ١٨)عاماً. وقد استخدمت الدراسة استبياناً الكترونياً كما استخدمت الدراسة نموذج يسمى نموذج الامتثال لأمان الهاتف الذكي study of cybersecurity across culture compliance والذى يهدف الى معرفة عمق وفهم سلوك أمن المعلومات للموظفين، واستكشاف التأثيرات الوطنية والتنظيمية والتكنولوجية (الخاصة بالهواتف الذكية) والشخصية. وقد توصلت الدراسة من خلال نتائجها على ضرورة الاستخدامات الآمنة للهواتف الذكية لدى الموظفين في العمل مع مراعاة الاختلافات الثقافية و المعرفية بين الجنسيات المختلفة وكذلك التحذير من التهديدات والجرائم السيبرانية عبر الهواتف الذكية.

٥-دراسة (Moskal,2020)[٨]

هدفت الدراسة نحو استكشاف أهمية تعزيز ثقافة الأمن السيبراني في الجامعات الامريكية وقد طبقت الدراسة على عينة من الجامعات الامريكية بلغ قوامها (١٠٠) جامعة أمريكية للاطلاع ومعرفة درجة الاهتمام بتدريس الأمن السيبراني. وقد أوضحت الدراسة تصور تطبيقي لإنشاء مركز متخصص للعمل على التدريب وزيادة الوعي التثقيفي للأمن السيبراني والمخاطر السيبرانية لدى طلاب بالجامعات الامريكية. وقد أوصت الدراسة بضرورة تدريس الأمن السيبراني بالجامعات الامريكية وكذلك العمل على زيادة الاهتمام الأمن السيبراني واعتباره أحد الدعائم الرئيسية للاقتصاد الأمريكي.

٦-دراسة (Nyinkeu et al., 2018) [٩]

هدفت هذه الدراسة لترسيخ مفهوم الأمن السيبراني الذي يجب غرسه لدى طلاب تكنولوجيا المعلومات، حيث قام الباحثون بإجراء مقابلات مباشرة مع مجموعة المبحوثين من طلاب تكنولوجيا المعلومات، وقد توصلت الدراسة من خلال نتائج استجابات عينة المبحوثين عن ضعف معرفة مفهوم الأمن السيبراني و أكدت على ضرورة أهمية تعزيز مفهوم الأمن السيبراني كما أكدت الدراسة على أهمية التمييز بين الأمن السيبراني وأمن الشبكات، وقد أوصت الدراسة بضرورة اتباع السلوكيات الأخلاقية الحميدة لدى مستخدمي شبكة الإنترنت و الأمور المتعلقة بها و البعد عن السلوكيات السلبية جراء استخدام شبكة الإنترنت.

٧-دراسة (Bustard,2018) [١٠]

هدفت هذه الدراسة لاستكشاف الانتهاكات والاخلاقيات المرتبطة بالأمن السيبراني، وقامت بتحديد وحدة مخصصة لذلك. كما سعت الدراسة لمعرفة أثر تعلم الطلبة لأخلاقيات الأمن السيبراني، وقد طبقت الدراسة على عينة من طلبة الماجستير، حيث تم عمل إعداد استبيان لقياس مدى قبول وتحقيق الرضا من قبل عينة الدراسة لتلك الوحدة وتقبلهم لتعلم الأخلاقيات و التصدي للهجمات الالكترونية من خلال الأمن السيبراني، وقد تم تدريس تلك الوحدة لمدة ثلاث سنوات متتالية من عام ٢٠١٤م الى 2017 م، وقد توصلت الدراسة من خلال نتائجها بأن عينة الدراسة لديها الرضا و القبول لتعلم الاخلاقيات المرتبطة بالأمن السيبراني بدرجة كبيرة، كما أكدت الدراسة على ضرورة التوعية للتصدي للهجمات و الانتهاكات السيبرانية حيث أن عدم التوعية يؤدى الى اثار سلبية على أمن المؤسسات و الهيئات، كما أكدت الدراسة على أهمية معالجة القضايا الأخلاقية المتعلقة بالأمن السيبراني.

المحور الثانى: الدراسات التي تناولت الأمن السيبراني والتهديدات السيبرانية

٨-دراسة (عادل عبد الصادق , ٢٠٢٢)[١١] عن: الإرهاب السيبراني والأمن القومي في بيئة متغيرة

تعرضت هذه الدراسة الإرهاب السيبراني والأمن القومي في بيئة متغيرة ومدى ارتباطها بالتطور التقني من جهة وتحول المصالح الاستراتيجية إلى الفضاء السيبراني من جهة ثانية. وتناولت الدراسة أثر انعكاس الفضاء الإلكتروني بتغير طبيعة وخصائص الأمن والقوة والصراع الدولي من خلال ثلاثة محاور أولها الأمن الإلكتروني وتأثره بالتقنيات الحديثة ,

العلاقات الدولية وعناصر القوة الأساسية ومدى تأثيرهما على الصراع في الفضاء الإلكتروني وظهور أشكال الجديدة للصراع وعلاقتها بالفضاء الإلكتروني. وقد أبرزت الدراسة العلاقة التاريخية بين التكنولوجيا والإرهاب وارتباط الرقمنة والإرهاب. قد توصلت الدراسة الى أن التطوير في التطبيقات الرقمية يؤدى الى هجرة المواقع الإلكترونية والمنتديات وغرف الدردشة والمدونات والتركيز على تطبيقات الشبكات الاجتماعية والهواتف الذكية. كما أظهرت نتائج الدراسة الممارسات الالكترونية الإرهابية ذات الطابع الرقمي عبر الفضاء الإلكتروني. كما بينت الدراسة التحديات وفرص المواجهة التي تواجه جهود مواجهة الإرهاب والتطرف عبر الشبكات الاجتماعية.

٩-دراسة (موسى بن تغري، ٢٠٢٠)[١٢] عن: الحرب السيبرانية والقانون الدولي الإنساني

سعت هذه الدراسة لإيجاد الحلول نحو تطوير قواعد وتشريعات القانون الدولي الإنسان لكي تتم مواءمتها مع النزاعات والحرب السيبرانية وقد توصلت الدراسة إلى نتيجة في غاية الأهمية وهي أن الحرب السيبرانية تمثل حرب حقيقية وليست خيالية ويمكن تطبيق قواعد القانون الدولي الإنساني عليها. كما أظهرت الدراسة من خلال نتائجها أن الهجمات السيبرانية تشكل نزاعات مسلحة حقيقيـــة في ثوبها الجديد والغير المألوف وتكون قابلة لتطبيق القانون الدولي الإنساني عليها. وكذلك مدى قابليتها للتطبيق ومدى إمكانية إلزام الأطراف الدولية نحوها.

١٠-دراسة (مالـك بـن فهـد الغبيـوي، ٢٠٢٠) [١٣]عن: الأمـن السـيبراني ودوره فـي الحـد مـن تهديـدات الأمـن الفكـري

تطلعت هذه الدراسة للتعـرف علـى الأمـن السـيبراني ودوره فـي الحد من تهديـدات الأمـن الفكـري واعتمد الباحث في دراسته على استبيان كأداة للدراسة. كما تم تطبيق المنهـج الوصفـي في الدراسة. وتوصلـت الدراسـة من خلال نتائجها كان من أبرزها اتفاق عينة الدراسة على خطورة التهديدات والجرائم الفكرية للأمـن السـيبراني والاتجاه نحو توظيف الأدوات التكنولوجية الحديثة لتعزيـز دور الأمـن السـيبراني بالمملكـة العربيـة السـعودية وكان من أبرز توصيـات الدراسة ضرورة تفعيـل دور الأمـن السـيبراني لرقابـة المحتـوى الفكـري ومتابعته إضافة الى نبـذ التطرف الفكـري ومقاومته لتقليص خطورته والحد من انتشاره عبر المواقع والصفحات الالكترونية.

١١-دراسة (Jemin Justin Lee et al., 2020) [١٤]

هدفت هذه الدراسة للكشف عن وسائل منع الجريمة قبل وقوعها من خلال استخدام تصميـــم نظام بيئيCPTED) (في عالم الفضاء الافتراضي، وتم تطبيقه على عينة بلغ قوامها 100من طلاب الدراسات العليا، وتم استخدام تحليل عامل مخاطر المعلومات الكمية (FAIR). وقد توصلت الدراسة من خلال النتائج ان علم المورفولوجيا في البيئة الافتراضية له تأثير مباشر في انتشار الجريمة، كما بينت النتائج أن استخدام لعبة بابجي لاختبار مكونات CPTED لابد له من تفاسير لافتراضات العالم الحقيقي مع إطلاق النيران في البيئة

الافتراضية للعبة. كما أكدت نتائج الدراسة أن جميع اللاعبين يصبحوا في لعبة بابجي رهن ارتكاب أعمال عنف وذلك طبقاً لقواعد اللعبة حتى يتثنى لهم استكمال مراحل اللعبة.

١٢-دراسة (Roden Judah A.,2019) [١٥]

هدفت هذه الدراسة لتقديم تحليلات متكاملة عن الألعاب الالكترونية المدعمة بالفيديو وأثارها على القائمين بممارسة تلك الألعاب. وتعرضت الدراسة لتاريخ صناعة الألعاب الالكترونية والمراحل التاريخية عبر الفترات الزمنية التي مرت بها تلك الألعاب الالكترونية وما أحدثته التطورات التكنولوجية الحديثة للأجهزة والبرمجيات من تحديثات سريعة ومتلاحقة لهذه الألعاب وكذلك علاقتها بالتغيرات الثقافية للمجتمع وارتباط التغيرات الثقافية والمجتمعية بالأمن المعلوماتي.

١٣-دراسة (William Crumpler et al.,2019) [١٦]

سعت هذه الدراسة للتطلع واستكشاف التحديات التي تواجهها الشركات التجارية في اختيار وتشغيل القوى العاملة الماهرة بمجال الأمن السيبراني للعمل على حماية الأنظمة ضد الهجمات السيبرانية واستخدم الباحث المنهج الوصفي للدراسة. كما قام الباحث بإجراء المقابلة مع عدد (٣٦) من أصحاب الشركات التجارية بالولايات المتحدة الأمريكية. وقد توصلت الدراسة الى ان ٨٢% من أصحاب الشركات التجارية يعانون من نقص المهارات للعمل مجال الأمن السيبراني وقد أوصت الدراسة بضرورة التعاقد مع مدربين مهرة وذوي الخبرة للعمل على التدريب والدعم للقوى العاملة والارتقاء بمستوى القوى العاملة ومهاراتها بمجال الأمن السيبراني.

١٤-دراسة (حسن محمد حسن , ٢٠١٨) [١٧]عن: مخاطر استخدام الفضاء السيبراني في الحياة الاجتماعية والثقافية والأسرية دون حماية وآثارها

تطلعت تلك الدراسة للتعرف على التأثيرات السلبية الناجمة عن استخدام مواقع التواصل الاجتماعي وبعض المواقع الأخرى على المعلمين من خلال التعرض للتشكيك لبعض الثوابت والمعتقدات الدينية والقيام بالترويج للأفكار الهدامة والمتناقضة مع الحقيقة لزعزعة العقيدة والاتجاه نحو التطرف والميل عن الاعتدال والانحراف الأخلاقي والضرب في العقيدة للخروج عن التعاليم الدينية السمحة. وقد أوصت الدراسة بتجنب تلك المواقع الهدامة والتي تبث الأفكار المتطرفة وأكدت الدراسة أن التسلح بالعلم والايمان ونشر تعاليم الدين الحنيف هو خير وسيلة للقضاء على التأثيرات السلبية الناجمة عن استخدام مواقع التواصل الاجتماعي.

١٥-دراسة (تغريد حمد الرفاعي, ٢٠١٨) [١٨]عن: درجة ممارسة وتعرض طلبة المرحلة المتوسطة في مدارس دولة الكويت للتنمر الإلكتروني وأثر متغير الجنس

هدفت هذه الدراسة لاستكشاف والتطلع لمعرفة ممارسة طلبة المرحلة المتوسطة للتنمر الإلكتروني بالمدارس الكويتية، ومدى تعرضهم هؤلاء الطلاب لعملية التنمر الإلكتروني، ولقد توصلت الدراسة الى نتائج كان من أبرزها أن معدل ممارسة التنمر الإلكتروني لعينة الدراسة من المرحلة المتوسطة في مدارس مدينة الكويت كان مرتفع، وكذلك درجة تعرض

الطلاب للتنمر الإلكتروني كانت مرتفعة. وقد أوصت الدراسة بضرورة عمل أنشطة وبرامج تثقيفية للطلاب تهدف لتعريفهم بحقوقهم، ومنحهم للقدرة في التصدي لظاهرة التنمر الإلكتروني. كما أوصت الدراسة بضرورة تطوير المناهج الدراسية وأهمية تضمينها برامج حديثة وتأهيل الطلاب لمواجهة هجمات التنمر الإلكتروني.

١٦-دراسة (Ion Goran,2017) [١٩]

هدفت هذه الدراسة للتطلع لمعرفة المحاور الرئيسية التي يعتمد عليها الأمن السيبراني وطرق التصدي للهجمات السيبرانية التي يتعرض لها طلاب المرحلة الثانوية، وتحديد المتطلبات اللازمة لتحقيق الأمن السيبراني الخاصة بطلبة المرحلة الثانوية. وقد قام الباحث بإجراء العديد من المقابلات مع معلمين ومعلمات المرحلة الثانوية وقد أبرزت الدراسة من خلال النتائج العديد من الهجمات السيبرانية، وكان في مقدمتها التصيد الإلكتروني، والبرمجيـــات الخبيثة التي تشمل التلاعب بنتائج الاختبارات الإلكترونية، وقد أوصت الدراسة بأهمية رفع مستوى وعي الطلاب بأساسيات الأمن السيبراني والتعرف على طرق تجنب محاولات الانتهاكات والهجمات السيبرانية.

١٧-دراسة (يوسف بوغرارة, ٢٠١٧) [٢٠]عن: الأمن السيبراني الاستراتيجية الجزائرية للأمن والدفاع في الفضاء السيبراني

سعت هذه الدراسة للتطلع لمعرفة فعالية الإصلاحات الجزائرية في تحقيق الارتقاء وتحسين مستويات عالية للأمن السيبراني، وقد استخدمت الدراسة المنهج الوصفي للعرض والتحليل القوانين والمعاهدات الدولية المختصة بالتهديدات والجرائم السيبرانية. وكذلك استخدمت المنهج المسحي لاستعراض الوقائع والاحداث المتعلقة بموضوع الدراسة. وقد توصلت الدراسة أن الأمن السيبراني يواجه صعوبات متعددة في مقدمتها تفاوت واختلاف قدرات الوسائل التكنولوجيا للأنظمة وكذلك وجود ثغرات سيبرانية التي تنقسم الى ثغرات تقنية وثغرات قانونية التي تتطلب المعالجة والإصلاحات الملحة.

التعقيب على الدراسات السابقة:

مما سبق ومن خلال استعراض للأدبيات والدراسات السابقة المتعلقة بالأمن السيبراني يمكن تحديد عدد من النقاط التي تمثل محل توافق أو اختلاف بين الدراســـة الحالية والدراسات السابقة التي ساعدت الباحثة في الوصول الى بعض العناصر التي ساهمت في توجيه الدراسة الحالية، ومن هذه النقاط:

- لقد اتفقت الدراسة الحالية مع بعض الدراسات السابقة في استخدام وتطبيـق أداة التحليل الإحصائي. وهي برنامج(SPSS) الذي تم استخدامه في تحليل البيانات ومعالجتها للوصول الى نتائج الدراسة.
- كما اتفقت الدراسة الحالية مع الدراسات السابقة في استخدام وتطبيق المنهج الوصفي للدراسة وكذلك استخدام المسح بالعينة على عينة الدراسة.
- بينما اختلفت الدراسة الحالية عن الدراسات السابقة في عينة الدراسة.

- كما اختلفت الدراسة الحالية عن الدراسات السابقة في تصميم أداة الدراسة وهي استبيانه تم تصميمها بواسطة الباحثة.
- اختلفت المتغيرات التي اعتمدت عليها الدراسة عن الدراسات السابقة.

الاستفادة من الدراسات السابقة:

١-من الناحية النظرية

لقد استفادت الباحثة من خلال ما تم استعراضه من دراسات سابقة لاستكشاف الأطر المعرفية للدراسة التي ركزت على الامن السيبراني وكيفية مقامة الهجمات السيبرانية. إضافة الى التعرف على الدور الفعال للإعلام الرقمي الحديث في تعزيز الامن السيبراني ومكافحة التهديدات والجرائم الإلكترونية وتجنب أثارها وتعميق جوانب التصور البحثي في هذا الاتجاه.

٢-من الناحية المنهجية:

ساهمت الدراسات السابقة في توجيه الباحثة نحو اختيار وتحديد الإطار المنهجي المناسب للدراسة الحالية وكذلك تحديد المنهج الملائم لها.

الإطار النظرى للدراسة

نظرية انتشارالمستحدثات (Diffusion of Innovations theory)

تعنى هذه النظرية (**Diffusion of Innovations Theory**) بطريقة تكيُّف التكنولوجيا الحديثة و تطويعها نحو نشر التكنولوجيا والأفكار الجديدة و المستحدثة بين أفراد المجتمعات المحددة و يرجع الفضل في ابتكار هذه النظرية الى (Everett Rogers) [٢١] الذى عرف نشر المستحدثات بأنها عملية يتم من خلالها انتشار فكرة أو مفهوم أو سلوك مستحدث بين أفراد نظام اجتماعى معين في فترة زمنية محددة و يكون معدل انتشار المستحدثات متفاوت بناءاً على عدة عوامل أو خصائص أساسية مثل :قابلية التداول أو التجريب (**Trialability**), درجة التعقيد وسهولة الفهم (**Compatability**) والمزايا النسبية للشئ المستحدث (**Advantage Relative**), قابلية الملاحظة ووضوح النتيجة **Observability**) و يعتمد مدخل هذه النظرية على مصطلحين أساسين هما **الانتشار (Diffusion)** و الذى يعنى بعملية نقل المستحدث عبر قنوات الاتصال في وقت محدد بين أعضاء النظام الاجتماعى حيث تبدأ عملية تبنى نقل الفكرة أو المستحدث. و المستحدث (**Innovation**) و الذى يعنى الفكرة أو المستحدث الجديد الذى يسود انتشاره بين أعضاء النظام الاجتماعى.

كما أن هناك عدة محددات أو عوامل أخرى ذات تأثير في عملية انتشار ونقل المستحدثات مثل:

- التكلفة المادية للشئ المستحدث فثم وجود علاقة عكسية بين انتشار المستحدث والتكلفة المادية فكلما زادت تكلفة المستحدث قل معدل انتشاره.

➢طبيعة المجتمع الذي يتبنى نشر المستحدث فكلما زاد معدل تحضر المجتمع سمح بوجود بيئة خصبة لانتشار المستحدث.

➢المستوى التعليمى للمجتمع الذي يتبنى نشر فكرة المستحدث فكلما ارتفعت درجة تعليم المجتمع و ارتقى كان ذلك أدعى لانتشار المستحدث والعكس صحيح.

➢العادات والتقاليد السائدة في المجتمع فكلما كان المجتمع أكثر انفتاحاً وتطلعاً للمستجدات والمستحدثات كان أكثر قبولاً وتوعية بإنتشار المستحدث.

مدى استفادة الدراسة الحالية من نظرية نظرية انتشارالمستحدثات (Diffusion of (Innovations theory

استفادت الدراسة الحالية من نظرية انتشارالمستحدثات (Diffusion of Innovations theory) في التعرف على مفاهيم الإعلام الرقمي والأمن السـيبراني والتهديدات والجرائم السيبرانية. بخلاف التعرف على طبيعة العلاقة بين الإعلام الرقمي والامن السيبراني. فضلاً عن في التعرف على مجالات تطبيق الأمـن السيبراني. حيث أنها تعد مستحدثاً جديدً يتنشر في المجتمعات التي تسعى الى تحقيق الامن والاستقرار ومن ثم تحقيق التنمية المستدامة.

تساؤلات الدراسة:

- ما هي طبيعة العلاقة بين الإعلام الرقمي والامن السيبراني وما هو الدور الذي يقوم به الإعلام الرقمي في دعم وتعزيز الامن السـيبراني؟
- الى أي مدى يكون تأثير الإعلام الرقمي فى مقاومة التهديدات والجرائم السيبرانية؟
- كيف يرى المبحوثون طبيعة الأمن السـيبراني؟ وكيف تكون رؤيتهم عن المفاهيم المرتبطة بالأمن السـيبراني والتهديدات والجرائم السيبرانية التي يمكن التعرض لها؟
- ما هي أهم التهديدات والجرائم السيبرانية التي تهدد الامن السيبراني والتي تمثل العائق الأساسي أمام تحقيق الاستقرار وتحقيق التنمية المستدامة؟
- كيف تكون العلاقة بين المحتوى المعلوماتي الرقمي والامن السيبراني؟

الإجراءات المنهجية للدراسة

نوع الدراسة (study Type)

ان هذه الدراسة تنتمي الى الدراسات الاستكشافية (Discovery Studies) حيث أنها تشتمل على أفكار مبتكرة تجمع بين الإعلام الرقمي والأمن السـيبراني وتقوم بتوفير قدر كبير من المعرفة المرتبط بذات الموضوع. فضلاً عن أنها تنتمي للدرسات الوصفية (Descriptive Studies) وذلك نظراً لكونها تسعى للبحث والتنقيب عن العوامل الأساسية والمؤثرة المرتبطة بالموضوع واستخراج التصورات والاراء لعينة الدراسة من مجتمع الاعلاميين المتخصصين عن الإعلام الرقمي ودوره في تعزيز الأمن السـيبراني و مقاومة التهديدات والجرائم السيبرانية.

منهج الدراسة (Study Syllabus):

تنتمي الدراسة الحالية للدراسات الوصفية (Descriptive Studies) التي استخدمت فيها الباحثة المنهج الوصفى (Survey Syllabus) والذي يعتمد على المسح بالعينة (Sample Survey Methodology) حيث يتم وصف الظاهرة المرتبطة بموضوع الدراسة للإجابة عن التساؤلات التي أثيرت فى مشكلة الدراسة وذلك من خلال استجابات المبحوثين من مجتمع الدراسة المتمثل في الاعلاميين المتخصصين في تخصصات متنوعة (الصحافة ,الإذاعة والتليفزيون) والعاملين بالمؤسسات الإعلامية المصرية. وهذا المنهج المستخدم ملائم لموضوع الدراسة ويهدف للتعرف على علاقة الإعلام الرقمي والامن السيبراني والدور الفعال الذي يقوم به الإعلام الرقمي في دعم وتعزيز الامن السيبراني بالمؤسسات الإعلامية المصرية.

وكذلك التطلع لاستكشاف أهم التهديدات والجرائم السيبرانية التي تهدد الامن السيبراني وتمثل العائق الأساسي أمام تحقيق الاستقرار وتحقيق التنمية المستدامة بالمؤسسات الإعلامية المصرية. حيث قامت الباحثة بتصميم استمارة استبيانه التي تمثل أداة الدراسة وهي عبارة عن استمارة تضمنت محورين أساسين. أحدهما كمقياس الاعــلام الرقمي ودوره في تعزيز الامن السيبراني (cyber security) بالمؤسسات الإعلامية المصرية والتي اشتملت (١٤) فقرة.

بينما المحور الثاني يمثل مقياس الاعــلام الرقمي ودوره في مكافحة التهديدات والجرائم السيبرانية بالمؤسسات الإعلامية المصرية والتي تضمنت (١٢) فقرة. وذلك بعد تحكيمه وضبطه من أساتذة وخبراء محكمين متخصصين.

وبعد الانتهاء من جمع الاستمارات العائدة من المستجوبين (عينة الدراسة) تم استبعاد الاستمارات الغير مستوفاة والغير مكتملة. شرعت الباحثة بالقيام والتحليل الوصفي للبيانات الاحصائية التي تم جمعها في استمارة استبيانه باستخدام برنامج الحزم الإحصائية للدراسات الاجتماعية (SPSS).

مجتمع وعينــة الدراسة(Study Community and Sample):

تم تطبيق أداة الدراسة وهي استمارة استبيانه (Questionnaire)على عينة من الاعلاميين المتخصصين في تخصصات متنوعة (الصحافة ,الإذاعة والتليفزيون) والعاملين بالمؤسسات الإعلامية المصرية وقد بلغ قوام عينة الدراسة (٦٤) مفردة من مجتمع الدراسة الذي يمثل مجتمع الإعلاميين من تخصصات مختلفة (الصحافة ,الإذاعة والتليفزيون). وقد اختيرت عينة الدراسة بعناية بالطريقة العمدية من الإعلاميين المصريين العاملين بالمؤسسات الإعلامية (مؤسسة الاهرام وأخبار اليوم , الجمهورية , والإذاعة والتليفزيون).

أدوات الدراســة:

اعتمدت الباحثة في الدراسة الحالية على استخدام استمارة الاستبانة (Questionnaire) التي تمثل أداة الدراسة وقد اشتملت تلك الاستبانة على محورين أساسين. المحور الأول الذي

يمثل مقياس الاعــلام الرقمي ودوره في تعزيز الامن السيبراني (cyber security) بالمؤسسات الإعلامية المصرية والذي اشتمل على (١٤) فقرة.

بينما تضمن المحور الثاني والذي يمثل مقياس الاعــلام الرقمي ودوره في مكافحة التهديدات والجرائم السيبرانية بالمؤسسات الإعلامية المصرية والذي تضمن (١٢) فقرة.

كما قامت الباحثة بتطبيق مقياس ليكرت الخماسي ومعامل الفا كرونبـاخ لقياس درجة ثبات وصدق فقرات المحاور من خلال استخدام برنامج الحزم الإحصائية للدراسات الاجتماعية (SPSS) حيث تم عمل التحليل الوصفي للبيانات الاحصائية المجمعة باستمارة الاستبانة.

إعداد أدوات الدراسة واجراءات الصدق والثبات:

في البداية تم سحب عينة عمدية استرشادية بلغ عدد قوامها (٧) مفردة من الإعلاميين من تخصصات مختلفة (الصحافة ,الإذاعة والتليفزيون) بالمؤسسات الإعلامية (مؤسسة الاهرام وأخبار اليوم , الجمهورية , والإذاعة والتليفزيون). لاختبار أداة الدراســة وهي استمارة الاستبانة (Questionnaire) التي تم تصميمها من قبل الباحثة وتم تطبيقها عليهم بعد ما تم تنقيحها وضبطها وعرضها على عدد من المحكمين المتخصصين.

وبعد خمســة عشر يوم من التطبيــق الاول تم اعادة تطبيق الاستبانة (Questionnaire) مرة أخرى على عينة الدراسة الاساسية (٦٤) مفردة من الإعلاميــن من تخصصات مختلفــة (الصحافة ,الإذاعــة والتليفزيون) بالمؤسســات الإعلاميــة (مؤسسة الاهرام وأخبار اليوم , الجمهورية والإذاعــة والتليفزيون). وهي مختلفة تمامــاً عن العينة الاسترشادية وقد أتت النتائج متوافقة ومتسقة بين كل من التطبيقين الاول والثاني بنسبة (٨٧%) مما يعنى القيام بتحقيق ثبات المقياس لأداة جمع البيانات والتأكد من صلاحية تطبيقها. حيث يقصد بالاتساق والتوافق في أداء أفراد العينة من فقرة لأخرى داخل الاستبانة، وعندما تكون الأداة متجانسة فإن الفقرة تقيس نفس العوامل التي تقيسها الأداة (غادة عيد،2012) [٢٢].

في حين تم استبعاد (٣) استمارة من المستجيبين الذين كانوا قد اشتركوا في التجربة الاسترشادية التي اشتملت على (٧) مفردة مختلفة عن عينة الدراسة.

المعالجة الاحصائيــة: -

تم استخدام برنامج الحزم الاحصائية (SPSS) لتحليل النتائج التي تم جمعها من عينة الدراسة من بين مجتمع الدراسة وقد تم تجميع (٦٤) استمارة استبيان من (٦٧) مفردة من الإعلاميــن من تخصصات مختلفــة (الصحافة ,الإذاعــة والتليفزيون) بالمؤسســات الإعلاميــة (مؤسسة الاهرام وأخبار اليوم , الجمهورية اليوم والإذاعــة والتليفزيون). بينما بلغ عدد المستجيبين (٦٤) مفردة فقط. الذين قاموا باستكمال استمارة الاستبانة وتم استبعاد الاستمارات الغير مستوفاة (٣) استمارات غير مكتملة. وتم استخدام جداول التكرارات والنسب , إضافة الى ذلك تم تطبيق مقياس ليكرت الخماسي لبيان درجة (الموافقة والرفض) على كل فقرة من فقرات الاستبانة.

كما تم تطبيق معامل الفا كرونباخ الذي يقيس معامل الثبات لفقرات الاستبانة ومدى التقارب والتجانس بين بعضها البعض. وكانت قيمة معامل الفا كرونباخ (٠,٩٣١٧) لقياس درجة ثبات وصدق فقرات المحور الاول. في حين بلغت قيمة معامل الفا كرونباخ(٠,٩٣٥٢)لقياس درجة ثبات وصدق فقرات المحور الثاني من الاستبانة. والقيم السابقة لمعامل الفا كرونباخ توضح التقارب والتجانس بين فقرات الاستبانة في حين بلغت قيمة معامل الفا كرونباخ (٠,٩٠١) لقياس درجة ثبات وصدق فقرات الاستبانة كوحدة واحدة وهذه القيمة تؤكد التجانس والتقارب بين فقرات الاستبانة.

محددات الدراسة:

أولاً: الحد الموضوعي الذي اعتمدت عليه الدراسة الحالية اشتمل على محورين أساسين:

المحور الاول: مقياس الاعـلام الرقمي ودوره في تعزيز الامـن السـيبراني (cyber security) والذي اشتمل (١٤) فقرة.

المحور الثاني: مقياس الاعـلام الرقمي ودوره في مكافحة التهديدات والجرائم السيبرانية والذي اشتمل على (١٢) فقرة.

الحد البشرى: تمثلت عينـة الدراسة من (٦٤) مفردة من الإعلاميـن المتخصصين في تخصصات مختلفـة (الصحافة ,الإذاعـة والتليفزيون) بالمؤسسـات الإعلاميـة (مؤسسة الاهرام وأخبار اليوم , الجمهورية والإذاعـة والتليفزيون).

الحد المكاني: اقتصرت الدراسة على المؤسسات الإعلامية المصرية الممثلة في (مؤسسة الاهرام وأخبار اليوم , الجمهورية والإذاعـة والتليفزيون).

الحد الزماني: تم تطبيق هذه الدراسة على عينة عمدية من الإعلاميـن المتخصصين في تخصصات مختلفـة (الصحافة ,الإذاعـة والتليفزيون) بالمؤسسـات الإعلاميـة (مؤسسة الاهرام وأخبار اليوم , الجمهورية والإذاعـة والتليفزيون). وذلك في الفترة الزمنية من شهر يناير ٢٠٢٢ الى نهاية يوليو ٢٠٢٢.

الإطار المعرفى للدراسة

ان التطورات الغير مسبوقة للوسائل التكنولوجية ذات المعلوماتية المتغيرة والتوسع في انتشار تطبيقات التقنيات الرقمية الحديثة باتت تستعمل في مجالات متعددة بصفة مستمرة في الحياة اليومية خاصة في الاعلام الرقمي وارتبطت هي الأخرى بالأمن المعلوماتي في مختلف المؤسسات الهيئات على مستوى الافراد والمجتمعات.و مما لا يدع مجالاً للشك أن الإعـلام الرقمي يلعـب دوراً فاعـلاً وأساسياً فـي تحقيـق الأمـن السيبراني والاستقرار وكذلك في تطوير وتحسين التنمية المستدامة مـن خـلال الدعـم الشامل ضبط الحـس الأمنـي والوقائـي وتوسـيع الأفق والاطر الثقافية والمعرفيـة لدى الافراد والشعوب وكذلك تعزيز الانتماء والولاء الوطني مـن خـلال التوعية الاعلاميـة عبر القنوات الفضائية القومية والخاصة وكذلك المواقع الاجتماعية والصفحات الإلكترونية وغيرها من الوسائل الإعلامية الرقمية الحديثة (مبـارك بـن واصـل الحازمـي, ٢٠٢١) [٢٣].

حيث يمثل الإعلام الرقمي الحديث وسيلة نافعة ضابطة وناعمة لنشر ثقافة الوعي والأمن المعلوماتي، وذلك بما توصلت به التكنولوجيا الحديثة من تطورات وعمل نقلة تكنولوجية رقمية غير مسبوقة فهي تمثل منصة واسعة الانتشار والاستخدام. ولكن الاستخدام قد يكون مشروع أو غير مشروع وذلك وفقا للنوايا الاجتماعية والأيديولوجية والنفسية لدى المستخدمين. هذا الأمر الذي فتح المجال للتوسع في الاستخدامات الغير مشروعة والتي تعد سبباً رئيساً في وضع الافراد والمجتمعات والحكومات أمام تحديات ليست يسيرة لأنواع مستحدثة من التهديدات والجرائم التي انتحلت الصفة الإلكترونية وأخذت أشكال متعددة مثل القيام بتدمير البيانات والمعلومات الحساسة بخلال القيام بسرقة أرصدة الأموال والحسابات المالية إضافة الى المقدرة على انتهاك الخصوصيات والقيام بفك الشفرات وانتهاك المواقع الرسمية وغيرها.

في عام (٢٠١٢م) سعت الأمم المتحدة لعمل دراسة مسحية عن طريق مكاتبها لحصر (١٩٣) دولة , وقد توصلت الى أن (١١٤) دولة فقط التي كانت تتبنى برامج للأمن السيبراني وقد أنشأت الولايات المتحدة معهد لإعداد وتنفيذ برامج قصيرة مختصة بالأمن السيبراني تكون بمثابة تدريب للطلاب والمعلمين واثرائهم بثقافة الأمن السيبراني في دورات تدريبية مكثفة ومتفاوتة (2016,Mangold) [٢٤].

ان الأمن السيبراني تتزايد أهميته يوماً بعد يوم فقد أصبـــح مرتبط بالعديد من المجالات والأنشطة الحياتية المتنوعة مثل الجوانب الاقتصادية والتعليمية، والاجتماعيــة، والإنسانية، إضافة الى أنه يعتبر ممثلا لقدرة الحكومات على حماية مصالحها وشعوبها. كما أنه الداعم الأساسي للنهوض نحو التقدم وتحقيق الطموحات التنموية المنشودة في مختلف المجالات الحياتية اليومية المتنوعة، (منى جبور،،٢٠١٢) [٢٥].

ان الأمـن السـيبراني يمثل سـلاحاً اسـتراتيجياً يتم استخدامه عن طريق الحكومـات لحمايـة الأفـراد والمجتمعات بعدمـا أصبحـت الحـرب السـيبرانية واقعـاً ملموساً وقد ظهـر مفهـوم الـردع السـيبراني كمفهوم خاصـاً لقطع الطريق على جميع الاعمال الضـارة ضـد الأُصـول الوطنيـة أو القومية فـي الفضـاء السيبراني، و يعتمد على ثلاثـة مبـادئ التي تتمثـل فـي المصداقيـة في الدفـاع والقـدرة علــى الــردع السـيبراني في أي لحظة لمنع وقوع الخطر بخلاف الرغبــة الموجودة فــي الــردع السـيبراني.و القيام بوضع الضوابـط والتشـريعات لحمايـة حقـوق الأفـراد (علم الدين بانقا,٢٠١٩) [٢٦].

مصطلحات الدراسة:

الإعلام الرقمي إصطلاحاً (Digital Media) ,

يعرف (Richard Berry)[٢٧] الإعلام الرقمي بأنه كل الوسائل الإعلامية الحديثة التي ترتبط بطريقة مباشرة أو غير مباشرة بتكنولوجيا الاتصال والمعلومات وتعتمد في المقام الأول على الشبكة العنكبوتية (الإنترنت). حيث أن جميع المعلومات والبيانات التي يتم تداولها من خلال وسائل الإعلام يتم ترميزها على صورة أرقام فضلاً عن كون معالجتها

يكون(Digital)كما يطلق عليها أحياناً الإعلام (online media) عن طريق الإنترنت ويشتمل الإعلام الرقمي وسائط متعددة (مثل الصور المرئية والصوت.)

الإعلام الرقمي إجرائياً (Digital Media)

تعرف الباحثة الإعلام الرقمي على أنه الإعلام الإلكتروني أو الإعلام التفاعلى وهو الشكل الجديد للاعلام الذى يعتمد بشكل كلى ليس على شبكة الإنترنت وفقط بل على التكنولوجيا الحديثة و الوسائل و الأدوات الرقمية مثل (الصحف الإلكترونية ,التلفزيون الرقمي, تلفزيون الإنترنت, منتديات الحوار ,المدونات, مواقع الشبكات الاجتماعية ,شبكات المجتمع الافتراضية, الإذاعات الرقمية, الهواتف النقالة التي تبث الإذاعات الرقمية, البث التلفزيوني التفاعلي والوسائط المتعددة) في نقل و تداول المواد الإعلامية و الصحفية إضافة الى التواصل مع القاعدة العريضة من الجمهور حيث أنه أصبح يحل تدريجياً بديلاً للإعلام التقليدي الذى يعتمد على الورق. فالإعلام الرقمي يعتمد بشكل أساسي على عرض البيانات والمعلومات المكتوبة والمرئية والمسموعة عبر الإنترنت من خلال استخدام الأجهزة الرقمية والهواتف الذكية.

الأمن السيبراني إصطلاحاً (Cyber Security)

تعنى كلمة الأمن السيبراني كل الوسائل والأدوات التقنية والفنية المتنوعة والتنظيمية والإدارية التي يمكن استخدامها أو تطبيقها في الكثير من المناحي التكنولوجية بهدف تجنب أضرار الهاكرز والأشخاص الذين يريدون اختراق الشبكات ويقومون بالتعرض لها بالمخاطر الالكترونية وكذلك تشمل حماية السرية والخصوصية ومواجهة مخاطر الفضاء السيبراني.

وقد عرفه (**Richard A. Kemmerer**, 2008)[٢٨] هو عبارة عن وسائل دفاعية تهدف لكشف وإحباط محاولات الاختراق وانتهاك التي يقوم بها القراصنة.

بينما عرفهما (**ياسمين والحسين**, ٢٠٢١)[٢٩] بأمن تكنولوجيا المعلومات الذي يشتمل على حزمة العمليات والإجراءات التي يتم اتخاذها لحماية الشبكات والأجهزة والبرامج والبيانات من الهجوم أو السرقة أو الاختراق أو التلف، ويشمل الأمن السيبراني مجموع الوسائل التقنية والتنظيمية والإدارية، لمنع سوء الاستغلال.

بينما تم تعريف الأمن السيبراني من قبل (المنتشري وحريري,٢٠٢٠) [٣٠] بأنه يمثل جميع الاجراءات الخاصة بحماية شبكات المعلومات ضد كل الأعمال والممارسات التي تهدف التلاعب بالمعلومات، وإلحاق الضرر بالمستخدمين، وكذلك الحماية ضد الاختراق، وبث البرمجيات الخبيثة والفيروسات.

الأمن السيبراني إجرائياً (Cyber Security)

تعرف الباحثة الأمن السيبراني على أنه هو الأمن المسئول عن حماية الأنظمة والمؤسسات من الاختراقات والهجمات الالكترونية والتهديدات والجرائم السيبرانية التي تتعرض لخصوصية البيانات والمعلومات لاسيما الحساسة منها سواء عن الافراد أو المؤسسات أو

غيرها كما أنه هو المسئول عن منع الدخول لغير المصرح لهم على تلك الأنظمة. فالأمن السيبراني يهتم بحماية المعلومات أو البيانات والتأكد من تأمين خصوصيتها بصفة أساسية. إضافة الى أنه يمثل واحد من أهم أذرع الاستراتيجية اللازمة للحكومات والهيئات والمؤسسات حيث أنه يعتبر جزء لا يتجزأ من الأسلحة الحديثة التي ينبغي التسلح بها لمنع التعرض للمخاطر السيبرانية الحديثة. فضلاً عن الامن السيبراني يمثل واحد من أهم الركائز الأساسية في الاقتصاد القائم على التكنولوجيا الذكية لتحقيق التنمية المستدامة.

التهديدات والجرائم السيبرانية إصطلاحاً

يقصد بكلمة التهديدات والجرائم السيبرانية (الإلكترونية) تلك الهجمات التي تتم باستخدام التقنيات الحديثة والهواتف الذكية والشبكات الإلكترونية وتستهدف سرقة المعلومات والبيانات خاصة البيانات الحساسة ذات القيمة العالية وإلحاق الضرر بالشبكات والأجهزة الإلكترونية الأخرى(Melnick J.,2018) [٣١].

التهديدات والجرائم السيبرانية إجرائياً (Cyber Threads)

تعرف الباحثة التهديدات والجرائم السيبرانية على أنها جميع الاختراقات أو الاستخدامات الغير مشروعة وما تشمله من تعديلات أو تعطيلات للشبكات وأنظمة التقنيات للمعلومات والاتصالات والأنظمة التشغيلية ومكوناتها (الأجهزة والبرمجيات والخدمات) التي تعنى بالنظام المعلوماتي وتتخذه كوسيلة لارتكاب جرائم غير تقليدية، إما ضد الأموال كالتحويل الإلكتروني غير المشروع للأموال، أو ضد الأشخاص كجريمة السب والقذف عبر الإنترنت أو غيرها.

و كلمة "**سيبراني**ُمشتقَّة من الكلمة اليونانية (Kybernetes) التي تعني فن القيادة والتحكم عن بعد

بينما كلمة **الفضاء السيبراني** طبقاً لتعريف وزارة الدفاع الأمريكية تعنى مجال مفتوح يتسم باستخدام البيئة الإلكترونية التي تعتمد على تكنولوجيا المعلومات وكذلك الطيف الكهرومغناطيسي في تخزين البيانات ومعالجتها وتعديلها وتبادلها عن طريق أنظمة شبكات الاتصال والبنية التحتية المادية المرتبطة بها" وقد استبقت بعض الدول لإعداد استراتيجيات قوية لحماية الامن السيبراني لديها ومكافحة التهديدات والجرائم السيبرانية مثل المملكة المتحدة البريطانية التي وضعت إستراتيجية للأمن السيبراني كان هدفها حماية الأنشطة التجارية السيبرانية على الإنترنت مع استثمار علوم التكنولوجيا وأمن المعلومات لتمكين التفوق في القدرة المعرفية والعلمية للأمن السيبراني وتوفير الفاعلية والمرونة لمنع التهديدات والجرائم السيبرانية (أميرة محمد محمد أحمد، ٢٠٢١) [٣٢].

وذلك في ظل صراع الحروب السيبرانية (حروب الجيل الخامس) التي تتزايد يوماً بعد يوم.

لذا يلزم البحث في الفضاء السيبراني والإلمام بما يمكن أن يتسبب في زيادة صراع الحروب السيبرانية والعمل على الحد من هذه الصراعات والوقوف على منع مسبباتها.

وتعنى كلمة **الحرب السيبرانية** هي الحرب التي تعتمد على التوظيف الكامل والمتكامل للعمليات الرقمية ,الأنشطة السيبرانية ,أنشطة الحاسوب ,الحرب النفسية وأمن العمليات. وهي نمط من

أنماط الحروب الحديثة كما أنها تعتبر شكل من أشكال الحروب التي تتسم بالسرعة ,المراوغة والمرونة بهدف تدمير المعلومات ونظم الاتصالات(.Espiner T ,2011) [٣٣].

التشهير الإلكتروني (Defamation)

وتعنى هذه الكلمة الافتراء أو إلصاق تهمة باطلة أو نشر بيان كاذب أو معلومات حقيقية ذات خصوصية، عن شخص أو بيئة ما. بهدف تحقيق أغراض نفعية متنوعة كتشويه سمعة المشهر به أو إلزامه الصمت نحو قضايا معينة أو مقايضته ماديا لكسب المال وهي جريمة ناتجة عن سوء نية، تمحق بالضحية ضرر سواء كان الضرر أدبي أو معنوي بالجهات أو بالأشخاص.

التنمر الإلكتروني (Bullying)

هو الاستخدام السيئ لتكنولوجيا الاتصالات والمعلومات الحديثة بغرض القيام بعمل التهديدات، المضايقات والإزعاجات والابتزازات، وغيرها من الصور التي تؤدى الى إيقاع الإيذاء والضرر بالمستخدمين.

أمثلة لأنواع التهديدات والجرائم السيبرانية

- الاعتداءات الشرسة على قواعد البيانات الخاصة أو العامة لأجهزة الحاسوب، وسائر الأجهزة
الإلكترونية وكذلك على الشبكات الرقمية وملحقاتها.

- الاعتداءات على المؤسسات الاقتصادية والمصرفية من خلال الهجوم على سرية البيانات والمعلومات والمعاملات والتداولات المالية سواء الرقمية أو غير الرقمية.

- القيام بعمل غسيل الأموال، والتهديدات والجرائم الإلكترونية عبر الوطنية، بالإضافة إلى القيام بالاستغلال غير المشروع للأطفال أو النساء والتعدي على حرمة الحياة الخاصة للأشخاص وكرامتهم من خلال جرائم مثل السب أو القذف والتشهير الإلكتروني وكذلك التصيد والتنمر الإلكتروني.

- ممارسة الإرهاب الإلكتروني عبر الفضاء السيبراني والذي يأخذ شكل جديد من أشكال الحروب الغير معلنة والغير مشروعة بين الدول وبعضها ويتمثل في القيام بعمليات تجريمية مثل التجسس والاختراق، والتهديدات والجرائم السيبرانية للنظم الدفاعية والبنية التحتية السيبرانية للدول. إضافة الى إتاحة الفرصة للقيام بعمل تشكيلات وتحالفات دولية يكون في مقدمتها الدول المتقدمة التي تقوم بعملية التصارع عبر الفضاء السيبراني الذي أصبح يمثل الساحة الميدانية للحروب السيبرانية.

- المصارعة عبر الفضاء السيبرانية والقيام بعمل تدخلات سواء مباشرة أو غير مباشر في الاستراتيجيات المتعلقة بالأمن السيبراني للعديد من الدول بهدف القيام باستحواذ على مصادر القوة عبر الفضاء السيبراني والقيام بالحيلولة دون تعرض بنيتها التحتية لأي خطر (محمد وائل القيسي ,2020) [٣٤].

مجالات الأمـــن السيبراني (Fields of Cyber Security)

لقد تعددت مجالات الأمن السيبراني وتطورت بشكل سريع وأصبحت منتشرة في الكثير من مناحي الحياة اليومية التي شهدت مساهمات كثيرة وغير مسبوقة في توفير الحماية غير العادية للبيانات وتأمين الشبكات بالأنظمة والبرامج الحديثة (سحر محمد صفا الله,٢٠١٩)[٣٥].

ومن أمثلة المجالات واسعة الانتشار التي تندرج تحت مظلة الأمن السيبراني:

١- أمن الشبكات (Network Security)

يتضمن ذلك حماية الشبكات المادية والسيرفرات (servers) وجميع الأجهزة المتصلة بها حيث يتم استخدام (firewall) لعمل monitoring لحركة المرور الواردة والصادرة وذلك للتصدي ومنع التهديدات، ويعد تأمين الشبكة اللاسلكية (Wireless Network) والتأكد من منع حدوث أي اتصالات عن بُعد غير مرغوب فيها بحيث تضمن بها خدمات الأمن السيبراني التحقيق والتيقن من أمان الشبكة من البيئة الخارجية. والسماح للمستخدمين المصرح لهم فقط إلى الشبكة وعدم التعرض لحدوث سلوكيات مشبوهة داخل الشبكة أو أي اختراقات.

٢- أمن التطبيق (Application Security)

يرتبط هذا النوع بتأمين التطبيقات الموجودة على الشبكة بهدف الحفاظ عليها من أي تهديدات من شأنها التركيز على تدمير تلك التطبيقات التي تمثل العمود الفقري للشبكة وخاصة الشركات التي تعمل على تطوير وبيع التطبيقات والخدمات السحابية الحديثة. ولكن بعض الأحيان التهيئة الخاطئة أثناء الإعدادات الأولية للأمان تكون سببًا أساسياً لحدوث اختراقات للبيانات والحسابات السحابية، في حين يتم استخدام خدمة سحابية كبيرة مثل Microsoft 365 كنوع من أنواع التأمين للتطبيقات الموجودة على الشبكة لكنها تحتاج لتخصيص إعدادات الأمان من خلال الإعدادات الافتراضية.

٣- أمن المعلومات (Information Security)

يختص هذا النوع من التأمين بأمن المعلومات وحماية بيانات الخاصة بالشركات إضافة الى البيانات التي يتم جمعها من العملاء وذلك من منطلق الحفاظ على خصوصية وسرية البيانات والامتثال للوائح والقوانين المنظمة للخصوصية، حيث أن الشركات لابد لها من الالتزام وتطبيق معايير أمن المعلومات، في حين ان الشركات التي تخل عن هذه المعايير تتعرض لعقوبات خاصة إذا كان الإهمال يؤدي إلى اختراق المعلومات التعريفية للأشخاص. لذا فإن الشركات التي تعمل في مجال الأمن السيبراني تعمل تامين جمع البيانات وتخزينها ونقلها، وتطبيق وسائل الحماية الكافية التي تضمن تشفير البيانات وحمايتها من التعرض للانتهاك.M .Black, 2018 (et) [٣٦].

٤- الأمن السحابي (Cloud Security)

يتميز العصر الحديث (الجيل الخامس) بما يسمى Cloud Computing (الحوسبة السحابية) تلك التقنيـــة التي أصبحت منتشرة وواسعة الاستخدام في مجالات شتى ومن أهم

تطبيقاتها Cloud Storage (التخزين السحابي) , ويلعب الأمن السحابي دور فعالاً في حماية البيانات المُخزنة من الاختراق أو الحذف أو التشوية , كما يقوم الأمن الحاسوبي بعمل الدعم وتوفير كل الحماية للمكونات والبيانات التي تدخل في عملية الحوسبة السحابية بما يضمن عدم الدخول إلى Cloud Computing.

٥- أمن العمليات (Operation Security)

يعد أمن العمليات Operation Security واحد من أهم أعمدة الامن السيبراني وهو جزء لا يتجزأ من الاستراتيجية الشاملة للأمن السيبراني. ويتضمن على جميع العمليات المختلفة التي من شأنها تعريف الخطوات والإجراءات التي ينبغي فعلها لصد العمليات العكسية التي تتم من قبل الأشخاص الذين يسعون للوصول إلى البيانات الحساسة بطرق غير مصرح بها.

٦- أمن المستخدم النهائي (End User Security)

و يقصد به أمان النقاط النهائية أو الطرفية (End Points) في النظام والمرتبطة بحماية الأجهزة المتصلة بالنظام ويتم استخدامها من قبل المستخدمين بطريقة مباشرة أنفسهم ويعد أمان المستخدم النهائي أمرًا في منتهى الأهمية والحيوية حيث أن معظم الهجمات الإلكترونية دائماً وأبداً تبدأ برسالة عبر بريد إلكتروني للتمكين من التصيد الاحتيالي. لذا يجب الاحتياط وزيادة التدريب بالوعي لأمن المستخدمين وتنمية المهارات لدى المستخدمين في التعامل واكتسابهم طرق اكتشاف رسائل البريد الإلكتروني المخادعة. هذا بخلاف حماية الأجهزة والتحقيق من أمن الكلمات المرورية المعقدة وحساسيتها.

٧- أمن إدارة الهوية والوصول (Identity Security & Access Management)

يمثل أمن إدارة الهوية والوصول Security & Access Management (ISAM) Identity واحد من أكثر المجالات أهمية التي يعنى بها الأمن السيبراني. وتشمل مجموعة القوانين والقواعد إضافة فضلاً عن الممارسات التي تتم على الشبكة وتضمن وصول الأشخاص المستخدمين المصرح لهم من خلال (System Administrator)الى المعلومات الصحيحة المطلوبة وذلك في الوقت المناسب والزمان المناسب وللأسباب الصحيحة.

٨. أمن إنترنت الأشياء (IOT Security)

لقد انتشرت تقنية إنترنت الأشياء بصورة واسعة في الفترة الأخيرة وتغلغلت في نواحي كثيرة من مجالات البيئة الرقمية التي تغطى جميع مجالات الحياة المعاصرة فهي تعد واحدة من أفضل التقنيـــات الواعدة للغاية التي تنمو بطريقة سريعة فقد نمت من ٢٣٥ مليار دولار في عام ٢٠١٧ إلى ٥٢٠ مليار دولار في عام ٢٠٢١. وهذه التقنية تعتمد على استخدام (Smarting Devices) وربطها بالإنترنت مثل الغسالة أو الثلاجة أو أي أجهزة منزلية أخرى. ويكون دور IOT Security التي تعد جزء من الامن السيبراني حماية البيانات وتأمين جميع الأجهزة المتصلة بالشبكة والقيام بصد أي هجمات أو انتهاكات على الشبكة تتم على الأجهزة المنزلية التي يتم التحكم بها من خلال من قبل إنترنت الأشياء IOT.

٩. أمن الأجهزة المحمولة (Mobile Security)

تعد الهواتف الذكية أكثر الوسائل أو الأجهزة التي تقع عرضة للهجمات السيبرانية، ويكون مستخدمها في خطر خاصة عند تنزيل التطبيقات جديدة وغير معروفة بموجب نظام تشغيل خاص بالهاتف، فضلًا عن مستقبلات وعدسات وأجهزة استشعار متعلقة به، وينطوي كل هاتف ذكي على عيوب محتملة تسمى أحيانًا أخطاء برمجية، بالإضافة إلى أخطاء من المستخدم ذاته حينما يفتح رابطا أو رسالة غير آمنة؛ مما يسمح للقراصنة بالسيطرة على الهاتف وإحداث خلل في أمن الهاتف وخصوصيته، ومن الممكن أن تجعل نظام التشغيل ينهار أو يتصرف على نحو غير متوقع عند استقبال رسالة تنطوي على خداع ما، أو ملفات تحتوي على برامج خبيثة. فقد أصبحت تلك الأجهزة مرصد ومطمع للهجمات والانتهاكات الإلكترونية من قبل الأشخاص ذوي الأغراض السيئة. وعند حدوث أي هجوم أو انتهاك تتأثر تلك الأجهزة وتتعطل جميع التطبيقات المرتبطة بها. لذا يلعب أمن الأجهزة المحمولة (Mobile Security) دوراً حيوياً في حماية وتأمين تلك الأجهزة وتعزيز الأمن الخاص بها. من خلال مجموعة من الممارسات والقواعد التي ينفذها عدد من المتخصصين.

نتائج الدراســـــة

جدول رقم (١) يوضح توزيع عينة الدراسة (الإعلاميين لدى المؤسسات الإعلامية) طبقاً للنوع

النوع	ك	%	المتوسط الحسابي	الانحراف المعياري
ذكر	٣١	٤٨,٤	١,٤٨	٠,٥٠٤
أنثى	٣٣	٥١,٦		

يتبين من الجدول رقم (١) أن نسبة الاناث لعينة الدراسة متقاربة الى حد ما مع نسبة الذكور فقد بلغت نسبة الذكور (٤٨,٤%) بعـــدد (٣١) مفردة من الإعلاميين العاملين بالمؤسسات الإعلامية المصرية, بينما بلغت نسبة الاناث (٥١,٦%) بعدد (٣٣) وهذا يوضح تجانس وتقارب وتوافق توزيع عينة الدراســـة من حيث النوع أو الجنس.

جدول رقم (٢): ميزان تقديري وفقاً لمقياس ليكرت الخماسى

الاستجـابة	المتوسط المترجح بالاوزان	طول الفترة	المستوى
أرفض بشدة	من ١ الى ١,٧٩	٠,٧٩	منخفض
أرفض	١,٨ الى ٢,٥٩	٠,٧٩	
محايد	٢,٦ الى ٣,٣٩	٠,٧٩	متوسط
أوافق	٣,٤ الى ٤,١٩	٠,٧٩	مرتفع
أوافق بشدة	٤,١٩ الى ٥	٠,٨٠	

يوضح الجدول رقم (٢) المتوسط المرجح لبيان نسبة الرفض والموافقة طبقاً لمقياس ليكرت الخماسى الذي يشمل على خمس درجـــات من التقييـــم (الرفض بشدة ,الرفض ,المحايدة ,الموافقة ,الموافقة بشدة) ونجد أن هذه الدرجات تنقسم الى مستويات متفاوتة منها المستوى المنخفض يتضمن (الرفض بشدة ,الرفض) والمستوى المرتفع يتضمن (الموافقة ,الموافقة بشدة) والمستوى المتوسط.

المحور الاول: مقياس الاعلام الرقمي في تعزيز الامن السيبراني (cyber security)

جدول رقم (٣): مقياس الاعــلام الرقمي في تعزيز الامن السيبراني (cyber security) طبقاً لمقياس ليكرت الخماسي.

م	المتغيرات		موافق بشدة	موافق	محايد	أرفض	أرفض بشدة	المتوسط الحسابي	الانحراف المعياري	الترتيب
١	ضرورة سن تشـريعات قوية لتحقيـق العمق الاستراتيجي للأمن السـيبراني في ظـل الإعـلام الرقمـي وعولمـة الرسـالة الإعلاميـة	ك	٢٠	١٧	٨	١١	٤	٣,٤٧	١,٤١٤	١٤
		%	٣١,٣	٢٦,٦	١٢,٥	١٧,٢	٦,٣			
٢	عرض وتحليل البيانات بطريقة أكثر جاذبية وتحفيزية نحو تقنيات الاعــلام الرقمي بالمؤسسات الإعلامية والمرتبطة بالأمن السيبراني	ك	١٧	٢٦	٩	٦	٦	٣,٦٦	١,٢٣٧	١١
		%	٢٦,٦	٤٠,٦	١٤	٩,٤	٩,٤			
٣	مسئولية الاعلام الرقمي مسئولية تضامنية ترعى المحتويات الإعلامية تحقيق الأمن المعلوماتي فهي ذات تفاعلية مباشرة مع المعنيين بالنواحي التقنية والأمنية	ك	٢٢	١٥	٩	١١	٧	٣,٥٣	١,٤٠٣	١٣
		%	٣٤,٤	٢٣,٤	١٤,١	١٧,٢	١٠,٩			
٤	الوعي بالتقنيات الحديثة للإعلام الرقمي والتقنيات المرتبطة بالأمن السيبراني تسهمان في تعزيز الامن السيبراني والقدرة على تحليل مخرجاتها	ك	١٨	٣٠	٧	٦	٣	٣,٨٤	١,٠٨٧	٥
		%	٢٨,١	٤٦,٨	١٠,٩	٩,٤	٤,٧			
٥	تصميمات الرسالة الإعلامية بالتقنيات الرقمية الحديثة ذات أولوية في تعزيز الوعي السيبراني اللازم لتحقيق الأمن السيبراني	ك	١٩	٢٥	٧	٧	٦	٣,٦	١,٣١٥	١٠
		%	٢٩,٧	٣٩,١	١٠,٩	١٠,٩	٩,٤			

٦	تقنيات الاعـــلام الرقمي ذات دور مؤثر وفعال في المشاركة في التحليل للحوادث السيبرانية والمساعدة في القضاء على العواقب السلبية لتلك للحوادث السيبرانية	ك	٢٣	٢٢	٥	١٠	٤	٣,٧٨	١,٢٦٦	٨
		%	٣٥,٩	٣٤,٤	٧,٨	١٥,٦	٦,٣			
٧	مساهمة تقنيـات الاعلام الرقمي الحديث في الحماية من التجسس الالكتروني ومنع التعرض لمخاطر الأمن السيبراني بالمؤسسات الإعلامية	ك	٢١	٢٨	٧	٣	٥	٣,٨٩	١,١٥٦	٤
		%	٣٢,٨	٤٣,٨	١٠,٩	٤,٧	٧,٨			
٨	دعم الاعـــلام الرقمي وتقنياته الحديثة الجهات الأمنية في تحقيق الامن السيبراني والاستقرار والسعي نحو البناء والتنمية المستدامة.	ك	٢٠	٢٧	١٢	٣	٢	٣,٩٤	٠,٩٩	٣
		%	٣١,٢	٤٢,٢	١٨,٨	٤,٧	٣,١			
٩	ضـرورة الربط والتنسـيق بيـن الجهات ذات الصلة بالإعـلام الرقمي والقائميـن الواقعيين بدعم وتحقيـق الأمـن السـيبراني	ك	٢٥	٢٦	٦	٤	٣	٤,٠٢	١,٠٨٢	١
		%	٣٩,١	٤٠,٦	٩,٤	٦,٣	٤,٧			
١٠	المساهمة الفعالة للإعلام الرقمي في اتخاذ القرارات الصائبة في شأن ممارسات الحوسبة على أسس قانونية وأخلاقية	ك	٢٠	٢٤	١١	٦	٣	٣,٦٣	١,٣٢٧	١٢
		%	٣١,٢	٣٧,٥	١٧,٢	٩,٤	٤,٧			
١١	المساهمة الفعالة في الإجراءات المضادة للمخاطر المرتبطة بالأمن السيبراني وتقييمات نقاط الضعف والقوة لنظم المعلومات وتحليل الهجمات الالكترونية واتخاذ الإجراءات المضادة المناسبة.	ك	٢٢	٢٧	٨	٤	٣	٣,٩٥	١,٠٧٥	٢
		%	٣٤,٤	٤٢,١	١٢,٥	٦,٣	٤,٧			

١٢	تحديد وتحليل الاحتياجات الملحة للمستخدمين وجعلها محل الاختيار والتكامل والتقييم المنتظم لإدارة النظم المبنية على الحاسب.	ك	٢٤	٢٤	٣	٦	٧	٣,٨٠	١,٣٣٢	٧
		%	٣٧,٥	٣٧,٥	٤,٧	٩,٤	١٠,٩			
١٣	الاستراتيجيات الاعلامية الحديثة ذات صياغة توافقية واتصالية مشتركة لتعزيز تحقيق الأمن السيبراني	ك	١٩	٢٧	٩	٥	٤	٣,٨١	١,١٣٩	٦
		%	٢٩,٧	٤٢,١	١٤	٧,٨	٦,٣			
١٤	منح قدرة التواصل الفعال مع كل المتابعين والمشتركين بشبكات النظم والمعلومات خاصة في المعلومات التقنية المرتبطة بالأمن السيبراني	ك	١٧	٣٠	٤	٨	٥	٣,٧٢	١,٢١٥	٩
		%	٢٦,٦	٤٦,٨	٦,٣	١٢,٥	٧,٨			
الوزن المرجح للمحور الاول									٣,٥٧٢	
الانحراف المعياري للمحور الاول									١,٢٣٤	
معامل الفا كرونباخ									٠,٩٣١٧	

يوضح الجدول رقم (٣) مقياس الاعلام الرقمي ودوره في تعزيز الامن السيبراني (cyber security) طبقاً لمقياس ليكرت الخماسي قد بلغت قيمة معامل الفا كرونباخ (٠,٩٣١٧) لقياس درجة ثبات وصدق فقرات هذا المحور من الاستبيان والتي تقيس الاتساق الداخلي بين فقرات محور مقياس الاعلام الرقمي ودوره في تعزيز الامن السيبراني (cyber security) وهذه القيمة تبين وتؤكد تجانس وترابط فقرات المحور بعضها مع بعض نحو الهدف الذي تم تصميم الاستبيان من أجله.

وبالنظر في الجدول السابق نجد أن فقرة " ضرورة الربط والتنسيق بين الجهات ذات الصلة بالإعلام الرقمي والقائمين بدعم وتحقيق الأمن السيبراني " جاءت في المرتبة الاولى في هذا المقياس كما تراها عينة الدراسة وقد بلغت قيمة المتوسط الحسابي (٤,٠٢) وقد بلغت قيمة الانحراف المعياري (١,٠٨٢) حيث أن أعلى نسبة من عينة الدراسة أبدت موافق بنسبة (٤٠,٦ %) بعدد (٢٦) مفردة بينما كانت نسبة موافق بشدة (٣٩,١ %) بعدد (٢٥) مفردة. وكانت نسبة المحايد من عينة الدراسة (٩,٤%) بعدد (٦) مفردة ونسبة الذين أبدو رأيهم الرفض (٦,٣%) بعدد (٤) مفردة ونسبة الذين أبدو الرفض بشدة (٤,٧%) بعدد (٣) مفردة.

وفي المرتبة الثانية جاءت فقرة " المساهمة الفعالة في الإجراءات المضادة للمخاطر المرتبطة بالأمن السيبراني وتقييمات نقاط الضعف والقوة لنظم المعلومات وتحليل الهجمات

الالكترونية واتخاذ الإجراءات المضادة المناسبة " فقد كانت نسبة موافـــــق (٤٢,١%) بعدد (٢٧) مفردة وكانت نسبة موافـــق بشدة (٣٤,٤%) بعدد (٢٢) مفردة بينما كانت نسبة المحايد (١٢,٥%) بعدد (٨) مفردة وكانت نسبة الذين أبدو بالرفض (٦,٣%) بعدد (٤) مفردة ونسبة بالرفض بشدة (٤,٧) بعدد (٣) مفردة فى حين بلغت قيمة المتوسط لهذه المتغير (٣,٧٠) و قيمة الانحراف المعياري (١,٢٩١).

ثم جاءت في المرتبة الثالثة فقرة " دعم الاعـــلام الرقمي وتقنياته الحديثة الجهات الأمنية في تحقيق الامن السيبراني والاستقرار والسعي نحو البناء والتنمية المستدامة" حيث بلغت قيمة المتوسط الحسابي (**٣,٩٤**) و قيمة الانحراف المعياري (٠,٩٩) وكانت نسبة الاكبر للفئة التي أفادت موافق بشدة (٣١,٢ %) بعدد (٢٠) مفردة من عينة الدراسة وكانت نسبة موافق (٤٢,٢%) من عينة الدراسة بعدد (٢٧) مفردة , وكانت نسبة المحايد من عينة الدراسة (١٨,٨%) بعدد (١٢) مفردة و نسبة الذين أبدو بالرفض (٤,٧%) بعدد (٣) مفردة و نسبة الذين أبدو بالرفض بشدة (٣,١%) بعدد (٢) مفردة.

ثم جاءت في المرتبة الرابعة فقرة " مساهمة تقنيـات الاعلام الرقمي الحديث في الحماية من التجسس الالكتروني ومنع التعرض لمخاطر الأمن السيبراني بالمؤسسات الإعلامية "حيث بلغت نسبة موافق (٤٣,٨ %) بعدد (٢٨) مفردة وكانت نسبة موافق بشدة (٣٢,٨ %) بعدد (٢١) مفردة , بينما كانت نسبة المحايد (١٠,٩ %) بعدد (٧) مفردة ونسبة الرفض (٤,٧%) بعدد (٣) مفردة , ونسبة الرفض بشدة (٧,٨%) بعدد (٥) مفردة , في حين بلغت قيمة المتوسط لهذا المتغير (٣,٨٩) وقيمة الانحراف المعياري (١,١٥٦).

ثم جاءت فقرة " الوعي بالتقنيات الحديثة للإعلام الرقمي والتقنيات المرتبطة بالأمن السيبراني تسهمان في تعزيز الامن السيبراني والقدرة على تحليل مخرجاتها " في المرتبة الخامسة وكانت نسبة موافق بشدة (٢٨,١ %) بعدد (١٨) مفردة وكانت نسبة موافق (٤٦,٨ %) بعدد (٣٠) مفردة , بينما كانت نسبة المحايد (١٠,٩ %) بعدد (٧) مفردة ونسبة الرفض (٩,٤%) بعدد (٦) مفردة , ونسبة الرفض بشدة (٤,٧%) بعدد (٣) مفردة , في حين بلغت قيمة المتوسط لهذه المتغير (٣,٨٤) و قيمة الانحراف المعياري (1.087).

وفى المرتبة السادسة جاءت فقرة " الاسـتراتيجيات الاعلاميـة الحديثة ذات صياغة توافقية واتصاليـة مشـتركة لتعزيـز تحقيـق الأمـن السـيبراني" حيث كانت نسبة موافق بشدة (29.7 %) بعدد (19) مفردة وكانت نسبة موافق (42.1 %) بعدد (27) مفردة , بينما كانت نسبة المحايد (14 %) بعدد (9) مفردة ونسبة الرفض (7.8%) بعدد (5) مفردة , ونسبة الرفض بشدة (٢,٥%) بعدد (١) مفردة , في حين بلغت قيمة المتوسط لهذه المتغير (3.81) و قيمة الانحراف المعياري (1.139).

وفى المرتبة السابعة جاءت فقرة " تحديد وتحليل الاحتياجات الملحة للمستخدمين وجعلها محل الاختيار والتكامل والتقييم المنتظم لإدارة النظم المبنية على الحاسب" حيث كانت نسبة موافق بشدة (٣٧,٥ %) بعدد (٢٤) مفردة وكذلك كانت نسبة موافق (٣٧,٥ %) بعدد (٢٤) مفردة , بينما كانت نسبة المحايد (٤,٧ %) بعدد (٣) مفردة ونسبة الرفض (٩,٤%) بعدد

(٧) مفردة , ونسبة الرفض بشدة (١٠,٩%) بعدد (٧) مفردة , في حين بلغت قيمة المتوسط لهذه المتغير (٣,٨٠) وقيمة الانحراف المعياري (١,٣٣٢).

ثم جاءت فقرة " مسئولية الاعلام الرقمي مسئولية تضامنية ترعى المحتويات الإعلامية تحقيق الأمن المعلوماتي فهي ذات تفاعلية مباشرة مع المعنيين بالنواحي التقنية والأمنية " في المرتبة قبل الاخيرة, حيث بلغت قيمة المتوسط الحسابي (٣,٥٣) و قيمة الانحراف المعياري (١,٤٠٣) وكانت النسبة الاعلى لمن أبدو بالموافقة (٢٣,٤ %) بعدد (١٥) مفردة من عينة الدراسة وكانت نسبة موافق بشدة (٣٤,٤%) من عينة الدراسة بعدد (٢٢) مفردة , وكانت نسبة المحايد من عينة الدراسة (٢٢,٥%) بعدد (٩) مفردة و نسبة الذين أبدو بالرفض (17.2%) بعدد (11) مفردة و نسبة الذين أبدو الرفض بشدة (10.9%) بعدد (7) مفردة.

ثم جاءت فقرة " ضرورة سن تشريعات قوية لتحقيق العمق الاستراتيجي للأمن السيبراني في ظل الإعلام الرقمي وعولمة الرسالة الإعلامية "في المرتبة الاخيرة حيث بلغت قيمة المتوسط الحسابي (٣,٤٧) وقيمة الانحراف المعياري (١,٤١٤) وكانت نسبة الموافقة (٢٦,٦ %) بعدد (١٧) مفردة من عينة الدراسة وكانت نسبة الموافقة بشدة (٣١,٣%) من عينة الدراسة بعدد (٢٠) مفردة , وكانت نسبة المحايد من عينة الدراسة (١٢,٥%) بعدد (٨) مفردة ونسبة الرفض (١٧,٢%) بعدد (١١) مفردة ونسبة الرفض بشدة (٦,٣%) بعدد (٤) مفردة.

مما سبق يتضح ان نتائج مقياس الاعلام الرقمي ودوره في تعزيز الامن السيبراني (cyber security) طبقاً لمقياس ليكرت الخماسي. جاءت بالموافقة بدرجة مرتفعة حيث بلغت قيمة الوزن المرجح لهذا المحور (٣,٥٧٢) وذلك وفقاً للميزان التقديري لمقياس ليكرت الخماسي بالجدول رقم (٣). كما بلغت قيمة الانحراف المعياري (١,٢٣٤).

المحور الثاني: مقياس الاعلام الرقمي في مكافحة التهديدات والجرائم السيبرانية.

جدول رقم (٤): الاعلام الرقمي في مكافحة التهديدات والجرائم السيبرانية من وجهة نظر عينة الدراسة طبقاً لمقياس ليكرت الخماسي.

م	المتغيرات		موافق بشدة	موافق	محايد	أرفض	أرفض بشدة	المتوسط الحسابي	الانحراف المعياري	الترتيب
١	يقوم الاعلام الرقمي بالتزويد الفعلي والتعريف بالقواعد والمعايير والتشريعات المتعلقة الأمن السيبراني	ك	٢٤	٢٢	٦	٧	٥	٣,٨١	١,٢٦٦	٦
		%	٣٧,٥	٣٤,٤	٩,٤	١٠,٩	٧,٨			
٢	يلعب الاعلام الرقمي دوراً حيوياً في الوصول للمجرمين المرتكبين للجرائم والهجمات السيبرانية	ك	٢٠	٢٤	٩	٨	٣	٣,٧٧	١,١٦٠	٧
		%	٣١,٣	٣٧,٥	١٤	١٢,٥	٤,٧			

٣	قيام الاعلام الرقمي بتدعيم وزيادة الاعتماد على وسائل وأنظمة الحماية الأمنية المتعلقة بالأمن السيبراني واستراتيجياته	ك	١٦	٢٢	٨	١٠	٨	٣,٤٢	١,٣٥٣	١٢
		%	٢٥	٣٤,٤	١٢,٥	١٥,٦	١٢,٥			
٤	مساعدة الاعلام الرقمي في اكتشاف التهديدات والجرائم السيبرانية وتحديد نوعية التهديدات والجرائم السيبرانية	ك	٢١	٢١	٧	١١	٤	٣,٦٨	١,٢٧٠	١٠
		%	٣٢,٨	٣٢,٨	١٠,٩	١٧,٢	٦,٣			
٥	الاعلام الرقمي يساهم بطريقة مباشرة في معالجة القصور التشريعي وردع وتجريم ارتكاب التهديدات والجرائم السيبرانية	ك	٢٢	٢٠	٩	٧	٦	٣,٦٩	١,٣٠٢	٩
		%	٣٤,٤	٣١,٣	١٤	١٠,٩	٩,٤			
٦	قيام الاعلام الرقمي بتقديم المعلومات الضرورية وعمل الاستعدادات اللازمة لتحقيق الوقاية قبل وقوع أي خطوات في التهديدات والجرائم السيبرانية	ك	٢٠	٢٩	٨	٤	٣	٣,٩١	١,٠٥٦	٢
		%	٣١,٣	٤٥,٣	١٢,٥	٦,٣	٤,٧			
٧	مساعدة الاعلام الرقمي في زيادة فرص وقدرات الأمن السيبراني وتقديم المساندة الحقيقية لفرق الطوارئ للتمكين في مواجهة التهديدات والجرائم السيبرانية	ك	٢٣	٢٣	٨	٨	٢	٣,٨٧	١,١٢٨	٤
		%	٣٥,٩	٣٥,٩	١٢,٥	١٢,٥	٣,١			
٨	الاعلام الرقمي يسهم بطريقة مباشرة في زيادة الانتماء الوطني وتحسين قدرات الوسائل الأمنية المستخدمة لحماية البنية التحتية للأمن السيبراني	ك	١٨	٢٢	١١	٩	٤	٣,٦٣	١,٢١٢	١١
		%	٢٨,١	٣٤,٤	١٧,٢	١٤	٦,٣			

٩	المساهمه الفعاله للإعلام الرقمي في نشر ثقافة الوعي الفكري والاجتماعي بالمخاطر الناجمة عن ارتكاب التهديدات والجرائم السيبرانية.	ك	٢٣	٣٠	٤	٥	٢	٤,٠٣	١,٠١٦	١
		%	٣٥,٩	٤٦,٩	٦,٣	٧,٨	٣,١			
١٠	العمل على رفع نسب التوعية بمخاطر التهديدات والجرائم السيبرانية من خلال برامج وانشطة نوعية عبر الوسائل الإعلامية الرقمية المتنوعة	ك	٢٠	٣٠	٤	٨	٢	٣,٩٠	١,٠٨١	٣
		%	٣١,٣	٤٦,٩	٦,٣	١٢,٥	٣,١			
١١	العمل على زيادة الخبرة والتاهيل والتدريب لدى العناصر المشتركة في مكافحة التهديدات والجرائم السيبرانية وكيفية التعامل مع الأنماط الجديدة للجرائم السيبرانية	ك	٢٠	٢٦	٤	٩	٥	٣,٧٢	١,٢٦٢	٨
		%	٣١,٣	٤٠,٦	٦,٣	١٤	٧,٨			
١٢	مساهمة الاعلام الرقمي في رصد ومتابعة وتحليل أحدث الأساليب المستخدمة في التهديدات والجرائم السيبرانية والتوعية بها	ك	٢١	٢٧	٥	٧	٤	٣,٨٣	١,١٨٢	٥
		%	٣٢,٨	٤٢,٢	٧,٨	١٠,٩	٦,٣			
الوزن المرجح للمحور الثاني									٣,٧٦٣٤	
الانحراف المعياري للمحور الثاني									١,١٣٥٩٦	
معامل الفا كرونباخ									٠,٩٣٥٢	

الجدول رقم (٤) يوضح مقياس الاعــلام الرقمي ودوره في مكافحة التهديدات والجرائم السيبرانية من وجهة نظر عينة الدراسة طبقاً لمقياس ليكرت الخماسى. وقد بلغت قيمة معامل الفا كرونباخ (٠,٩٣٥٢) لقياس درجة ثبات وصدق فقرات هذا المحور من الاستبيان والتي تقيس الاتساق الداخلي بين فقرات محور مقياس الاعــلام الرقمي ودوره في مكافحة التهديدات والجرائم السيبرانية وهذه القيمة التي تؤكد الترابط والتجانس بين فقرات المحور بعضها البعض نحو الهدف الذي تم تصميم الاستبيان من أجله. وبالرجوع الى الجدول السابق نجد أن فقرة " المساهمة الفعالة للإعلام الرقمي في نشر ثقافة الوعي الفكري والاجتماعي بالمخاطر الناجمة عن ارتكاب التهديدات والجرائم السيبرانية " جاءت في المرتبة الاولى كما تراها عينة الدراسة وقد بلغت قيمة المتوسط الحسابي لهذه الفقرة (٤,٠٣) وقد بلغت قيمة

الانحراف المعياري (١,٠١٦) حيث أن أعلى نسبة من عينة الدراسة أبدت رأى موافق بنسبة (46.9%) بعدد (30) مفردة بينما كانت نسبة موافق بشدة (٣٥,٩ %) بعدد (23) مفردة. وكانت نسبة المحايد من عينة الدراسة (6.3%) بعدد (4) مفردة ونسبة الذين أبدو الرفض (7.8%) بعدد (5) مفردة ونسبة الذين أبدو الرفض بشدة (٣,١%) بعدد (٢) مفردة.

وقد جاءت في المرتبة الثانية فقرة " قيام الاعلام الرقمي بتقديم المعلومات الضرورية وعمل الاستعدادات اللازمة لتحقيق الوقاية قبل وقوع أي خطوات في التهديدات والجرائم السيبرانية " حيث بلغت قيمة المتوسط الحسابي (٣,٩١) و قيمة الانحراف المعياري (١,٠٥٦) وكانت نسبة الاكبر للفئة التي أفادت موافق بنسبة (٤٥,٣%) بعدد (٢٩) مفردة من عينة الدراسة وكانت نسبة موافق بشدة (٣١,٣ %) بعدد (٢٠) مفردة من عينة الدراسة بينما كانت نسبة المحايد من عينة الدراسة (١٢,٥%) بعدد (٨) مفردة و نسبة الذين أبدو بالرفض (٦,٣%) بعدد (٤) مفردة و نسبة الذين أبدو بالرفض بشدة (٦,٣%) بعدد (٣) مفردة.

ثم جاءت فقرة "العمل على رفع نسب التوعية بمخاطر التهديدات والجرائم السيبرانية من خلال برامج وأنشطة نوعية عبر الوسائل الإعلامية الرقمية المتنوعة " في المرتبة الثالثة فقد كانت نسبة موافق (٣١,٣%) بعدد (٢٠) مفردة وكانت نسبة موافق بشدة (46.9%) بعدد (30) مفردة بينما كانت نسبة المحايد (٦,٣%) بعدد (٤) مفردة وكانت نسبة الذين أبدو بالرفض (١٢,٥%) بعدد (٨) مفردة ونسبة بالرفض بشدة (٣,١%) بعدد (٢) مفردة في حين بلغت قيمة المتوسط لهذه المتغير (٣,٩٠) وقيمة الانحراف المعياري (١,٠٨١).

ثم جاءت فقرة " مساعدة الاعلام الرقمي في زيادة فرص وقدرات الأمن السيبراني وتقديم المساندة الحقيقية لفرق الطوارئ للتمكين في مواجهة التهديدات والجرائم السيبرانية " في المرتبة الرابعة فقد بلغت تساوت نسبة الفئة الموافق مع فئة الموافق بشدة وكلا بلغت نسبته (٣٥,٩ %) بعدد (٢٣) مفردة, بينما تساوت نسبة الفئة المحايدة مع الفئة الرافضة وكلا منهم (١٢,٥ %) بعدد (٨) مفردة, ونسبة الرفض بشدة (٣,١%) بعدد (٢) مفردة , في حين بلغت قيمة المتوسط لهذا المتغير (٣,٨٧) وقيمة الانحراف المعياري (١,١٢٨).

ثم جاءت فقرة " مساهمة الاعلام الرقمي في رصد ومتابعة وتحليل أحدث الأساليب المستخدمة في التهديدات والجرائم السيبرانية والتوعية بها " في المرتبة الخامسة فقد كانت نسبة موافق (٣٢,٨%) بعدد (٢١) مفردة وكانت نسبة موافق بشدة (٤٢,٢%) بعدد (٢٧) مفردة بينما كانت نسبة المحايد (٧,٨%) بعدد (٥) مفردة وكانت نسبة الذين أبدو بالرفض (١٠,٩%) بعدد (٧) مفردة ونسبة بالرفض بشدة (٦,٣%) بعدد (٤) مفردة في حين بلغت قيمة المتوسط لهذه المتغير (٣,٨٧) وقيمة الانحراف المعياري (١,١٨٢).

وقد جاءت فقرة " الاعلام الرقمي يسهم بطريقة مباشرة في زيادة الانتماء الوطني وتحسين قدرات الوسائل الأمنية المستخدمة لحماية البنية التحتية للأمن السيبراني " في المرتبة قبل الاخيرة, حيث بلغت قيمة المتوسط الحسابي (٣,٦٣) و قيمة الانحراف المعياري (١,٢١٢) وكانت النسبة الاعلى لمن أبدو بالموافقة (٣٤,٤ %) بعدد (٢٢) مفردة من عينة الدراسة وكانت نسبة موافق بشدة (٢٨,١%) من عينة الدراسة بعدد (١٨) مفردة , وكانت نسبة

المحايد من عينة الدراسة (١٧,٢%) بعدد (١١) مفردة و نسبة الذين أبدو بالرفض (١٤%) بعدد (٩) مفردة و نسبة الذين أبدو الرفض بشدة (٦,٣%) بعدد (٤) مفردة.

ثم جاء في المرتبة الاخيرة فقرة " قيام الاعلام الرقمي بتدعيم وزيادة الاعتماد على وسائل وأنظمة الحماية الأمنية المتعلقة بالأمن السيبراني واستراتيجياته " حيث بلغت قيمة المتوسط الحسابي (٣,٤٢) وقيمة الانحراف المعياري (١,٣٥٣) وكانت نسبة الموافقة بشدة (٢٥ %) بعدد (١٦) مفردة من عينة الدراسة وكانت نسبة الموافقة (٣٤,٤ %) بعدد (٢٢) مفردة, وكانت نسبة المحايد من عينة الدراسة (١٢,٥%) بعدد (٨) مفردة ونسبة الرفض (١٥,٦%) بعدد (١٠) مفردة ونسبة الرفض بشدة (١٢,٥%) بعدد (٨) مفردة.

مما سبق يتضح أن دور الاعــلام الرقمي في مكافحة التهديدات والجرائم السيبرانية من وجهة نظر عينة الدراسة طبقاً لمقياس ليكرت الخماسي متنوع وله أثر بالغ وأكدت النتائج على ذلك من خلال الجدول السابق حيث يوضح مقياس ليكرت الخماسى لقياس مقياس الاعــلام الرقمي ودوره في مكافحة التهديدات والجرائم السيبرانية. فقد أسفرت النتائج التي عبرت عن عينة الدراسة وقد جاءت الموافقة بدرجة مرتفعة من وجهة نظر عينة الدراسة المتمثلة في الإعلاميين وبلغت قيمة الوزن المرجح لهذا المحور (٣,٧٦٣٤) وذلك وفقاً للميزان التقديرى لمقياس ليكرت الخماسى بالجدول رقم (٤). وقيمة الانحراف المعياري (١,١٣٥٩٦).

مما تم عرضه من النتائج السابقة يتضح أن العلاقة بين الأمن السيبراني والمحتوى المعلوماتي علاقة قوية فكلما زاد المحتوى المعلوماتي والعسكري والأمني والفكري والسياسي والاجتماعي والاقتصادي والخدمي والعلمي زادت أهمية الأمن السيبراني الذي أصبح من الضروريات الأساسية التي لا غنى عنها وأن الإعلام الرقمي يلعب دور رأس الحربة في تدعيم وتعزيز الأمن السيبراني ومقاومة التهديدات والجرائم والتهديدات والجرائم السيبرانية.

ويمكن تلخيص الدور الذي يقوم الاعلام الرقمي في تدعيم الأمن السيبراني والحد من التهديدات والجرائم السيبرانية في ضوء نتائج الدراسة في النقاط التالية:

- ❖مساهمة الاعلام الرقمي الفعالة في القيام بتحقيق الأهداف المنشودة للأمن السيبراني بأبعاده المختلفة والتي شملت (البعد الاقتصادي والاجتماعي والسياسي والقانوني) فقد أصبحت الدول والمجموعات الافتراضية تعنى اعتناء شديد بهذه الابعاد والاهتمام الفائق بالفضاء السيبراني للتحكم والسيطرة في الوقاية المبكرة للجرائم السيبرانية و يتوافق ذلك مع دراسة كل من (Nyinkeu et. , ٢٠١٨) , (William Crumpler et. 2019) , (موسى بن تغري, ٢٠٢٠) , (Moskal, ٢٠٢٠).
- ❖ المشاركة ذات الفاعلية الكبيرة للإعلام الرقمي في رفع قدرات الأمن السيبراني وكذلك تشجيع وتدعيم فرق الطوارئ المؤهلة في مواجهة الهجمات والتهديدات والجرائم السيبرانية ويتماشى ذلك مع دراسة (Jemin Justin Lee et., ٢٠٢٠) , (Bustard, ٢٠١٨).

- المساهمة الإيجابية المباشرة للإعلام الرقمي في العمل على تشجيع الدول نحو التحول الرقمي وتطبيق الرقمنة لدى جميع المؤسسات والهيئات والحكومات الشركات وإلزامهم بذلك.
- القيام بالمساعدة المباشرة للإعلام الرقمي في التنمية ونشر ثقافة الوعي الاجتماعي بالتهديدات والجرائم والمخاطر والتهديدات والجرائم السيبرانية والعمل على دعم وتوفير الحماية اللازمة على مستويات الأفراد والحكومات والهيئات.
- فعالية الاعلام الرقمي نحو تدعيم وحماية البنية التحتية المعلوماتية (السيبرانية) و الأمنية للقطاع العام أو الخاص على حد سواء وكذلك الدعم الكامل للإعلام الرقمي وبناء كوادر متميزة و متخصصة في مجال الامن المعلوماتي (السيبراني) من كافة فئات المجتمعات، والعمل على تعزيز المشاركة المجتمعية والشعبية، بالإضافة إلى تكوين فرق تحليل لبيانات شبكات التواصل الاجتماعي للاستباق و التنبؤ بالهجمات المستقبلية واستخدامات تقنيات الذكاء الاصطناعي لتحديد ومعالجة تلك الثغرات وتصور السيناريوهات المحتملة لمكافحة الهجمات السيبرانية (Da Veiga, A. ,٢٠١٩)[٣٧].
- المشاركة الفعالة للإعلام الرقمي في وضع ونقل الرؤية المستقبلية لصناع القرار في القيام بتأسيس أنظمة تقنية حديثة متضمنة وسائل وأنظمة الحماية الأمنية والوطنية. وكذلك العمل على سن تشريعات وقوانين تكون رادعة لمرتكبي التهديدات والجرائم السيبرانية. ويتفق هذا مع دراسة (أسماء أحمد أبو زيد علام, 2021) ودراسة (Roden Judah A. ,٢٠١٩).
- مشاركة الاعلام الرقمي في النهوض والقيام بالمبادرات الإيجابية للشروع في عمل البرامج التنشيطية والتثقيفية والانشطة النوعية المتنوعة لضمان تنفيذ استراتيجيات تضمن الحفاظ وتطوير قدرات الأمن السيبراني والوقوف على منع التهديدات والجرائم السيبرانية مثل التنمر الإلكتروني و التشهير الإلكتروني أو غيرها ويتفق ذلك مع دراسة (Luurs, G. , ٢٠١٨)[٣٨].
- التوجيه والإرشاد والتوعية الذي يقوم به الاعلام الرقمي للفئات المجتمعية المختلفة نحو إعداد وتدريب كوادر ذات خلفية قوية علمية وعملية بالأمن السيبراني بحيث تصبح قادرة على رصد وتحليل ومتابعة الأساليب المتنوعة التي يتم استخدامها في ممارسة الهجمات والتهديدات والجرائم السيبرانية. على أن تمثل هذه الكوادر فرق دفاعية ذات فاعلية تقوم بمكافحة التهديدات والجرائم السيبرانية بعد التحقيق منها. ويتوافق ذلك مع دراسة (تغريد حمد الرفاعي, ٢٠١٨) ودراسة (عادل عبد الصادق , ٢٠٢٢).

التوصيـــــات

- ضرورة وضـــع اســـتراتيجية متكاملـــة لمكافحـــة التهديدات والجرائم السيبرانية وذلك مـــن زوايـــا مختلفـة يمكن تطبيقها علـى كافـة المستويات لحمايـة الافراد والمجتمـعات مـن الشـائعات والأخبـار المضللـة التي تتسبب في انتشـار التهديدات والجرائم السيبرانية وتنـوعها سواء على الناحية الاجتماعية والسياسـية والامنيـة والاقتصاديـة.
- القيام بتوفير بيئة مناسبة ذات فاعلية وذات مرونة وقادرة على مواكبة التغيرات السريعة. وتعنى بإنشاء الآليـات اللازمة في النواحي المتنوعة (القانونيـة والأمنيـة والتقنيـة والإعلامية والتعليميـة) للحـد مـن مخاطـر التهديدات والجرائم السيبرانية وانتشـارها والمحـــافظة علـــى الأمـــن السـيبراني.
- القيام باتخاذ كافة الإجراءات الاحترازية اللازمة للحماية والتحصين ضد التهديدات والجرائم أو الهجمات أو التخريبات السيبرانية والقيام بالتحديثات المستمرة للتقنيات والبرامج المضادة للاعتداءات والفيروسات الخبيثة، بخلاف اعتماد وتحديث الوسائل التقنية المستخدمة والخاصة بالتشفير الرقمي , البصمة الرقمية، والتصديق الرقمي، تحديث برنامج جدار النار (Firefox)، وتحديث التقنيات الاخرى...الخ.
- العمل على تأهيل كوادر أو عناصر بشرية مدربة تكون متخصصة في الأمن السيبراني ومتعمقة في مجال الفضاء السيبراني وتكون حائط صد لأي محاولات تهديدية لأمن النبوك العامة أو الخاصة كما تكون داعم أساسي لأمن الخدمات البنكية الإلكترونية. فضلاً عن قدرتها على التحكم في مختلف التقنيات المجودة (البرمجيات، الأجهزة الإلكترونية، نظم التشغيل الشبكات، الإنترنت،...الخ).
- ضرورة تطبيق معايير الجودة الدولية (ISO) international standardization organization في العمل بالأنظمة المعلوماتية أو السيبرانية وشبكات الاتصال ذات المواصفات القياسية وذلك لضمان تحقيق سلامة أمن المعلومات والبيانات وحمايتها وأمن الشبكات من الاختراقات المحتملة. إضافة الى استخدام الأنظمة التشغيلية ذات المصادر المفتوحة (open source software) مثل أنظمة تشغيل الـLinux والـUnix التي تتميز بالقوة والمرونة والاستقرار وقوة التأمين المحكمة.
- قيام الكوادر أو العناصر بشرية المدربة باتخاذ كافة الإجراءات الاحترازية اللازمة للحماية ضد العمليات المتنوعة الاحتيال والنصب المالي والمصرفي الإلكتروني وبعمليات التعدي والتجسس والتخريب والتدمير وكل ما يتعلق بالتعاملات الإلكترونية ببطاقات الدفع الإلكترونية المصرفية.
- المشاركة الفعالة لجميع المؤسسات والهيئات ووقوفها جنباً الى جنب وباشتراك منظمات المجتمـع المـدني لعمل برامـج وأنشطة وحملات توعيـة وتثقيفية لجميع المستخدمين لديها نحو أهمية الأمن السيبراني وكيفية الالتزام بتعليماته والتوجيه للالتزام بالإرشادات الضرورية لمواجهـة ما يتوقع من المخاطـر والتهديدات والجرائم السـيبرانية.

- القيام بإنشاء مواقع الكترونية وصفحات على الانترنت متخصصة تكون تحت سيطرة الجهات المختصة تهدف للقيام بنشر ثقافة وتوعية نحو تعزيز الأمن السيبراني.
- ضرورة قيام المستخدمين بفهم المبادئ والأساسيات لأمان البيانات والمعلومات وتنفيذ خطوات الأمان وفي مقدمتها اختيار كلمات مرور قوية تشتمل على (حروف وأرقام وعلامات)والحذر من الاعجاب أو المتابعة للمرفقات الموجودة أو المصحابة للبريد الإلكتروني أو النسخ الاحتياطي للبيانات.
- ضرورة قيام المسؤولين وصناع القرار بالمشاركة الفعالة في صياغة و متابعة المستجدات و المستحدثات سواء في القوانين والتشريعات الخاصة بالأمن السيبراني لاسيما ما تختص بحماية التعاملات الإلكترونية , البنكية , البيانات الشخصية و الحسابات الخاصة أو غيرها.

المراجـــــع:

١-طالـة وكهينـة، لاميـة سـلام. (٢٠٢٠) الجريمـة الإلكترونيـة بعد جديد لمفهوم الإجرام عبر منصـات التواصـل الاجتماعي، مجلــة الـرواق للدراسات الاجتماعية والإنســانية، مج(٦) ,ع (٤).

٢-فرحات، علاء الدين. (٢٠١٩), الفضاء السيبراني تشكيل ساحة المعركة في القرن الحادي والعشرين، مجلة العلوم القانونية والسياسية، مج(١٠). ع(٣).

٣-هيام محمد الهادي.(٢٠٢٠) تعرض المراهقين للجرائم الإلكترونية عبر وسائل الإعلام الرقمي وتأثيرها على إدراكهم للأمن الاجتماعي المصري، المجلة العربية لبحوث الإعلام والاتصال، ع(٢).

٤-اية عمر فرج.(٢٠٢٢), دواعي تعزيز ثقافة الأمن السيبراني في ظل التحول الرقمي – جامعة الأمير سطام بن عبد العزيز نموذجاً , مجلة جامعة سوهاج الدولية التربوية.

٥-أسماء أحمد أبو زيد علام، (٢٠٢١) ,استراتيجيات خطاب صحافة التكنولوجيا العربية تجاه الأمن السيبراني، المجلة المصرية لبحوث الرأي العام، مج (٢٠) , ع (٢).

٦- منال حسن محمد إبراهيم. (٢٠٢١) ,الوعي بجوانب الأمن السيبراني في التعليم عن بعد , المجلة العلمية لجامعة الملك فيصل - العلوم الإنسانية والإدارية , مج(٢٢), ع(٢) , ص ص ٢٩٩-٣٠٥.

7-Ameen, A., Tarhini, B., Shah, M., Madichie, D., Paul, J. and Choudrie, J. (2021).Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce. Computers in Human Behavior, 114(n/a), doi.org/10.1016/j.chb.2020.106531 .

8-Moskal. E (2020), A Model of Establishing Cyber Security Center of Excellence. Information Systems Education Journal, Vol. (13), No. (6), PP 97-102.

9-Nyinkeu, N., Anye, D., Kwededu, L. & Buttler, W. (2018). Cyber education outside the cyber space: the case of catholic university institute of Buea. International journal of technology in teaching and learning. Vol. (14), No. (2), PP: 90-98.

10-Bustard, J. (2018). Improving student engagement in the study of professional ethics: concepts and an example in cyber security. Scientific engineer ethics. No. (24), pp: 683-692.

١١-عادل عبد الصادق. (٢٠٢٢) , الإرهاب السيبراني والأمن القومي في بيئة متغيرة , مؤسسة الاهرام , مجلة السياسة الدولية , مج (٥٧),ع (٢٢٧) , ص ص ٢٤٤-٢٤٧.

١٢-موسى بن تغري. (٢٠٢٠) , الحرب السيبرانية والقانون الدولي الإنساني , مجلة الاجتهاد القضائي , مج (١٢),ع (٢) , ص ص ١٩٩-٢٠٧.

١٣-مالك بن فهد الغبيوي، (٢٠٢٠) الأمن السيبراني ودوره في الحد من تهديدات الأمن الفكري، رسالة ماجستير، قسم الدراسات الاستراتيجية، جامعة نايف العربية للعلوم الأمنية.

14- Jemin Justin Lee , Myong-Hyun Go , Yu-Kyung Kim , Minhee Joo. (٢٠٢٠) , A Multi-Component Analysis of CPTED in the Cyberspace Domain , Free PMC article , Vol. (20),No.(14) , DOI: 10.3390/s20143968

15-Roden Judah A. (2019) Video Game Industry Analysis: History, Growth, and Architecture, Master Thesis, Lamar University, The Faculty of the College of Graduate Studies.

16-William Crumpler & James A. Lewis (2019), The Cybersecurity Workforce Gap, the Center for Strategic and International Studies (CSIS).

١٧-حسن محمدحسن، (٢٠١٨) مخاطر استخدام الفضاء السيبراني في الحياة الاجتماعية والثقافية والأسرية دون حماية وآثارها .المؤتمر السابع لأمن وسلامة الفضاء السيبراني (الإنترنت) في الدول العربية .بيروت ص ص: ٢٥-٢٣.

١٨-تغريد حمد الرفاعي، (٢٠١٨) درجة ممارسة وتعرض طلبة المرحلة المتوسطة في مدارس دولة الكويت للتنمر الإلكتروني وأثر متغير الجنس .مجلة العلوم التربوية. جامعة الكويت. ع (٤) ,ص ص ١٣٢-١١١.

19-Ion Goran (2017), Cyber Security Risks in Public High Schools, Master of Science in Digital Forensics and Cybersecurity, City University of New York (CUNY).

٢٠-يوسف بوغرارة، (٢٠١٧) الاستراتيجية الجزائرية للأمن السيبراني والدفاع في الفضاء السيبيري، مجلة الدراسات الإفريقية وحوض النيل، المركز الديمقراطي العربي، برلين، ألمانيا، مج (١)، ع (٣).

21-E. M. Rogers (2004). A Prospective and Retrospective Look at the Diffusion Model, Journal of Health Communication, Vol. (9),No. (1) ,PP: 13-17.

٢٢-غادة عيد. (٢٠١٢) القياس والتقويم التربوي مع تطبيقات برنامج، SPSSالكويت: مكتبة الفلاح للنشر والتوزيع.

٢٣-مبارك بن واصل الحازمي، (٢٠٢١) الإعلام العربي والأمن القومي، المجلة المصرية لبحوث الاتصال الجماهيري، عدد مايو، كلية الإعلام، جامعة بني سويف.

24-Mangold, L.V. (2016). An Analysis of Knowledge Gain in Youth Cybersecurity Education Programs, PhD Thesis, Northcentral University San Diego, California, U.S.A

٢٥- منى الجبور، (٢٠١٢) الأمن السيبراني: التحديات ومستلزمات المواجهة .اللقاء الأول للمختصين في أمن وسلامة الفضاء السيبراني, جامعة الدول العربية: المراز العربي للبحوث القانونية والقضائية. بيروت , ص ص: 27-28.

٢٦-علم الدين بانقا. (٢٠١٩) مخاطر الهجمات الإلكترونية (السيبرانية) وآثارها الاقتصادية: دراسة حالة دول مجلس التعاون الخليجي .الكويت: المعهد العربي للتخطيط، سلسلة دراسات تنموية، ع(٣٦).

27-Richard Berry(2018), just because you play guitar and are from nasheville doesn't mean you are country singer the emergency of mediaum identivtes in prodcusting, prodcusting new aural cultures and digital media ,palgrave macmillan.

28-Richard A. Kemmerer, Cyber security, University of California Santa Barbara, Department of Computer Science.

٢٩-ياسمين بلعسل، الحسين عمروش. (٢٠٢١) التهديدات والجرائم الإلكترونية والأمن السيبراني في الوطن العربي، مجلة نوميروس الأكاديمية، مج (٢) , ع (٢).

٣٠-فاطمة يوسف المنتشري ورنده حريري. (٢٠٢٠) درجة وعى معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات .المجلة العربية للتربية النوعية، المؤسسة العربية للتربية والعلوم والآداب، مج (١٤) ,ص ص ٩٥-١١٥.

31-Melnick, J. (2018). describe the 10 most common cyber attack types:. Retrieved 12 2, 2018, from https://blog.netwrix.com/2018/05/15/top 10 most common types of cyber-attacks/.

٣٢- أميرة محمد محمد أحمد، (٢٠٢١) استراتيجيات مكافحة التهديدات والجرائم الإلكترونية في العصر المعلوماتي تعزيزا لرؤية مصر 2030دراسة استشرافية، مجلة البحوث الإعلامية، كلية الإعلام جامعة الأزهر، ع(58).

33-Espiner T. (2011). UK Cyber-readiness is patchy, ZDNet, UK, 2011. http://goo.gl/G108XJ. Retrieved MAY 17, 2022, from UK cyber readiness is 'patchy', says Chatham House: https://www.zdnet.com/article/uk-cyber-readi-ness-is-patchy-says-chatham-house/

٣٤-محمد وائل القيسي. (٢٠٢٠) مستقبل الأمن الاستراتيجي العالمي في ظل التحديات التكنو معلوماتية والفضاء السيبراني .مجلة دراسات إقليمية: جامعة الموصل، مركز الدراسات الإقليمية، مج (١٣) , ع (٤٤) ., ص ص 139–173.

٣٥-سحر محمد صفا الله. (٢٠١٩) المنطقة العربية في مؤتمر دافوس للأمن السيبراني خلال السنوات الأخيرة , مجلة قضايا ونظرات .مركز الحضارة للدراسات والبحوث. ع (١٤), ص ص.٩٧-١٠٠.

36-Black. M., Chapman, D. & Clark, A. (2018). The enhanced virtual laboratory: extending cyber security awareness through a web-based laboratory. Information systems education journal (ISED), Vol. (16), No. (6), PP: 4-11.

37-Da Veiga, A. (2019). Achieving a security culture. In I. Vasileiou and S. Furnell (eds.) Cybersecurity Education for Awareness and Compliance, Hershey, PA: IGI Global. (PP. 72–92).

38-Luurs, G. (2018). Chatting about cyberbullying: An activity systems analysis of cyberbullying. A doctoral dissertation, North Carolina State University.