تصور مقترح لدور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني في ضوء خبرات بعض الدول

إعداد
د. رشا عبد القادر محمد الهندي
مدرس بقسم التعليم العالي والتعليم المستمر
كلية الدراسات العليا للتربية- جامعة القاهرة

مستخلص البحث:

هدف البحث إلى تعرُّف دور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني في ضوء خبرات بعض الدول، وقد اعتمد البحث على المنهج الوصفي مستخدمًا الاستبانة كأداة لجمع البيانات باعتبارها من أهم وأنسب أدوات المنهج الوصفي، وقد تكونت الاستبانة من (٢٥) فقرة، وتم تطبيقها على عينة من طلاب الدراسات العليا (الماجستير- الدكتوراه) بكلية الدراسات العليا للتربية جامعة القاهرة مكونة من (٩٣) طالبًا تم اختيارهم بطريقة عشوائية بنسبة (٢٣.٣٦%) من المجتمع الأصلي للطلاب البالغ (٣٩٨) طالبًا في العام الجامعي ٢٠٢٠/ ٢٠٢١م، وتوصلت نتائج البحث إلى تقديم تصور مقترح لدور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني في ضوء خبرات بعض الدول.

الكلمات المفتاحية: الأمن السيبراني – التوعية – جامعة القاهرة – الدراسات العليا.

A suggested vision of the role of Cairo University in awareness of graduate students about cyber security in light of the experiences of some countries

Abstract

The research aims to know the role of Cairo University in awareness of post graduate students about cybersecurity in the light of the experiences of some countries, and the research relied on the descriptive approach, using the questionnaire as a data collection tool consisting of (25) phrases, as it is one of the most important and most appropriate tools of the descriptive analytical approach on a sample of graduate students(Masters - PhD) at the Faculty of Graduate Studies of Education at Cairo University, It is composed of (93) students, randomly selected, at a rate of (23.36%) from the original population of (398) student in the academic year 2020/2021. The results of the research showed that presenting a proposed vision for the role of Cairo University in educating graduate students about cybersecurity in the light of the experiences of some countries.

Key words: Cyber security- awareness - Cairo University - Graduate studies.

المقدمة :

منذ ظهور الإنترنت والتكنولوجيا الرقمية والثورة المعلوماتية في القرن الحادي والعشرين بدأت المجتمعات تتغير تغيرًا سريعًا وجذريًّا؛ حيث أدت الأهمية المتزايدة للمعرفة إلى جانب العولمة والآثار المترتبة على التطور التكنولوجي وثورة المعلومات والاتصالات في عصر الثورة الصناعية الرابعة إلى إيجاد عالم مختلف تمامًا.

وتختلف الثورة الصناعية الرابعة عن الثورات السابقة في شدتها وتعقيدها واتساع نطاقها بحكم استنادها في جوهرها إلى ظاهرة تكنولوجية جديدة اسمها التحول الرقمي، أي: اندماج التكنولوجيات الرقمية وتغلغلها السريع في البنية التحتية لكل مؤسسة؛ فقد ساهمت في حدوث تقارب بين تلك التكنولوجيات؛ حيث تندمج مجموعة كبيرة من التكنولوجيات التي تشتمل على إنترنت الأشياء والحوسبة السحابية وتحليل البيانات الضخمة والذكاء الاصطناعي والأمن السيبراني لتوجد نظامًا بيئيًّا يتيح استفادة متبادلة بين مختلف أنواع التكنولوجيات بحيث تستفيد كل واحدة من الأخرى وتساهم في تطويرها، وبذلك وجدت الشركات التجارية والمجتمعات على حدٍّ سواء نفسها أمام فرص وتحديات غير مسبوقة.

وقد صاحب التطور السريع في تكنولوجيا المعلومات والاتصالات نموٌّ متزايد في استخدام أجهزة الحاسبات والاتصالات في كثير من القطاعات الحيوية مثل المؤسسات المالية والاتصالات والنقل والتعليم والرعاية الصحية، وغيرها، هذا بالإضافة إلى تزايد أعداد مستخدمي الإنترنت؛ حيث بلغ نحو ٤٨.٥ مليون مستخدم في مصر بكثافة ٥٥.٧ % في عام ٢٠١٩/ ٢٠٢٠ (وزارة الاتصالات وتكنولوجيا المعلومات، ٢٠٢١)، وقد زاد عدد مستخدمي الإنترنت من ١,١ بليون مستخدم بنسبة (١٦,٨%) في عام ٢٠٠٥ إلى ٤,١ بليون مستخدم بنسبة (٥٣,٦%) من عدد السكان حول العالم في عام ٢٠١٩ يستخدم معظمهم وسائل التواصل الاجتماعي، مما يجعلها أكبر تجمع للتفاعل البشري، ويفتح الباب لتبادل الأفكار والخبرات الجيدة، لكنَّه في المقابل يُعَرِّض أخلاقيات المجتمع للخطر نظرًا لصعوبة مراقبة محتوى الإنترنت (ITU, 2019).

فالنمو الاقتصادي واستقرار أية دولة يعتمد على توافر عامل الأمن وتوافر بنية تحتية قوية لتكنولوجيا المعلومات والاتصالات، وتُعَد الهجمات السيبرانية من أخطر التحديات الاقتصادية التي ينفذها مجرمو الإنترنت، كما أنها تؤثر أيضًا على الأمن القومي في الفضاء السيبراني، ولذلك فإن هناك حاجة ملحة إلى تأمين الفضاء السيبراني لضمان نمو اقتصاد البلاد وحمايتها.

وبناءً عليه يقدم الأمن السيبراني حلًّا لأبرز التحديات الملحة التي تواجه المجتمعات بصفة عامة والجامعات بصفة خاصة؛ حيث يلعب دورًا محوريًّا في معالجة التحديات المستقبلية نظرًا لاستخدامه كتكنولوجيا لإدارة الشبكات، فتقديم خدمات تكنولوجيا المعلومات والاتصالات بشكل أكثر أمانًا وسلاسةً من خلال نظام أمن سيبراني فَعَّال يساعد في تحقيق عدد من أهداف التنمية المستدامة التي وضعتها الأمم المتحدة بما في ذلك: إتاحة تكنولوجيا المعلومات والاتصالات للجميع بصورة آمنة وشفافة (الهدف التاسع)؛ حيث إن انتشار تكنولوجيا المعلومات والاتصالات والترابط العالمي يوفر إمكانات كبيرة لتسريع التقدم البشري وتقليل الفجوة الرقمية وتطوير مجتمعات المعرفة، مثله في ذلك مثل الابتكار العلمي والتكنولوجي في مجالات متنوعة مثل الطب والطاقة، ومع ذلك ينبغي أن يكون بناء الثقة وتوفير الأمان في استخدام تكنولوجيات المعلومات والاتصالات من أجل التنمية المستدامة من الأولويات، خاصةً في ضوء التحديات المتنامية، بما في ذلك إساءة استخدام هذه التكنولوجيا باستعمالها في أنشطة ضارة بدءًا بالتحرش ووصولًا إلى الجريمة والإرهاب (لوران بروبست وآخرون، ٢٠١٧).

لذلك فمن المهام الأساسية التي ينبغي أن تتصدى لها الجامعة في زماننا هذا توعية الطلاب بصفة عامة، وتوعيتهم بالأمن السيبراني بصفة خاصة من خلال التدريس، والبحث العلمي، وخدمة المجتمع، وأن تعمل على نشر المعرفة وإثراء المهارات العلمية في أمن المعلومات بهدف مكافحة الانتهاكات والجرائم السيبرانية، كما يجب على أعضاء هيئة التدريس توعية الطلاب وتحذيرهم من التهديدات الإلكترونية، ومن هنا وافق مجلس جامعة القاهرة على استحداث برنامج يمنح بكالوريوس الشبكات والأمن السيبراني في كلية الحاسبات والذكاء الاصطناعي بنظام الساعات المعتمدة كأول برنامج من نوعه في الجامعات المصرية الحكومية يجمع بين المجالين (موقع جامعة القاهرة، ٢٠٢١).

بالإضافة إلى تعاون وزارة الاتصالات وتكنولوجيا المعلومات مع شركة Cisco العالمية في مبادرة الأمن السيبراني بتقنية التعلم عن بعد لتعزيز الثقافة الرقمية للتعامل مع البيانات واستخدام شبكة الإنترنت بشكل آمن بما يساهم في تدعيم حماية البيانات الشخصية والخصوصية عند استخدام وسائل الاجتماعات والتواصل عبر الإنترنت، كما تتيح المبادرة محتوى تعليميًّا تفاعليًّا للمتدرب(جامعة بنها، ٢٠٢١).

كما اهتمت الجامعة المصرية اليابانية بفتح دبلومة مهنية في الأمن السيبراني في قسم علوم وهندسة الكمبيوتر بالجامعة بالتعاون مع إحدى الشركات اليابانية الرائدة في مجال الأمن السيبراني لإعداد كوادر علمية مدربة للتصدي للهجمات السيبرانية وحل مشكلات الأمن السيبراني والعمل على إكساب الطلاب المهارات العملية والمعرفية النظرية لتأمين أنظمة الحاسب وشبكات الكمبيوتر ومراكز البيانات، وبالإضافة إلى ذلك فإنها تؤهلهم لإجراء تقييم أمني واختبار الاختراق واكتشاف التهديدات والهجمات السيبرانية(بوابة الأهرام، ٢٠٢١).

الدراسات السابقة:

ونظرًا لأهمية موضوع الأمن السيبراني والحاجة إليه نجد أنه قد تناولته **دراسات عديدة**، وسوف يتم عرض الدراسات السابقة من الأحدث إلى الأقدم، ومنها: دراسة إبراهيم(٢٠٢١) التي هدفت إلى الكشف عن فاعلية برنامج تدريبي مقترح لتنمية الوعي بجوانب الأمن السيبراني في التعليم عن بعد لدى معلمات العلوم بالمرحلة الابتدائية في المملكة العربية السعودية، وتم استخدام المنهج التجريبي ذو التصميم شبه التجريبي ذي المجموعة الواحدة، وتوصلت الدراسة إلى وجود فرق ذي دلالة إحصائية بين متوسطي درجات المعلمات في التطبيقين القبلي والبعدي لمقياس الوعي؛ لصالح التطبيق البعدي؛ ويدل هذا على فاعلية البرنامج التدريبي المقترح.

ودراسة المنتشري (٢٠٢٠) التي هدفت إلى تعرُّف درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات، وتم استخدام المنهج الكمي الوصفي التحليلي. وتوصلت الدراسة إلى أن معلمات المرحلة المتوسطة على درجة متوسطة من الوعي بكل من مفاهيم الأمن السيبراني، وخطر الأمن

السيبراني، وانتهاكات الأمن السيبراني، وعدم وجود فروق ذات دلالة احصائية عند مستوى (٠.٠٥) تعزي إلى متغيري المؤهل الدراسي وعدد سنوات الخبرة بين استجابات المعلمات، ووجود فروق تعزي إلى متغير دورات تدريبية في الأمن السيبراني.

ودراسة القحطاني (٢٠١٩) التي سعت إلى تعرُّف مدى توفر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي من وجهة نظرهم من خلال تعرُّف آرائهم حول المفهوم الأقرب له، وأهم الجرائم التي يتعامل معها، وطرق الوقاية المجتمعية من جرائم الفضاء السيبراني، والمعوقات المجتمعية لتحقيق الوقاية من هذه الجرائم، وتم استخدام المنهج المسح الاجتماعي. وتوصلت النتائج إلى أقرب مفهوم للأمن السيبراني من وجهة نظر عينة الدراسة هو " استخدام مجموعة من الوسائل التقنية والتنظيمية والإدارية لمنع الاستخدام غير المصرح به ومنع سوء الاستغلال واستعادة المعاملات الإلكترونية ونظم الاتصالات والمعلومات التي تحتويها وجريمة الاحتيال الإلكتروني أكثر جريمة يتعامل معها الأمن السيبراني، والتوعية الإعلامية للمجتمع من أهم طرق الوقاية المجتمعية لمشكلات الفضاء السيبراني. ومن أهم المعوقات هو التطور الهائل في نظم المعلومات ووسائل التكنولوجيا التي يتعامل معها أفراد الأسرة.

ودراسة الصحفي وعسكول (٢٠١٩) التي هدفت إلى الكشف عن مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة، وتم استخدام المنهج الكمي، وتوصلت الدراسة إلى وجود ضعف وقصور لدى معلمات الحاسب الآلي في الوعي بمفاهيم الأمن السيبراني، ووجود ضعف لدى معلمات الحاسب الآلي في الوعي بمستوى الأمن السيبراني.

ودراسة نينكيو وآخرين (Nyinkeu et Al., 2018) التي سعت إلى تحديد مفاهيم الأمن السيبراني التي ينبغي تعزيزها لدى طلاب تكنولوجيا المعلومات، وتوصلت الدراسة إلى أهمية تعزيز مفاهيم الاستخدام الآمن للإنترنت، والتمييز بين الأمن السيبراني وأمن الشبكات.

بينما دراسة ناكاما وباولت (Nakama & Paullet, 2018) التي هدفت إلى تعليم طلاب الجامعة كيفية التصدي للهجمات السيبرانية في مجتمعات هاواي الريفية؛ حيث الحاجة إلى التغيير من بيئة موجهة من المعلم في المدارس الثانوية إلى بيئة موجهة للطالب في الجامعة، حيث يُتَوَقَّع من الطلاب إدارة تعلمهم بأنفسهم، لذلك يجب تنمية بعض المهارات لدى الطلاب ليتعلموا كيفية التنقل في نظام إدارة التعلم، وإرسال وتلقي الرسائل بفعالية بين الطلاب وأعضاء هيئة التدريس، وتوصلت الدراسة إلى إكساب الطلاب استراتيجيات التعلم عبر الإنترنت، وساهمت أيضا في تنمية الأمن السيبراني لدى طلاب الجامعة عبر المراحل الدراسية بها.

ودراسة جانستر وأولسون (Jansäter & Olsson, 2018) التي سعت إلى استكشاف وتحديد العوامل المختلفة التي تؤثر على عدم التركيز على الأمن السيبراني في المدن الذكية، وأن هناك مشكلة جوهرية فيما يتعلق بمستوى الأمن السيبراني في المدن الذكية، وأنها تفتقر إليه، وتوصلت الدراسة إلى وجود عدم تركيز على الأمن السيبراني ويرجع ذلك إلى انخفاض مستوى التوافق الاستراتيجي داخل المؤسسات، نتيجة عدم تمثيل استراتيجية نظم المعلومات، مما يترتب عليه زيادة في العمل مع تكنولوجيا المعلومات والأنظمة بالإضافة إلى عدم التوافق بين الاستراتيجية التنظيمية واستراتيجية نظم المعلومات بجانب عدم وجود أجندة مناسبة للأمن السيبراني في المنظمات.

أما دراسة كوغلينج (coughlin, 2017) فقد هدفت إلى تصميم برنامج للوعي بالأمن السيبراني لدى طلبة السنة الأولى بالجامعة للطلاب غير المتخصصين في تكنولوجيا المعلومات إلى أخطار الأمن السيبراني التي يتعرض لها المراهقون وغير البالغين الراشدين، وتقييم الأساليب المتاحة التي يمكن من خلالها تدريبهم على أن يكونوا أكثر إدراكًا لقضايا الأمن السيبراني وتمكينهم من الدفاع عن أنفسهم ضد الهجوم بشكل أفضل، وتوصلت النتائج إلى أن الطلاب يتعرضون للعديد من الهجمات الإلكترونية التي من شأنها أن تؤثر بالسلب على الطلاب، كما أشارت إلى وجود مجموعة من الحلول التي يمكن من خلالها التصدي للهجمات الإلكترونية.

ودراسة كريتزنجر وآخرين (Kritzinger et Al.,2017) سعت إلى استعراض المبادرات الخاصة برفع مستوى الوعي بالأمن السيبراني لدى الطلبة في مدارس جنوب أفريقيا والمدارس البريطانية، وأظهرت نتائج الدراسة وجود عدد من المبادرات شملت دمج مفاهيم الأمن السيبراني ضمن المناهج الدراسية، وتدريب المعلمين، ووضع سياسات خاصة بالأمن السيبراني، وسن قوانين وتشريعات لمافحة الانتهاكات السيبرانية، ودمج الآباء في برامج التوعية بالأمن السيبراني، وعقد ورش عمل وأيام مفتوحة وندوات لهذا المجال، والتوعية عبر وسائل الإعلام.

وهدفت دراسة موسكال (Moskal, 2015) إلى وضع تصور لإنشاء مركز للتميز في الأمن السيبراني في الجامعات الأمريكية بهدف تهيئة الخريجين للعمل في هذا المجال، وتم عمل دراسة مسحية شملت ١٠٠ جامعة أمريكية، وذلك بمراجعة الوثائق الرسمية لمعرفة مدى الاهتمام بتدريس علوم الأمن السيبراني وتطويرها، وأكدت على خطر الانتهاكات والمخاطر السيبرانية، وأوصت الدراسة بضرورة الاهتمام بالأمن السيبراني باعتباره من أهم الدعائم للاقتصاد الأمريكي في المستقبل.

أما دراسة بوسي وساديرا (pusey & sadera, 2011) فقد هدفت إلى تحديد درجة وعي المعلمين وطلبة كلية إعداد المعلمين بمفاهيم الأمن السيبراني، والانتهاكات السيبرانية، والسلامة السيبرانية، ودرجة معرفتهم بتدريس هذه المفاهيم، وتوصلت الدراسة إلى أن درجة معرفة المعلمين بمفاهيم الأمن السيبراني، الانتهاكات السيبرانية، والسلامة السيبرانية، درجة منخفضة جدا، وأن ٢٠% منهم فقط لديه وعي بدرجة متوسطة بتلك المفاهيم، وأظهرت النتائج بأهمية توعية المعلمين والطلبة بمفاهيم والانتهاكات السيبرانية، كما أظهرت أيضا أنه لا يوجد لدى المعلمين تصور واضح لكيفية تدريس تلك المفاهيم، أو كيفية إدراجه أثناء ممارساتهم التدريسية.

التعقيب على الدراسات السابقة:

اتضح من خلال عرض الدراسات السابقة ما يلي:

نواحي الاتفاق والاختلاف بين الدراسات السابقة والدراسة الحالية:

باستعراض الدراسات السابقة تتبين أوجه الشبه والاختلاف بينها وبين الدراسة الحالية، وما أفادته تلك الدراسات لهذه الدراسة الحالية.

يتضح من الدراسات السابقة أن الدراسة الحالية تتفق معها في الاهتمام بالوعي بالأمن السيبراني لدى الأفراد بصفة عامة، ولدى الطلاب بصفة خاصة.

أوجه الاتفاق مع الدراسات السابقة:

اتفقت الدراسة الحالية مع الدراسات السابقة في استخدام الاستبانة كأداة للدراسة، ومنها: دراسة القحطاني (٢٠١٩)؛ ودراسة الصحفي وعسكول (٢٠١٩). وقد اعتمدت الدراسة الحالية على المنهج الوصفي في تحليل البيانات والوصول للنتائج، واتفقت في ذلك مع دراسة المنتشري (٢٠٢٠)؛ بينما اختلفت مع بعض الدراسات الأخرى التي استخدمت المنهج المسحي كما في دراسة القحطاني (٢٠١٩)؛ ودراسة موسكال (Moskal, 2015)، والمنهج التجريبي كما في دراسة إبراهيم (٢٠٢١).

أوجه الاختلاف مع الدراسات السابقة:

كما اختلف البحث الحالي مع الدراسات السابقة في عينة الدراسة؛ حيث تناول البحث الحالي طلاب الدراسات العليا، بينما اقتصرت بعض الدراسات السابقة على عينة طلاب المرحلة الثانوية كما في دراسة كلٍّ من كرتيزنجر وآخرون (Kritzinger et Al., 2017)؛ والصحفي وعسكول (٢٠١٩)، وطلاب الجامعة كما في دراسة كوغلينج (Coughlin, 2017)؛ والقحطاني (٢٠١٩)، وعينة المعلمات كما في دراسة بوسي وساديرا (Pusey & Sadera, 2011).

وتتميز الدراسة الحالية عن الدراسات السابقة بأنها تتناول دور الجامعة في توعية طلاب الدراسات العليا بجامعة القاهرة بالأمن السيبراني في ضوء خبرات بعض الدول من حيث التدريس، والبحث العلمي، وخدمة المجتمع. وقد استفاد البحث من الدراسات السابقة في بلورة مشكلة البحث، وتحديد الإطار النظري له، ومِنْ ثَمَّ اختيار المنهج المناسب لإجراء البحث.

مشكلة البحث وأسئلته :

تبرز الحاجة إلى ضرورة فهم ماهية الأمن السيبراني كمتغير جديد في العلاقات الدولية مع انفجار الثورة المعلوماتية ودخول العصر الرقمي خاصةً وما نتج عنه من تداعيات عديدة في القرن الحادي والعشرين بسبب ظهور تهديدات للأمن الإلكتروني للمعلومات والبيانات الشخصية للمستخدمين وللمستخدمين أنفسهم، وظهور جرائم سيبرانية أصبحت تشكِّل تحديًا كبيرًا للأمن القومي، وكذلك الدولي، لدرجة اعتبار الفضاء السيبراني بمثابة المجال الخامس في الحروب بعد البر والبحر والجو والفضاء، وهو ما استدعى ضرورة وجود ضمانات أمنية ضمن هذه البيئة الرقمية تبلورت بشكل أساسي في ظهور الأمن السيبراني cyber security كبُعد جديد ضمن أجندة الدراسات الأمنية.

ويعتبر الأمن السيبراني أعلى تحديات الأمن القومي في القرن الحادي والعشرين، كما يبرز التحدي الثقافي والفكري كإحدى بوابات التهديدات السيبرانية، وذلك عن طريق الغزو الفكري في شبكات التواصل ونشر ثقافة العنف والتحريض على الإجرام، وهذا ما يستدعي العناية بالمحتوى الإلكتروني القائم على نشر العلم والتعريف بالحضارات (لوران بروبست وآخرون، ٢٠١٧).

وبناءً على ما سبق ولأن طلاب الجامعة جزء لا يتجزأ من المجتمع المصري فمن الأمور الهامة والأساسية أن يدركوا أهمية الأمن السيبراني، وذلك لأنهم يمثلون درعًا من دروع الأمن القومي للحماية من التهديدات التي تحدث لاختراق الأنظمة الإلكترونية والمعلوماتية.

وبناءً على ما سبق عرضه من الدراسات العربية والأجنبية نجد أن بعض الدراسات قد أكدت وجود ضعف في وعي المعلمين والطلاب بكلٍّ من مفاهيم الأمن السيبراني والانتهاكات السيبرانية، وأكدت أهمية توعيتهم بالمفاهيم والانتهاكات السيبرانية، ومنها: دراسة فاطمة المنتشري (٢٠٢٠)، ودراسة الصحفي وعسكول (٢٠١٩)، ودراسة بوسي وساديرا (pusey & sadera, 2011)، كما أظهرت دراسة كوغلينج (Coughlin, 2017)، ودراسة موسكال (Moskal, 2015) وجود خطر على الطلاب

نتيجة تعرضهم للعديد من الهجمات والمخاطر السيبرانية التي تؤثر عليهم بالسلب، بينما أظهرت دراسة جانستر وأولسون (Jansäter & Olsson, 2018) عدم التركيز على الأمن السيبراني، أما دراسة ناكاما وباولت (٢٠١٨) فقد أكدت أهمية تنمية الأمن السيبراني لدى طلاب الجامعة عبر المراحل الدراسية المختلفة، وضرورة إكساب الطلاب إستراتيجيات التعلم عبر الإنترنت، وقد أكدت دراسة نينكيو وآخرين (Nyinkeu et Al., 2018)، ودراسة موسكال (Moskal, 2015) أهمية تعزيز مفاهيم الاستخدام الآمن للإنترنت، وضرورة الاهتمام بالأمن السيبراني باعتباره أهم دعائم الاقتصاد في المستقبل، كما أضافت دراسة كريتزنجر وآخرين (Kritzinger & others, 2017) ضرورة دمج مفاهيم الأمن السيبراني مع المناهج الدراسية.

وإذا كانت تلك الدراسات قد تناولت الأمن السيبراني لدى الطلاب والمعلمين فإن ذلك يبرز الحاجة إلى الاهتمام بالوعي بالأمن السيبراني لدى طلاب الدراسات العليا؛ حيث إنهم طلاب بحث يستخدمون شبكة المعلومات الدولية في البحث العلمي، وهم في حاجة ماسَّة إلى الوعي بمخاطر الهجمات الإلكترونية، ومن هنا تبرز الحاجة إلى ضرورة فهم ماهية الأمن السيبراني كمتغير جديد في العلاقات الدولية، وهذا هو ما يسعى البحث الحالي إلى دراسته.

وفي ضوء ذلك تحددت مشكلة البحث الحالي في السؤال الرئيس التالي:

ما دور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني في ضوء خبرات بعض الدول؟

ويتفرع من هذا السؤال الرئيس مجموعة من الأسئلة الفرعية، وهي:

١- ما الإطار المفاهيمي للأمن السيبراني؟

٢- ما الخبرات العالمية والعربية في مجال الأمن السيبراني؟

٣- ما درجة وعي طلاب الدراسات العليا في جامعة القاهرة بالأمن السيبراني؟

٤- ما التصور المقترح لدور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني؟

أهداف البحث:

يهدف البحث إلى تعرُّف دور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني في ضوء خبرات بعض الدول، وذلك من خلال استعراض الإطار المفاهيمي للأمن السيبراني وأهدافه، وتحديد أبعاد الأمن السيبراني ومجالات استخدامه، واستعراض بعض الخبرات العالمية والعربية في مجال الأمن السيبراني، بالإضافة إلى تعرُّف درجة وعي طلاب الدراسات العليا في جامعة القاهرة بالأمن السيبراني، وصولًا إلى تصور مقترح لدور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني.

أهمية البحث:

تنبع أهمية هذا البحث من أهمية الموضوع الذي يتناوله، ويتمثل ذلك فيما يلي:

١- أهمية الأمن السيبراني؛ وذلك لكونه أحد أهم تحديات الأمن القومي في القرن الحادي والعشرين.

٢- تبنى البحث الحالي اتجاهًا جديدًا من الاتجاهات الحديثة في التعليم.

٣- العمل على نشر ثقافة الأمن السيبراني والاستخدام الآمن للإنترنت.

٤- كما تنبع أهمية البحث من خلال توجيه المسئولين إلى إدراج مفاهيم الأمن السيبراني ضمن البرامج المقدَّمة للطلاب.

٥- من المأمول أن يسهم هذا البحث في تشجيع المسئولين في الجامعة على الاهتمام بعقد دورات تدريبية بشكل مستمر لأعضاء هيئة التدريس والطلاب في مجال الأمن السيبراني.

٦- إمكانية أن يلقي هذا البحث الضوء على معرفة دور الجامعة في توعية طلاب الدراسات العليا بالأمن السيبراني والالتزام بالأمن السيبراني عند التعامل مع مصادر المعلومات المختلفة.

منهج البحث وأداته :

اعتمد البحث الحالي على المنهج الوصفي في جمع وتحليل واستخلاص كل ما يتعلق بالأمن السيبراني، وبناءً على هذا تم الرجوع إلى التقارير والدراسات السابقة، بالإضافة إلى الأدبيات التي تناولت الأمن السيبراني، ثم توضيح أهداف الأمن السيبراني، مع الإشارة إلى مجالات استخدامه، وأهميته، وأبعاده، وبعض الخبرات العالمية والعربية في مجال الأمن السيبراني، كما اعتمد البحث على الاستبانة باعتبارها إحدى أدوات المنهج الوصفي لتعرُّف درجة وعي عينة البحث من طلاب الدراسات العليا بجامعة القاهرة بالأمن السيبراني.

حدود البحث:

- اقتصر **الحد الموضوعي للبحث** على التوصل إلى تصور مقترح لدور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني في ضوء تجارب بعض الدول من خلال استعراض مفاهيم الأمن السيبراني، بالإضافة إلى طرق المحافظة على الأمن السيبراني، مع تعرُّف مستوى وعي الطلاب بالأمن السيبراني، مع عرض بعض التجارب العالمية والعربية في مجال الأمن السيبراني المتمثلة في ماليزيا – السعودية – أمريكا– أستراليا باعتبارها من الدول الرائدة في مجال الأمن السيبراني.
- واقتصرت **حدوده البشرية والمكانية** على عينة من طلاب الدراسات العليا (الماجستير والدكتوراه) في كلية الدراسات العليا للتربية بتخصصاتها المختلفة، **أما الحدود الزمانية** فكانت خلال الفصل الأول من العام الدراسي ٢٠٢٠/ ٢٠٢١، وهو زمن تطبيق أداة البحث .

مصطلحات البحث: تم عرض المفاهيم المختلفة للبحث الحالي في إطاره النظري

التعريف الإجرائي للأمن السيبراني:

هو عبارة عن عمليات الحماية التي يمكن أن تقوم بها جامعة القاهرة لحماية طلاب الدراسات العليا من العمليات المرتبطة بتقنيات الاتصالات والمعلومات للحد من الخسائر والأضرار والجرائم المرتبطة بهذه التقنيات من خلال التدريس والبحث العلمي وخدمة المجتمع.

خطوات السير في البحث:

تمثلت إجراءات البحث الحالي فيما يلي:

- مراجعة الأدبيات التي تتعلق بالأمن السيبراني، وهي تتناول الإطار المفاهيمي للأمن السيبراني، وعناصر الأمن السيبراني، وأهدافه، وأبعاده، وأهميته، بالإضافة إلى مجالات استخدامه، وبعض التجارب العالمية والعربية في مجال الأمن السيبراني.
- إعداد الجانب الميداني وتحديد الهدف منه.
- إعداد أداة البحث الميداني.
- اختيار عينة البحث وتطبيق أداة البحث عليها.
- جمع البيانات وإجراء المعالجة الإحصائية عليها.
- وضع تصور مقترح لدور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني في ضوء خبرات بعض الدول.

الإطار النظري للبحث:

يشمل الإطار النظري مجموعة من العناصر، وهي: الإطار المفاهيمي للأمن السيبراني، وعناصر الأمن السيبراني، وأهدافه، وأبعاده، وأهميته، بالإضافة إلى مجالات استخدامه، وبعض التجارب العالمية والعربية في مجال الأمن السيبراني.

أولًا: الإطار المفاهيمي للأمن السيبراني:

السيبرانية مشتقة من كلمة "سايبر Cyber"، وهي تعني كل ما يتعلق أو يرتبط بالحواسيب وتكنولوجيا المعلومات والواقع الافتراضي (قاموس اكسفورد، ٢٠٢١).

وغالبًا ما يكون "الأمن السيبراني" مشابهًا لمصطلح "أمن المعلومات"، وهما يستخدمان معًا لوصف أمان البنية التحتية لمعلومات المؤسسة، ولكنه يختلف عنه في أن الأمن السيبراني له بعدٌ آخر للأمن، ألا وهو حماية الأرواح البشرية من الهجمات الإلكترونية، نظرًا لانتشار أنظمة المعلومات في البنية التحتية الحيوية (Von Solms and van Niekerk, 2013, 97).

وقد أكد كيمرر (Kemmerer, 2003,1) أن الأمن السيبراني هو عبارة عن وسائل دفاعية من شأنها كشف وإحباط المحاولات التي يقوم بها القراصنة.

ويُعرَّف "أمن المعلومات" بأنه حماية موارد المعلومات وعناصرها الحاسمة بما في ذلك الأنظمة والأجهزة التي تستخدم تلك المعلومات وتخزنها وتنقلها، بينما الأمن السيبراني لا يشمل فقط حماية موارد المعلومات، ولكنه يشمل أيضًا حماية الأصول الأخرى، بما في ذلك الشخص نفسه، وإذا كان دور العامل البشري في أمن المعلومات منحصرًا في عملية الأمن فإنه في الأمن السيبراني له بُعد إضافي، وهو أن البشر يُعَدُّون أهدافًا محتملة للهجمات الإلكترونية أو حتى المشاركة عن غير قصد في هجوم إلكتروني، وهذا البُعد الإضافي له آثار أخلاقية على المجتمع بالكامل منذ حماية بعض الفئات الضعيفة؛ ولذلك فإنه يعتبر مسئولية مجتمعية (Von Solms and van Niekerk, 2013, 97, 98).

وقد تعددت تعريفات الأمن السيبراني، ومنها على سبيل المثال:

تعريف الاتحاد الدولي للاتصالات (ITU, 2008,2) للأمن السيبراني بأنه: مجموعة من الأدوات والسياسات والمفاهيم الأمنية وضمانات الأمان والمبادئ التوجيهية وأساليب إدارة المخاطر والإجراءات والتدريب وأفضل الممارسات والضمان والتقنيات التي يمكن استخدامها لحماية البيئة السيبرانية وأصول المنظمة والمستخدم .

بينما في **التقرير الصادر عن الاتحاد الدولي للاتصالات** (٢٠١١، ١٧) يعرف الأمن السيبراني بأنه: مجموعة من المهمات مثل: (تجميع وسائل، وسياسات، وإجراءات أمنية، ومبادئ توجيهية، ومقاربات لإدارة المخاطر، وتدريبات، وممارسات فضلى، وتقنيات) يمكن استخدامها لحماية البيئة السيبرانية وموجودات المؤسسات والمستخدمين.

ويُعرِّف المغربي ولوزافيو (Elmaghraby and Losavio, 2014, 491) الأمن السيبراني من الجانب الأمني بأنه يشمل الوصول غير القانوني إلى المعلومات والهجمات التي تسبب اضطرابات جسدية في توافر الخدمة.

ويشير المبارك (٢٠١٦) إلى أن مفهوم "الأمن السيبراني" هو مفهوم أوسع من "أمن المعلومات"، وهو يتضمن تأمين البيانات والمعلومات التي تُتَداول عبر الشبكات الداخلية أو الخارجية والتي يتم تخزينها في خوادم داخل أو خارج الشركة من الاختراقات، كما أن مفهوم

"أمن المعلومات" هو حماية المعلومات أو أنظمة المعلومات من النفاذ غير المصرح أو السرقة أو التعديل أو التشهير لحفظ سرية وخصوصية العملاء وبقاء المعلومات محفوظة.

ويعرف جبور (٢٠١٦) الأمن السيبراني بالحل الأمثل لمتابعة الاستخدام الواسع للإنترنت وتطبيقاته وأنظمته المختلفة للتقليل من المخاطر التي تنشأ من سوء الاستخدام، حيث توجد محتويات غير مشروعة وغير مرغوب فيها ذات تأثير سلبي على أخلاقيات وقيم المجتمع وتؤدي إلى تغييرات في شخصية الأفراد، وميل البعض منهم إلى سلوكيات منحرفة، وبالتالي كثرة الجرائم من خلال التقليد أو ممارسة ألعاب معينة تشجع على ذلك، ولهذا لابد من بناء مجتمع واعٍ مسئول ومدرِك لهذه المخاطر يستطيع التعامل معها وفقًا لقواعد السلامة، مع إدراكه للعواقب القانونية للتصرفات اللامسئولة والتي تُعَرِّض الآخرين للخطر أو السرقات.

ويُقصد بالأمن السيبراني أيضًا: " التكنولوجيات والعمليات والضوابط الهادفة إلى حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية التي تتضمن عادةً محاولة الوصول إلى المعلومات الحساسة أو تغييرها أو إتلافها، ويمكن أن تؤدي هذه الهجمات في حالة نجاحها إلى ابتزاز المال من الضحية أو التعدي على حقوق الملكية الفكرية أو تعطيل تقديم الخدمات" (لوران بروبست وآخرون ،٢٠١٧، ١٢).

ويعرف السالم (٢٠١٩) الأمن السيبراني بأنه: مجموعة من الأُطُر القانونية والتنظيمية، وإجراءات سير العمل، والوسائل التقنية والتكنولوجية التي تمثل الجهود المشتركة للقطاعين الخاص والعام المحلية والدولية والتي تهدف إلى حماية الفضاء السيبراني الوطني من خلال توافر أنظمة المعلومات وتمتين الخصوصية وحماية سرية المعلومات الشخصية واتخاذ جميع الإجراءات الضرورية لحماية الأفراد من مخاطر الفضاء السيبراني.

وخلاصة ما سبق أن الأمن السيبراني يتحدد في أنه:

عمليات الحماية التي يمكن أن تقوم بها الجامعة أو الأفراد لحماية العمليات المرتبطة بتقنيات الاتصالات والمعلومات للحد من الخسائر والأضرار والجرائم المرتبطة بهذه

التقنيات، أي: اتخاذ التدابير اللازمة لحماية موارد المعلومات والأشخاص من الهجمات الإلكترونية.

وللأمن السيبراني **عناصر** يجب أن تتوافر لضمان حماية المعلومات، ومنها (الصحفي وعسكول، ٢٠١٩، ٤٩٨، ٤٩٩):

- **السرية والأمن:** أي: التأكد من أن المعلومات لا تُكْشَف ولا يُطَّلَع عليها من قِبَل أشخاص غير مصرَّح لهم بذلك.
- **التكاملية وسلامة المحتوى:** التأكد من أن محتوى المعلومات صحيح ولم يتم تعديله أو تدميره أو تغييره أو العبث به في أي مرحلة من مراحل المعالجة أو التبادل، سواء في مرحلة التعامل الداخلي أو المعلومات أو عن طريق التدخل غير المشروع.
- **استمرارية توفر المعلومات أو الخدمة:** التأكد من استمرار عمل النظام المعلوماتي واستمرار القدرة على التفاعل مع المعلومات وتقديم الخدمة لمواقع المعلوماتية، وأن المستخدم لن يتعرض لمنع الاستخدام أو الدخول إلى النظام.
- **عدم إنكار التصرف المرتبط بالمعلومات ممن قام به:** أي: ضمان عدم إنكار الشخص المتصل بالمعلومات أو مواقعها بقيامه بتصرف ما، بحيث تتوافر قدرة إثبات هذا التصرف وأنَّ شخصًا ما في وقت معين قد قام به، وأيضًا عدم قدرة مستلم رسالة معينة على إنكار استلامه لهذه الرسالة.

ويمكن استخدام تقنيات الأمن السيبراني لضمان توافر النظام، وسلامته، ومصداقيته، وسريته، وعدم الإنكار، كما يمكن استخدام الأمن السيبراني لضمان احترام خصوصية المستخدم، وأيضًا يمكن استخدام تقنيات الأمن السيبراني لإثبات مصداقية المستخدم (ITU,2009,6) .

وبناءً عليه يجب توافر مجموعة من العناصر لضمان حماية المعلومات، ألا وهي: السرية والأمن، والتكامل وسلامة المحتوى، واستمرارية توفر المعلومة، بالإضافة إلى عدم إنكار التصرف المرتبط بالمعلومات ممن قام به.

وهناك العديد من التحديات التي تواجه الأمن السيبراني، ومن أهمها:

- **خطر اختراق وتخريب البِنَى التحتية للاتصالات وتكنولوجيا المعلومات:** وذلك من خلال نشر برمجيات خبيثة وفيروسات لتخريب أو تعطيل البِنَى التحتية للاتصالات وتكنولوجيا المعلومات (المجلس الأعلى للأمن السيبراني ٢٠١٧- ٢٠٢١).
- **التجسس السيبراني:** هو ممارسة استخدام تقنية المعلومات للحصول على معلومات سرية بدون إذن من أصحابها، وهو الأكثر استخدامًا لكسب الإستراتيجية الاقتصادية والعسكرية ميزة، ويتم إجراؤها باستخدام تقنيات التكسير والبرامج الضارة (المجلس الأعلى للأمن السيبراني(٢٠١٧- ٢٠٢١) .
- **خطر سرقة الهوية الرقمية والبيانات الخاصة:** تعد سرقة الهوية الرقمية من أخطر الجرائم التي تهدد مستخدمي الإنترنت ومستقبل الخدمات الإلكترونية؛ حيث قد تتعرض البيانات الشخصية للمستخدم للسرقة بهدف انتحال شخصيته والاستيلاء على ممتلكاته وأمواله أو ظهور اسمه في تعاملات مشبوهة أو غير قانونية (المجلس الأعلى للأمن السيبراني (٢٠١٧- ٢٠٢١)، ٢٠٢١) .
- **الاحتيال (الهندسة الاجتماعية):** وذلك عبر استغلال خدمة تحويل رقم الضحية إلى رقم المحتال عبر وسائل التواصل الاجتماعي بغرض الابتزاز (الوصابي، ٢٠٢١).

ثانيًا: أهداف الأمن السيبراني:

يهدف الأمن السيبراني إلى تأمين البيئة السيبرانية، وهو نظام قد يشمل أصحاب المصلحة الذين ينتمون إلى العديد من المنظمات العامة والخاصة باستخدام مكونات متنوعة وأساليب مختلفة للأمن على هذا النحو، فهناك مجموعة من السياسات والإجراءات المستخدمة لحماية الشبكات المتصلة (بما في ذلك أجهزة الكمبيوتر والأجهزة والمعلومات المخزنة، والمعلومات أثناء التنقل) من الوصول غير المصرَّح به أو التعديل أو السرقة أو الانقطاع أو التهديدات الأخرى(ITU,2009, 7).

وقد حدد الصائغ (٢٠١٨) أهداف الأمن السيبراني كالتالي:

- توفير بيئة آمنة تتمتع بقدر كبير من الموثوقية في مجتمع المعلومات.
- تعزيز حماية أنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحتويه من بيانات.
- التصدي لهجمات وحوداث أمن المعلومات التي تستهدف المستخدمين والمؤسسات.
- توفير المتطلبات اللازمة للحد من المخاطر والجرائم السيبرانية التي تستهدف المستخدمين.
- مقاومة البرمجيات الخبيثة وما تستهدفه من إحداث أضرار بالغة بالمستخدمين وأنظمة المعلومات.
- الحد من التجسس والتخريب الإلكتروني على مستوى الوزارة والمعلمين.
- التخلص من نقاط الضعف في أنظمة الحاسوب والأجهزة المحمولة بأنواعها، وسد الثغرات في أنظمة المعلومات.

ومما سبق يتضح أن الأمن السيبراني يهدف إلى توفير بيئة آمنة، وحماية الأنظمة والبيانات، بالإضافة إلى السرية والتصدي لهجمات وحوادث أمن المعلومات، وسد جميع الثغرات في أنظمة المعلومات المختلفة.

ثالثًا: أبعاد الأمن السيبراني:

بُعد الأمان هو عبارة عن مجموعة من إجراءات الأمان المصمَّمَة لمعالجة جانب معين من أمان الشبكة يتم تحديده بثمانية أبعاد (التحكم في الوصول- المصادقة- عدم الإنكار- سرية البيانات- أمن الاتصالات- سلامة البيانات- التوفر- الخصوصية)، وهذه الأبعاد تحمي من جميع التهديدات الأمنية الرئيسية. ولا تقتصر هذه الأبعاد على الشبكة، ولكنها تمتد أيضًا إلى التطبيقات ومعلومات المستخدم النهائي. وتنطبق أبعاد الأمان على مقدمي الخدمات أو المؤسسات التي تقدِّم خدمات أمنية لعملائها، ويتم تطبيق أبعاد الأمان على التسلسل الهرمي لمعدات الشبكة ومجموعات المنشآت والتي يشار إليها باسم "طبقات الأمان"، وهي: طبقة أمن البنية التحتية – طبقة أمن الخدمات – طبقة حماية التطبيقات (ITU,2009, 10).

ومن ناحية أخرى يتضمن الأمن السيبراني ثلاثة أبعاد هي (الصيدلاني، د.ت):

- **البعد الأول:** يشتمل على السرية، والنزاهة، والتوافر.
  - السرية: تمنع الكشف عن المعلومات للأشخاص أو الموارد أو العمليات غير المصرَّح بها.
  - النزاهة: تشير إلى دقة البيانات وتناسقها وموثوقيتها.
  - التوافر: يضمن إمكانية الوصول إلى المعلومات من قِبَل المستخدمين المصرَّح لهم عند الحاجة.
- **البعد الثاني:** ويتضمن حماية حالات البيانات في الفضاء الإلكتروني: البيانات في العبور، البيانات في التخزين، البيانات قيد المعالجة.
- **البعد الثالث:** وتشمل المهارات والتخصصات المستخدَمة لتوفير الحماية.
  - المهارة الأولى: تتضمن التقنيات والأجهزة والمنتجات المتاحة لحماية أنظمة المعلومات والتصدي لمجرمي الإنترنت.
  - المهارة الثانية: وضع السياسات والإجراءات والإرشادات التي تُمكِّن مستخدمي الفضاء الإلكتروني من البقاء آمنين.
  - المهارة الثالثة: الوعي بتهديدات الفضاء الإلكتروني وإنشاء ثقافة للتعلم.

كما صنف السمحان(٢٠٢٠، ١٥) أبعاد الأمن السيبراني إلى: الأبعاد العسكرية، والأبعاد السياسية، و الأبعاد الاقتصادية، والأبعاد القانونية.

ومما سبق يتضح أن للأمن السيبراني ثلاثة أبعاد هي: السرية والنزاهة والتوافر، حماية حالات البيانات في الفضاء الإلكتروني، بالإضافة إلى المهارات والتخصصات المستخدمة لتوفير الحماية.

رابعًا: أهمية الأمن السيبراني:

تزداد أهمية الأمن السيبراني بسبب الاعتماد المتزايد لأنظمة الكمبيوتر على الإنترنت والشبكات اللاسلكية (واي فاي، بلوتوث، الحوسبة السحابية) لتخزين المعلومات وتبادلها، وبسبب ظهور إنترنت الأشياء. وقد أثبتت التجارب الحديثة أن معظم التكنولوجيات عرضة للاختراق، بما في ذلك السيارات، وأنظمة الإنذار، والأجهزة الطبية القابلة للزرع، والبنية التحتية العامة لأنظمة الطيران، والتطبيقات المصرفية الهاتفية،

وتكنولوجيا المدن الذكية، وعمومًا يَسمح استخدام أدوات الحماية المناسبة بتسريع تقديم الخدمات والتنفيذ السلس للعمليات (لوران بروبست وآخرون،٢٠١٧، ١٢).

ويذكر ستيوارد وشيلينج فورد (Steward & Shilingford, 2011) الأهمية التربوية للأمن السيبراني كالتالي:

- ضمان سرية وخصوصية الوثائق التعليمية والحفاظ على سلامتها بشكل مستمر.
- متابعة ومراقبة وتطوير وضبط نظام المعلومات والأمن في المدرسة.
- حماية المعلمات والمدرسة من الهجمات السيبرانية في الفضاء السيبراني.

خامسًا: مجالات استخدام الأمن السيبراني:

يُستَخْدَم الأمن السيبراني في مجالات عديدة، من أهمها (السواط وآخرون، ٢٠٢٠):

١- حماية جميع الأجهزة الخاصة المحمولة والمعدات التقنية وكذلك وسائط التخزين من خطر الهجمات والاختراقات الإلكترونية والتدمير الجزئي أو الكلي.

٢- التعامل الآمِن مع خدمات تصفح الإنترنت من خلال نشر المعلومات والإجراءات التي تعمل على توعية الأفراد بخطورة الهجمات والجرائم الإلكترونية، ووسائل الاحتيال.

ويعمل الأمن السيبراني على حماية الأفراد من الأفكار المتعصبة والدخيلة على المجتمع، ومن تدمير الانتماء الوطني واختراق معلومات أمنية أو شخصية تؤثر على الدولة والمجتمع وغيرها من الأخطار، وتأتي هذه الحماية من خلال إستراتيجيات هامة تقوم بها الجهة المسئولة عن الأمن السيبراني في الدول في محاولة منها للتقليل من مخاطر الإنترنت في كافة مواقعه(السواط وآخرون، ٢٠٢٠).

وبناءً عليه فإن الأمن السيبراني يعمل على حماية كلٍّ من الفرد والأجهزة من خلال حماية الأجهزة الخاصة بالفرد والتعامل الآمن مع الخدمات التي تقدمها شبكة الإنترنت، بالإضافة إلى توعية الفرد بشأن الجرائم والهجمات السيبرانية.

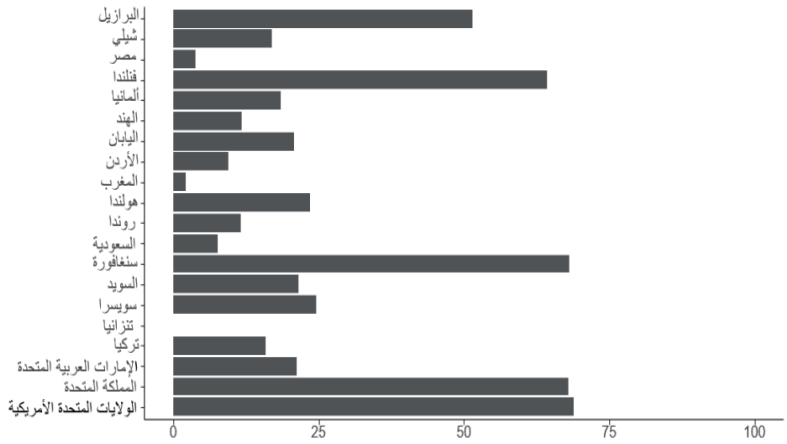
ويتضح من العرض السابق تزايد المخاطر السيبرانية كلما زادت هيمنة تكنولوجيا المعلومات والاتصالات على مستوى الحياة، وبذلك أصبحنا أمام جرائم حقيقية تتم عن طريق شبكة الإنترنت بأشكال مختلفة؛ كسرقة الأموال، والنصب والاحتيال، وكذلك

القرصنة باعتبارها الجريمة الأكثر شيوعًا في العالم الرقمي، وسيتم فيما يلي عرض بعض التجارب العربية والعالمية في مجال الأمن السيبراني .

سادسًا: بعض التجارب العالمية والعربية في مجال الأمن السيبراني:

تحتل الولايات المتحدة الأمريكية وسنغافورة والمملكة المتحدة وفنلندا المراكز الأولى في مجال الأمن السيبراني، وهذا يتوافق مع التداخل الموضوعي بين الذكاء الاصطناعي والأمن السيبراني؛ إذ يستخدم المطورون تكنولوجيا الذكاء الاصطناعي بصورة متزايدة كأداة لصقل قدرات تطبيقات الأمن السيبراني، في حين أن الالتزام بالمبادئ الأخلاقية للذكاء الاصطناعي يفترض إيجاد بيئة آمنة تسمح بتبادل المعلومات وتخزينها. وتتوافق هذه النتائج أيضًا مع المؤشر العالمي للأمن السيبراني الصادر عن الاتحاد الدولي للاتصالات في عام ٢٠١٧ الذي يشير إلى سنغافورة باعتبارها الدولة الأكثر التزامًا ببناء القدرات والتعاون والجاهزية الفنية في مجال الأمن السيبراني، فاعتماد الاقتصاد المحلي على التدفق السلس لرأس المال وحركة النقل الجوي وشحن البضائع جعل سنغافورة تشجع اعتماد أفضل الممارسات الإقليمية وتبادلها، حيث استضافت في عام ٢٠١٨ اجتماع رابطة أمم جنوب شرق آسيا. كما تبرز المسائل التنظيمية في فنلندا والمملكة المتحدة؛ حيث تتعلق النقاشات بتطبيق اللائحة العامة لحماية البيانات، وخاصةً مسئولية شبكات التواصل الاجتماعي عن المحافظة على خصوصية البيانات(لوران بروبست وآخرون ،٢٠١٧، ٣٨).

وتحتل البرازيل المرتبة الخامسة بين أفضل الدول أداءً على صعيد الأمن السيبراني، وهنا أيضًا تمثِّل المشكلات المتعلقة بالبيئة التمكينية للأمن السيبراني الغالبية العظمى من النشاط على الإنترنت، وإلى جانب اللائحة العامة لحماية البيانات تبرز القرصنة بشكل واضح في المناقشات على الإنترنت، وهذا ما يشير إلى تحول البرازيل إلى نقطة جذب للقراصنة الذين يستهدفون النظام المصرفي المحلي في البلاد. كما تعد البرازيل موطنًا لبرامج ضارة سيئة السمعة مثل (Trojans Bancos و ZeuS و SpyEye و CARBERP)؛ حيث بلغت الخسائر الناجمة عن سرقة بيانات بطاقات الائتمان وحدها ٢٢,٥ مليار دولار أمريكي في عام ٢٠١٧(لوران بروبست وآخرون ،٢٠١٧، ٣٨).



شكل (١)

مؤشر جاهزية الأمن السيبراني في ٢٠ دولة من دول العالم

المصدر: (لوران بروبست وآخرون، ٢٠١٧، ص ٣٨)

ومن الشكل السابق يتضح أن مصر تحتل المركز الثامن عشر من بين ٢٠ دولة من دول العالم في مجال الأمن السيبراني، وهذا يدل على أن هناك ضعف فى الوعي بالأمن السيبراني في المجتمع المصري.

وفيما يلي عرض لبعض التجارب العربية والعالمية في مجال الأمن السيبراني:

❖ **أستراليا (مركز الأمن السيبراني الأسترالي، ٢٠٢١):**

تم إنشاء مركز الأمن السيبراني في أستراليا Australian Cyber Security Center ، وهو مركز لدعم الأمن وتعزيزه في العصر الرقمي والتصدي للحوادث الرقمية والتبليغ عنها.

ويعد المعهد الأسترالي لبحوث الأمن السيبراني أول مركز أسترالي إستراتيجي منسق في مجال البحوث والتعليم بين الوكالات الحكومية والقطاع الخاص والباحثين عام ٢٠١٤، وهو يسعى إلى تركيز الحكومة على الأمن السيبراني من خلال الجمع بين شبكة تعاونية للتصدي للتهديدات السيبرانية وتحسين فرص تطوير مهنيين متخصصين في مجال الأمن السيبراني.

وتعاني أستراليا من نقص في مهارات الأمن السيبراني، وهذه المهارات الخاصة ضرورية في العالم المتصل بالتكنولوجيا إلا أنها تعاني من نقص في المعروض، وشهد المعهد عجزًا في مجال أمن المعلومات يبلغ ١.٥ مليون متخصص عام ٢٠٢٠.

ويلتزم المعهد بتزويد الأستراليين بمهارات الأمن السيبراني الصحيحة، ورفع مستويات الوعي الأمني الإلكتروني حتى يتمكن الجميع من الاستفادة من الفرص المتاحة في الفضاء السيبراني.

ويقدم المعهد تعليمًا أمنيًّا في المرحلة الجامعية والدراسات العليا من خلال منهج دراسي متسق وتعليم متميز، وتعمل الحكومة مع القطاع الخاص ومؤسسات خدمة الولايات والأقاليم على دعم التوسع في التدريب على الأمن السيبراني في منظمات التدريب ليشمل ذلك تطوير التدريب المهني على الأمن السيبراني، والتركيز على طلاب الجامعات.

❖ **الولايات المتحدة الأمريكية (المركز الوطني المتكامل لأبحاث التعليم السيبراني، ٢٠٢١):**

اهتمت الولايات المتحدة الأمريكية بتعزيز الأمن السيبراني من خلال المناهج الدراسية في البرامج المختلفة (بكالوريوس- ماجستير)، بالإضافة إلى جعل مقررات علوم الحاسب والأمن السيبراني جزءًا أساسيًّا من المناهج الدراسية في مختلف المراحل التعليمية، ويشرف على هذه المناهج المركز القومي لبحوث التعليم السيبراني المتكامل، وقد أُسِّسَ هذا المركز عام ٢٠١٦، وهو يسعى إلى تعزيز قدرات جميع المعلمين في مجال الأمن السيبراني، ودمج الطلبة لاستكشاف الفضاء السيبراني بكل أبعاده، وإعداد أجيال من الخريجين المتخصصين في مجالات العلوم والتكنولوجيا والرياضيات والهندسة والأمن السيبراني.

❖ **ماليزيا (مركز الأمن السيبراني الماليزي، ٢٠٢١):**

تعتبر تجربة ماليزيا من التجارب الرائدة في مجال الأمن السيبراني، ويلتزم مركز الأمن السيبراني في ماليزيا بتقديم مجموعة واسعة من الخدمات والبرامج والمبادرات التي يقودها الابتكار في مجال الأمن السيبراني لتقليل ضعف الأنظمة الرقمية، وفي الوقت نفسه تعزيز اعتماد ماليزيا على نفسها في الفضاء الإلكتروني.

وقد بدأت ماليزيا بتوظيف الأمن السيبراني في التعليم بغرض التوعية الأمنية عبر الإنترنت والتثقيف وتعزيز الوعي بشأن المشكلات التكنولوجية والاجتماعية التي تواجه مستخدمي الإنترنت، وخاصةً المخاطر التي تواجه مستخدمي الإنترنت، وقد استهدفت هذه المبادرة توعية الطلاب والأعضاء والمنظمات والمواقع الاجتماعية، وخصصت لكل منهم موقعًا على الإنترنت يصف مخاطر السيبرانية وكيفية الوقاية منها، ولأهمية الأمر تم وضع الأمن السيبراني في ماليزيا تحت إشراف وزير الاتصالات والوسائط المتعددة في ماليزيا اعتبارًا من ٢١ مايو ٢٠١٨.

❖ **المملكة العربية السعودية (الهيئة الوطنية للأمن السيبراني، ٢٠٢١):**

تعتبر تجربة المملكة العربية السعودية إحدى التجارب العربية الرائدة في مجال الأمن السيبراني؛ حيث حققت المرتبة الثانية من بين ١٩٣ دولة في العالم، والمركز الأول على مستوى الوطن العربي والشرق الأوسط وقارة آسيا في المؤشر العالمي للأمن السيبراني الذي تصدره وكالة الأمم المتحدة المتخصصة في تكنولوجيا المعلومات والاتصالات والاتحاد الدولي للاتصالات محققةً بذلك قفزة بـــ ١١ مرتبة عن العام ٢٠١٨، وبأكثر من ٤٠ مرتبة منذ إطلاق رؤية ٢٠٣٠ ؛ حيث كان ترتيبها ٤٦ عالميًّا في نسخة المؤشر للعام ٢٠١٧.

وقد تأسست الهيئة الوطنية للأمن السيبراني بتاريخ ١١/٢/ ١٤٣٩هـــ لتكون الجهة المختصة في المملكة بالأمن السيبراني، وهي تهدف إلى تعزيزه، وحماية الشبكات، وأنظمة تقنية المعلومات، وأنظمة التقنيات التشغيلية ومكوناتها من أجهزة وبرمجيات، وما تقدمه من خدمات، وما تحويه من بيانات من أي اختراق أو تعطيل أو تعديل أو دخول أو استخدام أو استغلال غير مشروع، كما يشمل هذا المفهوم أمن المعلومات والأمن الإلكتروني والأمن الرقمي، ونحو ذلك.

وقد تمت إضافة برامج في بعض الكليات خاصة بالأمن السيبراني، بالإضافة إلى إنشاء كلية الأمن السيبراني والبرمجة والذكاء الاصطناعي؛ حيث تسعى إلى بناء وتأهيل قدرات وطنية شابة محترفة بأحدث الوسائل التقنية التي يمكن من خلالها المساعدة في تحقيق أهداف رؤية ٢٠٣٠، والعمل على منافسة الدول المتقدمة وبالأخص في المجال السيبراني.

الجانب الميداني للبحث:

يتضمن الجانب الميداني للبحث: أهدافه، وأداة البحث، وكيفية إعدادها، وعينة البحث، ثم المعالجة الإحصائية للوصول إلى نتائج البحث ومناقشتها، وفيما يلي توضيح ذلك:

١- أهداف الجانب الميداني للبحث:

يهدف الجانب الميداني للبحث إلى تعرُّف درجة توافر وعي طلاب الدراسات العليا بجامعة القاهرة بمفهوم الأمن السيبراني، وطرق المحافظة عليه.

٢- أداة البحث:

صممت الاستبانة لتكون الأداة التي سيعتمد عليها البحث لتعرُّف درجة وعي طلاب الدراسات العليا بجامعة القاهرة بمفهوم الأمن السيبراني، وطرق المحافظة عليه.

٢-١ بناء أداة البحث:

مر بناء الاستبانة بالمراحل الآتية:

- الاطلاع على الأدبيات النظرية والدراسات والأبحاث الأجنبية ذات الصلة بموضوع البحث الحالي فيما يتعلق بالأمن السيبراني.
- صياغة العبارات المرتبطة بالأمن السيبراني والتي بلغت (٢٥) عبارة موزعة على محورين (مفهوم الأمن السيبراني- وطرق المحافظة على الأمن السيبراني)، وأمام كل عبارة ثلاث استجابات تقيس بمجملها درجة توافر الوعي. وقد قُدِّرَت استجابات أفراد العينة على عبارات الاستبانة وفقًا لمقياس ثلاثي متدرج على النحو التالي: **(عالية)**: تقدر بثلاث درجات، و**(متوسطة)**: تقدر بدرجتين، و**(منخفضة)**: تقدر بدرجة واحدة.
- وقد تم الاعتماد على مقياس ليكرت الثلاثي المكوَّن من ثلاث فئات للحصول على نتائج دقيقة من عينة البحث، وتم احتساب المدى كالتالي: (٣-١= ٢)، ثم تَمَّ تقسيمه على عدد خلايا المقياس للحصول على طول الخلية المطلوب، وذلك بالحساب التالي: (٢/ ٣= ٠.٦٧)، واعتمد المعيار على ثلاثة مستويات للحكم على مستوى إجابات أفراد عينة البحث حول

درجة توافر الوعي بمفهوم الأمن السيبراني وطرق المحافظة عليه كالتالي: تنخفض درجة توافر المعيار عندما يكون المتوسط الحسابي من ١ إلى أقل من ١.٦٧، وتكون متوسطة عندما يكون المتوسط الحسابي من ١.٦٧ إلى أقل من ٢.٣٣، وتكون عالية عندما يكون المتوسط الحسابي من ٢.٣٣ إلى ٣.

- تم عرض الاستبانة في صورتها الأولية على مجموعة من المحكَّمين من أعضاء هيئة التدريس المعنيين بهذا المجال لتعرُّف آرائهم حول دقة صياغة العبارات ودرجة ارتباطها بالمجال الخاص بها.
- في ضوء آراء السادة المحكَّمين تم وضع الاستبانة في صورتها النهائية، وتضمنت الاستبانة محورين:

✓ **الأول**: يتعلق بمفهوم الأمن السيبراني، وقد تم في هذا المحور عرض ١٠ عبارات، وهي: إدراك أهمية الأمن السيبراني، الإلمام بمفهوم الأمن السيبراني، الإلمام بمخاطر الهجمات الإلكترونية، لديَّ معرفة بمخاطر فتح روابط ومرفقات البريد الإلكتروني، لديَّ معرفة بمخاطر فيروسات الهواتف الذكية، لديَّ معرفة بالإجراءات اللازمة لحماية نظم المعلومات من الاختراق، لديَّ معرفة بمفهوم الاحتيال الالكتروني، لديَّ معرفة تامة بمخاطر تنزيل البرامج والملفات من الإنترنت، لديَّ إلمام بطرق المحافظة على الأمن السيبراني، أحتاج إلى دورات تدريبية في الأمن السيبراني.

✓ **الثاني**: أشار إلى طرق المحافظة على الأمن السيبراني، وقد تم في هذا المحور عرض ١٥ عبارة جاءت كالتالي: استخدام برنامج للحماية من الفيروسات بصورة مستمرة، أقوم بتحديث برنامج الحماية من الفيروسات بصورة مستمرة، أفحص جهاز الحاسب الآلي بصورة منتظمة، استخدام جدار الحماية على جهاز الحاسوب الخاص بك، أقوم بتحديث نظام التشغيل بصورة دورية، أقوم بعمل نسخة احتياطية للملفات المهمة، أفتح رسالة إلكترونية غير معروفة لديَّ، أقوم بالرد عندما تصلني رسالة بريد إلكتروني عن الفوز بجائزة نقدية، أتسوق أو أشتري سلعة مُعْلَن عنها في مواقع

التواصل الاجتماعي، أعلم الخصائص اللازمة لإنشاء كلمة مرور جيدة عند الدخول للمواقع على الإنترنت، استخدام نفس كلمة المرور لجميع مواقع التواصل الاجتماعي والبريد الإلكتروني وإجراء عمليات مالية مثل مواقع البنوك أو التسوق الإلكتروني، لديَّ معرفة بخطورة إرسال كلمة المرور عبر البريد الإلكتروني، أقوم بقراءة شروط وتعليمات المستخدم لبرنامج مجاني قبل الضغط على أوافق، أقوم بتغيير كلمة المرور بانتظام، أقوم بإعداد نسخة احتياطية للبيانات المخزَّنة في جهازي.

- كما اشتملت الاستمارة على جزء يتعلق بالبيانات الأساسية ، ومنها: الدرجة العلمية المقيَّد بها طالب الدراسات العليا بكلية الدراسات العليا للتربية بجامعة القاهرة، والتخصص.

٢-٢ تقنين أداة البحث:

تم التقنين أداة البحث (الاستبانة) من خلال التحقق من الصدق والثبات على النحو التالي:

(أ) صدق الاستبانة:

تم التحقق من صدق الاستبانة من خلال صدق المحكَّمين؛ حيث تم عرض الاستبانة في صورتها الأولية كأداة لجمع البيانات على أساتذة متخصصين في المجال التربوي بهدف استطلاع آرائهم حول دقة الصياغة اللغوية لفقرات الاستبانة، ووضوح تلك الصياغة وسلامتها، ومدى انتماء كل فقرة إلى المحور الذي أدرجت فيه، وبعد ذلك تَمَّ إجراء ما يلزم من تعديلات في ضوء آراء السادة المحكمين.

(ب) ثبات الاستبانة:

تم حساب معامل الثبات عن طريق معامل ثبات " ألفا كرونباخ" لكل محور من محاور الاستبانة، وللاستبانة كاملةً، وجاءت النتائج كما هو موضح في الجدول التالي رقم (١):

جدول (١)

معامل الثبات لأبعاد كل محور من محاور الاستبانة، وللاستبانة كاملةً باستخدام معامل "ألفا كرونباخ"

محاور الاستبانة	عدد الفقرات	قيم معامل ألفا كرونباخ
مفهوم الأمن السيبراني	١٠	٠.٨٦٣
طرق المحافظة على الأمن السيبراني	١٥	٠.٨٣٨
الاستبانة كاملة	٢٥	٠.٨٥

وتشير نتائج جدول (١) إلى أن قيمة معامل الثبات (ألفا كرونباخ) في الاستبانة كاملةً كانت ٠.٨٥ ، وهي قيمة مقبولة تشير إلى تجانس عبارات الاستبانة، وإلى أنَّ الأداة المستخدَمة تتمتع بثبات عالٍ، وتؤكد تلك النتائج صلاحية الاستبانة ومناسبتها لتحقيق أهداف البحث الحالي.

٣- مجتمع وعينة البحث:

تألَّف مجتمع البحث الذي اشتُقَّت منه عينة البحث من طلاب الدراسات العليا بكلية الدراسات العليا بجامعة القاهرة في العام الدراسي ٢٠٢٠/ ٢٠٢١، وقد بلغ عدد الطلاب عينة البحث (٩٣) طالبًا في التخصصات الآتية: (أصول التربية – المناهج وطرق التدريس– علم النفس التربوي– علم النفس الإرشادي– تكنولوجيا التعليم– التعليم العالي والتعليم المستمر– التربية الخاصة– دراسات الطفولة)، وقد تم اختيارهم بطريقة عشوائية بنسبة (٢٣.٣٦%) من المجتمع الأصلي للطلاب البالغ (٣٩٨) طالبًا.

ويوضح جدول (٢) توزيع أفراد العينة (طلاب الماجستير والدكتوراه) حسب متغيرات الدرجة العلمية والنوع في مجال الأمن السيبراني الذين تم إجراء البحث عليهم:

جدول (٢)

توزيع أفراد العينة حسب متغيرات الدرجة العلمية والنوع في مجال الأمن السيبراني

المتغيرات	الفئات	التكرار	النسبة المئوية للطلاب %
الدرجة العلمية	ماجستير	٤٦	٤٩.٥
	دكتوراه	٤٧	٥٠.٥
النوع	ذكر	٢٦	٢٨
	أنثى	٦٧	٧٢

ويتضح من جدول (٢) أن نسبة الطلاب الذكور بلغت (٢٨%)، بينما بلغت نسبة الطالبات (٧٢%)، ويرجع ذلك إلى أن أعداد الطالبات المتقدمات للدراسات العليا بالماجستير والدكتوراه أعلى من أعداد الطلاب المتقدمين، أما بخصوص الدرجة العلمية فقد بلغت نسبة الطلاب المقيدين بالماجستير (٤٩.٥%)، بينما بلغت نسبة الطلاب المقيدين بالدكتوراه (٥٠.٥%).

٤- المعالجة الإحصائية:

تم إدخال البيانات الخاصة باستمارة الاستبيان على برنامج " Spss for window " المستخدم في تحليل البحوث الاجتماعية وأنواع الأسئلة المختلفة في استمارة الاستبيان، وقد فرضت الأهداف التي يسعى البحث إلى تحقيقها الجمع بين التحليلين الكمي والكيفي للبيانات، فاعتمد التحليل الكمي على حساب التكرارات واستخدام المتوسط الحسابي، واستخراج النسب المئوية، والانحراف المعياري، وجاء التحليل الكيفي للنتائج من خلال ربط نتائج البحث الحالي بنتائج الدراسات السابقة وما تم عرضه في الإطار النظري للبحث، وذلك لبيان النتائج العامة للبحث والتوصل إلى تصور مقترح لدور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني في ضوء خبرات بعض الدول.

٥- نتائج البحث الميداني وتفسيرها:

بعد إجراء المعالجات الإحصائية لبيانات البحث يمكن عرض نتائج البحث الميداني وتفسيرها على النحو التالي:

- **أولًا:** النتائج الخاصة بآراء أفراد العينة حول درجة وعيهم بمفهوم الأمن السيبراني، وتفسيرها.
- **ثانيًا:** النتائج الخاصة بآراء أفراد العينة حول درجة وعيهم بطرق المحافظة على الأمن السيبراني وتفسيرها.

وفيما يلي عرض لتلك النتائج:

أولًا: النتائج الخاصة بآراء أفراد العينة حول الوعي بمفهوم الأمن السيبراني:

توضح هذه النتائج وعي الطلاب بمفهوم الأمن السيبراني، وقد جاءت كما يلي:

جدول (٣)

التكرارات والمتوسطات الحسابية والانحرافات المعيارية والترتيب

حول درجة توافر وعي أفراد العينة بمفهوم الأمن السيبراني

الاستجابات / العبارة	التكرارات والنسبة المئوية	عالية	متوسطة	منخفضة	المتوسط الحسابي	الانحراف المعياري	الترتيب	درجة الوعي
١- إدراك أهمية الأمن السيبراني.	ك	٢٨	٣٤	٣١	١.٩٦٧	٠.٨٠٠	٨	متوسطة
	%	٣٠.١	٣٦.٦	٣٣.٣				
٢- الإلمام بمفهوم الأمن السيبراني.	ك	١٨	٣٨	٣٧	١.٧٩٥	٠.٧٤٥	٩	متوسطة
	%	١٩.٤	٤٠.٩	٣٩.٨				
٣- الإلمام بمخاطر الهجمات الإلكترونية.	ك	٤٤	٣٩	١٠	٢.٣٦٥	٠.٦٧٢	٢	مرتفعة
	%	٤٧.٣	٤١.٩	١٠.٨				
٤- لديَّ معرفة بمخاطر فتح روابط ومرفقات البريد الإلكتروني.	ك	٣٩	٤٠	١٤	٢.٢٦٨	٠.٧٠٩	٤	متوسطة
	%	٤١.٩	٤٣	١٥.١				
٥- لديَّ معرفة بمخاطر فيروسات الهواتف الذكية.	ك	٤٤	٣٩	١٠	٢.٣٦٥	٠.٦٧٢	٢	مرتفعة
	%	٤٧.٣	٤١.٩	١٠.٨				
٦- لديَّ معرفة بالإجراءات اللازمة لحماية نظم المعلومات من الاختراق.	ك	٣٧	٣٨	١٨	٢.٢٠٤	٠.٧٤٥	٥	متوسطة
	%	٣٩.٨	٤٠.٩	١٩.٤				
٧- لديَّ معرفة بمفهوم الاحتيال الإلكتروني.	ك	٢٦	٤٤	٢٣	٢.٠٣٢	٠.٧٢٩	٧	متوسطة
	%	٢٨	٤٧.٣	٢٤.٧				
٨- لديَّ معرفة تامة بمخاطر تنزيل البرامج والملفات من الإنترنت.	ك	٣٠	٤٣	٢٠	٢.١٠٧	٠.٧٢٩	٦	متوسطة
	%	٣٢.٣	٤٦.٢	٢١.٥				
٩- لديَّ إلمام بطرق المحافظة على الأمن السيبراني.	ك	٧	٤٥	٤١	١.٦٣٤	٠.٦٢١	١٠	منخفضة
	%	٧.٤	٤٧.٤	٤٣.٢				
١٠- أحتاج إلى دورات تدريبية في الأمن السيبراني.	ك	٥٧	٢٥	١١	٢.٤٩٤	٠.٧٠١	١	مرتفعة
	%	٦١.٣	٢٦.٩	١١.٨				
المستوى العام لمحور مفهوم الأمن السيبراني					٢.١٢٣	٠.٧١٢	متوسط	

ويوضح جدول (٣) المتوسطات الحسابية للفقرات الخاصة بآراء أفراد العينة حول الوعي بمفهوم الأمن السيبراني؛ حيث تراوحت بين (١.٦٣٤- ٢.٤٩٤)، بمتوسط عام للمحور (٢.١٢٣)، ويدل ذلك على أن مستوى محور الوعي بمفهوم الأمن السيبراني بشكل عام متوسط، وقد جاءت العبارة رقم (١٠) والتي تنص على: " أحتاج إلى دورات تدريبية في الأمن السيبراني " في المرتبة الأولى بمتوسط (٢.٤٩٤)، وبدرجة وعي مرتفعة ، ويرجع ذلك إلى حاجة الطلاب الفعلية إلى دورات تدريبية تخص الأمن السيبراني، وأنه أمر بالغ الأهمية لحماية خصوصياتهم، ووعيهم بأن أجهزتهم غير آمنة، وضرورة اتخاذ التدابير اللازمة لحماية أجهزتهم من الاختراق من خلال دخلاء للوصول إلى بيانات المستخدم الشخصية من خلال ثغرات، وهذا ما أوصت به دراسة فاطمة المنتشري (٢٠٢٠) التي أكدت على أهمية عقد دورات تدريبية للمعلمات في مجال الأمن السيبراني، وجاءت العبارة رقم (٣) والتي تنص على: " الإلمام بمخاطر الهجمات الإلكترونية"، والعبارة رقم (٥) والتي تنص على: "لديَّ معرفة بمخاطر فيروسات الهواتف الذكية" في المرتبة الثانية بمتوسط حسابي (٢.٣٦٥)، وبدرجة وعي مرتفعة، ويرجع ذلك إلى وعي وإلمام الطلاب بوجود فيروسات تهاجم هواتفهم الشخصية، وهذا ما أكدت عليه دراسة كوغلينج (٢٠١٨) وموسكال (٢٠١٥) اللتان أكدتا على خطر الانتهاكات والمخاطر السيبرانية، وجاءت العبارة (٤) والتي تنص على: " لديَّ معرفة بمخاطر فتح روابط ومرفقات البريد الإلكتروني" في المرتبة الرابعة بمتوسط (٢.٢٦٨)، وبدرجة وعي متوسطة، ويرجع ذلك إلى خبرة بعض الطلاب بنتيجة فتح هذه الروابط، وما يؤدي إليه ذلك من مهاجمة هواتفهم الشخصية، أما العبارة رقم (٦) والتي تنص على: " لديَّ معرفة بالإجراءات اللازمة لحماية نظم المعلومات من الاختراق" فقد جاءت في المرتبة الخامسة بمتوسط حسابي (٢.٢٠٤) وبدرجة وعي متوسطة، وهذا ما أكدت عليه دراسة نورة القحطاني (٢٠١٩) من خلال أهم طرق الوقاية المجتمعية لمشكلات الفضاء السيبراني، أما العبارة رقم (٨) والتي تنص على: " لديَّ معرفة تامة بمخاطر تنزيل البرامج والملفات من الإنترنت" فقد جاءت في المرتبة السادسة بمتوسط (٢.١٠٧)، وبدرجة وعي متوسطة، ويرجع ذلك إلى ضعف وعي بعض الطلاب بخطورة تنزيل

البرامج والملفات من شبكة الإنترنت والتعامل معها، أما العبارة رقم (٧) والتي تنص على: " لديَّ معرفة بمفهوم الاحتيال الإلكتروني " فقد جاءت في المرتبة السابعة بمتوسط (٢.٠٣٢)، وبدرجة وعي متوسطة، ولذلك فإنه يجب تنمية وعي الطلاب بمعنى الانتحال الإلكتروني وتعرُّف صوره المختلفة، وذلك من خلال عرض بعض الأفلام التي توضح ذلك، وهذ ما أكدت عليه دراسة نينكيو وآخرين (٢٠١٨) والتي أوصت بضرورة التركيز على المفاهيم الأخلاقية المتعلقة باستخدام شبكة الإنترنت، أما العبارة رقم (١) والتي تنص على:" إدراك أهمية الأمن السيبراني " فقد جاءت في المرتبة الثامنة، بمتوسط (١.٩٦٧)، وبدرجة وعي متوسطة، ويرجع ذلك إلى ضعف وعي الطلاب بأن التكنولوجيا عرضة للاختراق بما في ذلك السيارات وأنظمة الإنذار والتطبيقات المصرفية، وهذا ما أكدت عليه دراسة فاطمة المنتشري (٢٠٢٠) ودراسة الصحفي وعسكول (٢٠١٩)، أما العبارة رقم (٢) والتي تنص على: " الإلمام بمفهوم الأمن السيبراني" فقد جاءت في المرتبة التاسعة، بمتوسط (١.٧٩٥)، وبدرجة وعي متوسطة، وهذ ما أكدت عليه دراسة بوسي وساديرا (٢٠١١) من حيث ضرورة الإلمام بمفهوم الأمن السيبراني، أما العبارة رقم (٩) والتي تنص على: " لديَّ إلمام بطرق المحافظة على الأمن السيبراني " فقد جاءت في المرتبة العاشرة والأخيرة بمتوسط حسابي (١.٦٣٤)، وبدرجة وعي منخفضة، ويرجع ذلك إلى ضعف وعي الطلبة بطرق المحافظة على الأمن السيبراني، بالإضافة إلى وجود تقصير من قِبَل المؤسسات التعليمية في القيام بدورها التوعوي، وهذا ما أكدت عليه دراسة الرفاعي (٢٠١٨) من حيث ضرورة إعداد قوانين للحد من مشكلة التنمر الإلكتروني، وإعداد برامج توعوية لتثقيف أفراد المجتمع بحقوقهم وواجباتهم في استخدام التكنولوجيا.

ثانيًا: النتائج الخاصة بآراء أفراد العينة حول درجة الوعي بطرق المحافظة على الأمن السيبراني:

توضح هذه النتائج آراء أفراد العينة حول طرق المحافظة على الأمن السيبراني، وقد جاءت النتائج كالتالي:

جدول (٤)

التكرارات والمتوسطات الحسابية والانحرافات المعيارية والترتيب

حول درجة توافر وعي أفراد العينة بطرق المحافظة على الأمن السيبراني

العبارة / الاستجابات	التكرارات والنسبة المئوية	عالية	متوسطة	منخفضة	المتوسط الحسابي	الانحراف المعياري	الترتيب	درجة الوعي
١- استخدام برنامج للحماية من الفيروسات بصورة مستمرة.	ك	٤٢	٣٠	٢١	٢.٢٢٥	٠.٧٩٥	٥	متوسطة
	%	٤٥.٢	٣٢.٣	٢٢.٦				
٢- أقوم بتحديث برنامج الحماية من الفيروسات بصورة مستمرة.	ك	٢٩	٤١	٢٣	٢.٠٦٤	٠.٧٤٩	٦	متوسطة
	%	٣١.٢	٤٤.١	٢٤.٧				
٣- أفحص جهاز الحاسب الآلي بصورة منتظمة.	ك	٣٠	٣٦	٢٧	٢.٠٣٢	٠.٧٨٦	٨	متوسطة
	%	٣٢.٣	٣٨.٧	٢٩				
٤- استخدام جدار الحماية على جهاز الحاسوب الخاص بك.	ك	٣٢	٣٣	٢٨	٢.٠٤٣	٠.٨٠٦	٧	متوسطة
	%	٣٤.٤	٣٥.٥	٣٠.١				
٥- أقوم بتحديث نظام التشغيل بصورة دورية.	ك	٢٥	٣٦	٣٢	١.٩٢٤	٠.٧٨٣	١٠	متوسطة
	%	٢٦.٩	٣٨.٧	٣٤.٤				
٦- أقوم بعمل نسخة احتياطية للملفات المهمة.	ك	٤٣	٣١	١٩	٢.٢٥٨	٠.٧٧٨	٤	متوسطة
	%	٤٦.٢	٣٣.٣	٢٠.٤				
٧- أفتح رسالة إلكترونية غير معروفة لديَّ.	ك	٩	٢٦	٥٨	١.٤٧٣	٠.٦٦٩	١٤	منخفضة
	%	٩.٧	٢٨	٦٢.٤				
٨- أقوم بالرد عندما تصلني رسالة بريد إلكتروني عن الفوز بجائزة نقدية.	ك	٣	١٠	٨٠	١.١٧٢	٠.٧٥٧	١٥	منخفضة
	%	٣.٢	١٠.٨	٨٦				
٩- أتسوق أو أشتري سلعة معلنًا عنها في مواقع التواصل الاجتماعي.	ك	٦	٤٢	٤٥	١.٥٨٠	٠.٦١٣	١٣	منخفضة
	%	٦.٥	٤٥.٢	٤٨.٤				

العبارة / الاستجابات	التكرارات والنسبة المئوية	عالية	متوسطة	منخفضة	المتوسط الحسابي	الانحراف المعياري	الترتيب	درجة الوعي
١٠- أعلم الخصائص اللازمة لإنشاء كلمة مرور جيدة عند الدخول للمواقع على الإنترنت.	ك	٤٢	٣٥	١٦	٢.٢٧٩	٠.٧٤٢	٢	متوسطة
	%	٤٥.٢	٣٧.٦	١٧.٢				
١١- استخدام نفس كلمة المرور لجميع مواقع التواصل الاجتماعي والبريد الإلكتروني وإجراء عمليات مالية على مواقع البنوك أو التسوق الإلكتروني.	ك	١٤	٣٦	٤٣	١.٦٨٨	٠.٧٢١	١١	متوسطة
	%	١٥.١	٣٨.٧	٤٦.٢				
١٢- لديّ معرفة بخطورة إرسال كلمة المرور عبر البريد الإلكتروني.	ك	٤٩	٢٢	٢٢	٢.٢٩٠	٠.٨٢٨	١	متوسطة
	%	٥٢.٧	٢٣.٧	٢٣.٧				
١٣- أقوم بقراءة شروط وتعليمات المستخدم لبرنامج مجاني قبل الضغط على "أوافق".	ك	٢٧	٣٩	٢٧	٢	٠.٧٦٦	٩	متوسطة
	%	٢٩	٤٢	٢٩				
١٤- أقوم بتغيير كلمة المرور بانتظام.	ك	١٤	٣٤	٤٥	١.٦٦٦	٠.٧٢٧	١٢	منخفضة
	%	١٥.١	٣٦.٦	٤٨.٤				
١٥- أقوم بإعداد نسخة احتياطية للبيانات المخزنة في جهازي.	ك	٤١	٣٦	١٦	٢.٢٦٨	٠.٧٣٩	٣	متوسطة
	%	٤٤.١	٣٨.٧	١٧.٢				
المستوى العام لمحور طرق المحافظة على الأمن السيبراني					١.٩٣٠	٠.٧٥٠		متوسطة

ويوضح جدول (٤) المتوسطات الحسابية للفقرات الخاصة بآراء أفراد العينة حول الوعي بطرق المحافظة على الأمن السيبراني؛ حيث تراوحت بين (١.١٧٢- ٢.٢٩٠)، بمتوسط عام للمحور (١.٩٣٠)، ويدل ذلك على أن مستوى محور الوعي بطرق المحافظة على الأمن السيبراني بشكل عام متوسط، وقد جاءت العبارة (١٢) والتي تنص على: " لديَّ معرفة بخطورة إرسال كلمة المرور عبر البريد الإلكتروني" في المرتبة الأولى بمتوسط (٢.٢٩٠)، وبدرجة وعي متوسطة، ويرجع ذلك إلى التطور التكنولوجي الذي فرض على الطلاب التعامل في السنوات الأخيرة من خلال البريد الإلكتروني بينهم وبين أعضاء هيئة التدريس، فجعلهم على حذر وتخوف من إرسال كلمة المرور الخاصة بالبريد الشخصي لهم، وجاءت العبارة (١٠) والتي تنص على: " أعلم الخصائص اللازمة لإنشاء كلمة مرور جيدة عند الدخول للمواقع على الإنترنت" في المرتبة الثانية بمتوسط حسابي (٢.٢٧٩)، وبدرجة وعي متوسطة، ويرجع ذلك إلى قراءة التعليمات الخاصة بإنشاء كلمة المرور بحيث تكون قوية أو متوسطة، وتوضيح درجة قوة كلمة المرور مما يدل على وعي الطلاب بالأمن السيبراني في مجال حماية الأجهزة الخاصة والمحمولة من مخاطر الاختراق الإلكتروني والهجمات السيبرانية، وهذا ما أكدت عليه دراسة الصحفي وعسكول (٢٠١٩)، وجاءت العبارة (١٥) والتي تنص على: " أقوم بإعداد نسخة احتياطية للبيانات المخزنة في جهازي" في المرتبة الثالثة بمتوسط (٢.٢٦٨)، وبدرجة وعي متوسطة، ويرجع ذلك إلى تخوف الطلاب من فقدان بياناتهم، لذلك فإنهم يقومون بعمل نسخة احتياطية للبيانات مما يدل على وعي الطلاب بحماية البيانات من مخاطر الاختراق، أما العبارة رقم (٦) والتي تنص على: " أقوم بعمل نسخة احتياطية للملفات المهمة" فقد جاءت في المرتبة الرابعة بمتوسط حسابي (٢.٢٥٨) وبدرجة وعي متوسطة، ويرجع ذلك إلى فقد الكثير من بيانات الطلاب المخزنة على أجهزتهم، ولذلك فإنهم بدءوا في عمل نسخ احتياطية لكل بياناتهم بصورة مستمرة خوفًا من فقدها، أما العبارة رقم (١) والتي تنص على: " استخدام برنامج للحماية من الفيروسات بصورة مستمرة" فقد جاءت في المرتبة الخامسة بمتوسط (٢.٢٢٥)، وبدرجة وعي متوسطة، والعبارة رقم (٢) والتي تنص على: " أقوم بتحديث برنامج الحماية من الفيروسات بصورة مستمرة" فقد جاءت في المرتبة السادسة بمتوسط (٢.٠٦٤)، وبدرجة وعي

متوسطة، ويرجع ذلك إلى وعي الطلاب بحماية الأجهزة الخاصة والمحمولة من مخاطر الاختراق الإلكتروني، وهذا ما أكدت عليه دراسة السواط وآخرين (٢٠٢٠) من ارتفاع درجة الوعي بالأمن السيبراني في مجال التعامل الآمن مع خدمات تصفح الإنترنت لدى الطلاب، والعمل على تأمين أجهزتهم من مخاطر الاختراق أو انتهاك أمن معلوماتهم، أما العبارة رقم (٤) والتي تنص على:" استخدام جدار الحماية على جهاز الحاسوب الخاص بك " فقد جاءت في المرتبة السابعة، بمتوسط (٢.٠٤٣)، وبدرجة وعي متوسطة، وأما العبارة رقم (٣) والتي تنص على: " أفحص جهاز الحاسب الآلي بصورة منتظمة" فقد جاءت في المرتبة الثامنة، بمتوسط (٢.٠٣٢)، وبدرجة وعي متوسطة، وأما العبارة رقم (١٣) والتي تنص على: "أقوم بقراءة شروط وتعليمات المستخدم لبرنامج مجاني قبل الضغط على "أوافق" " فقد جاءت في المرتبة التاسعة بمتوسط حسابي (٢) بدرجة وعي متوسطة، ويرجع ذلك إلى تكاسل الطلاب عن قراءة التعليمات لتنزيل وتثبيت أي برنامج على الأجهزة، أما العبارة رقم (٥) والتي تنص على:" أقوم بتحديث نظام التشغيل بصورة دورية" فقد جاءت في المرتبة العاشرة، بمتوسط (١.٩٢٤)، وبدرجة وعي متوسطة، وأما العبارة رقم (١١) والتي تنص على:" استخدام نفس كلمة المرور لجميع مواقع التواصل الاجتماعي والبريد الإلكتروني وإجراء عمليات مالية على مواقع البنوك أو التسوق الإلكتروني" فقد جاءت في المرتبة الحادية عشرة، بمتوسط (١.٦٨٨)، وبدرجة وعي متوسطة، ويرجع ذلك إلى خوف الطلاب من نسيان كلمة المرور، ويسبب ذلك مشاكل عدة خاصةً أثناء إجراء المعاملات المالية ويسهل عملية الاختراق، لذلك فهم في حاجة إلى تعزيز الوعي لديهم بمخاطر ذلك، وأما العبارة رقم (١٤) والتي تنص على: " أقوم بتغيير كلمة المرور بانتظام فقد جاءت في المرتبة الثانية عشرة، بمتوسط (١.٦٦٦)، وبدرجة وعي منخفضة، ويرجع ذلك إلى الحاجة إلى رفع الوعي بمخاطر الهجمات السيبرانية نظرًا لعدم تغيير كلمة المرور، وهذا ما أكدت عليه دراسة فاطمة المنتشري (٢٠٢٠)، وأما العبارة رقم (٩) والتي تنص على: " أتسوق أو أشتري سلعة معلنًا عنها في مواقع التواصل الاجتماعي" فقد جاءت في المرتبة الثالثة عشرة، بمتوسط (١.٥٨٠)، وبدرجة وعي منخفضة، ويرجع ذلك إلى ضعف الوعي بعملية الشراء الإلكتروني والخوف من السرقات، وهذا ما أكدت عليه دراسة نورة القحطاني (٢٠١٩)، أما العبارة

رقم (٧) والتي تنص على: " أفتح رسالة إلكترونية غير معروفة لديَّ" فقد جاءت في المرتبة الرابعة عشرة، بمتوسط (١.٤٧٣)، وبدرجة وعي منخفضة، وهذا ما أكدته دراسة الصحفي وعسكول (٢٠١٩)، أما العبارة رقم (٨) والتي تنص على: " أقوم بالرد عندما تصلني رسالة بريد إلكتروني عن الفوز بجائزة نقدية" فقد جاءت في المرتبة الخامسة عشرة، بمتوسط (١.١٧٢)، وبدرجة وعي منخفضة، ويرجع ذلك إلى حاجة الطلاب إلى رفع الوعي بمخاطر ذلك والتأكد من مصادر رسائل البريد الإلكتروني، وهذا ما أكدت عليه دراسة الصحفي وعسكول (٢٠١٩).

التصور المقترح لدور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني في ضوء خبرات بعض الدول:

من خلال ما تم عرضه من إطار نظري شمل الإطار المفاهيمي للأمن السيبراني، وأهميته، وأهدافه، ومجالات استخدامه، ثم عرض خبرات بعض الدول في الأمن السيبراني، ثم ما تم التوصل إليه من نتائج في الجانب الميداني للبحث من طلاب جامعة القاهرة عينة البحث ظهرت الحاجة إلى الانطلاق لتحديد التصور المقترح لدور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني في ضوء خبرات بعض الدول والذي يعتمد على العديد من العناصر، وهي: منطلقات التصور المقترح وأهدافه، ثم المحتوى، وآليات تنفيذه، ومعوقات التنفيذ، وأخيرًا سبل التغلب على المعوقات، وسوف نعرض هذا فيما يلي تفصيلًا:

١- منطلقات التصور المقترح:

- الإستراتيجية الوطنية للأمن السيبراني ٢٠١٧/ ٢٠٢١ التي أصدرها المجلس الأعلى للأمن السيبراني.
- "أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه على النحو الذي ينظمه القانون"، مادة (٣١) من الدستور المصري (يناير، ٢٠١٤).
- أهمية الأمن السيبراني الذي يعتمد على أنظمة الكمبيوتر على الإنترنت، والشبكات اللاسلكية، والحوسبة السحابية لتخزين المعلومات وتبادل ظهورها.

- دور الجامعة في توعية الطلاب من خلال وظائفها المختلفة كالتدريس، والبحث العلمي، وخدمة المجتمع.

٢- أهداف التصور المقترح:

يرتكز الهدف الأساسى على دور جامعة القاهرة في توعية طلاب الدراسات العليا بالأمن السيبراني في ضوء خبرات بعض الدول بحيث تقدم توعية لفئة عمرية بحاجة إلى بيئة آمنة بهدف التصدي لهجمات وحوادث أمن المعلومات، والحد من التخريب الإلكتروني في المجتمع، ويتفرع من هذا الهدف العام بعض الأهداف الفرعية، وهي:

- حماية الأنظمة التقنية المختلفة في الجامعة.
- التصدي للهجمات ومخاطر أمن المعلومات في الجامعة.
- الحد من المخاطر والجرائم السيبرانية التي تستهدف الطلاب.
- الحد من التخريب الإلكتروني على مستوى الجامعة ووزارة التعليم العالي.
- توعية طلاب الدراسات العليا بمخاطر الهجمات السيبرانية وكيفية التصدي لها.

٣- محتوى التصور المقترح:

بعد تحديد منطلقات التصور المقترح وأهدافه اتضحت الحاجة إلى تحديد محتواه، وذلك من خلال محاور أساسية تشمل التدريس، والبحث العلمي، وخدمة المجتمع، وفيما يلي عرض لهذه المحاور بالتفصيل:

- **المحور الأول: توعية طلاب الدراسات العليا بالأمن السيبراني من خلال التدريس:**
  - إدراج بعض المفاهيم عن الأمن السيبراني في المناهج والمقررات.
  - ضرورة توفير مقررات دراسية تتعلق بالأمن السيبراني في جميع الكليات تهدف إلى تعليم الطلاب أساسيات الحماية.
  - استحداث برامج عن الأمن السيبراني لطلاب الدراسات العليا بجامعة القاهرة.
  - استحداث مقرر في برامج إعداد المعلم في كلية التربية عن الأمن السيبراني للتوعية بالانتهاكات السيبرانية.
  - إدراج مقرر إجباري حول الأمن السيبراني ضمن الخطة الدراسية لكافة البرامج التعليمية لجميع طلاب المرحلة الجامعية لتعزيز الثقافة السيبرانية.
- **المحور الثاني: توعية طلاب الدراسات العليا بالأمن السيبراني من خلال البحث العلمي:**

- تشجيع أعضاء هيئة التدريس والباحثين بالكليات المختلفة على القيام بالبحوث العلمية في مجال الأمن السيبراني.
- توفير برامج أكاديمية للدراسات العليا في مجال الأمن السيبراني مثل برامج الماجستير والدكتوراه.
- ضرورة تحقُّق طلاب الدراسات العليا من مصداقية المعلومات المتداوَلة على شبكة الإنترنت.
- توعية الطلاب بعمل نسخة احتياطية من الرسالة العلمية في ذاكرة خارجية.

- **المحور الثالث: توعية طلاب الدراسات العليا بالأمن السيبراني من خلال خدمة المجتمع:**

- إنشاء مركز للأمن السيبراني في الجامعة، وتتفرع منه وحدة خاصة بكل كلية من كليات الجامعة.
- تقديم برامج تدريبية في مجال مكافحة جرائم الحاسب الآلي، والجرائم المعلوماتية لأعضاء هيئة التدريس والعاملين بالجامعة.
- عقد ورش عمل لطلاب الدراسات العليا حول إجراءات الحماية ضد المخاطر والانتهاكات السيبرانية.
- عقد ندوات علمية لنشر ثقافة الأمن السيبراني بالجامعة.
- عقد شراكة بين الجامعة ووزارة الإعلام لعمل حملات إعلامية لتوعية المجتمع بصفة عامة، والطلاب بصفة خاصة للوقاية من مشكلات الأمن السيبراني.
- عقد مؤتمر سنوي بالجامعة عن أمن المعلومات بهدف توعية الطلاب وأعضاء هيئة التدريس والعاملين بالجامعة نحو الأمن السيبراني.

٤- آليات تنفيذ التصور المقترح :

تتمثل آليات تنفيذ التصور المقترح فيما يلي:

- تَبَنِّي الجامعة فكرة الأمن السيبراني من خلال إتاحة مقررات وبرامج عن الأمن السيبراني.
- نشر ثقافة الأمن السيبراني على مستوى طلاب الجامعات.

- إقامة ندوات ومؤتمرات تؤكد على أهمية الأمن السيبراني، والعمل على الحد من الانتهاكات والجرائم السيبرانية.
- تكاتف المجتمع المدني والجمعيات الأهلية مع الجامعة بتقديم برامج لتوعية جميع أفراد الأسرة بضرورة وأهمية الأمن السيبراني لحماية أنفسهم.
- إعداد برامج توعوية لتثقيف الطلاب وأعضاء هيئة التدريس والعاملين في الجامعة بحقوقهم وواجباتهم في استخدام التكنولوجيا.

٥- معوقات تنفيذ التصور المقترح :

- نقص التوعية الإعلامية والحوار المجتمعي في هذا الشأن مما أدى إلى ضعف وعي أفراد المجتمع وخاصة طلاب الدراسات العليا بأهمية وضرورة الأمن السيبراني.
- عدم وجود منظومة أمن للمعلومات في الجامعات تقدم التوعية والحماية بالأمن السيبراني.
- ضعف البنية التحتية التكنولوجية بالجامعات.
- صعوبة وارتفاع تكلفة شراء برمجيات الحماية المرخصة.
- نقص الكوادر المؤهلة نتيجة عدم وجود أقسام مختصة في مجال الأمن السيبراني في الجامعات.

٦- سبل التغلب على معوقات التصور المقترح:

- نشر ثقافة الأمن السيبراني بين الجميع عبر وسائل الإعلام التقليدية والجديدة.
- العمل على إيجاد منظومة أمن للمعلومات في الجامعات تقدم التوعية بالأمن السيبراني.
- تطوير البنية التحتية من خلال تقوية شبكات الإنترنت، ورفع سبل الأمن والحماية للحد من مخاطر الأمن السيبراني.
- التنسيق والتعاون بين الجامعات ووزارة التعليم العالي لشراء برمجيات الحماية المرخصة.
- استحداث أقسام علمية مختصة في مجال الأمن السيبراني، والاستعانة ببعض الخبرات من وزارة التعليم العالي لتطوير وسائل الأمن السيبراني في الجامعات.

قائمة المراجع:

أولاً: المراجع العربية:

إبراهيم، منال حسن محمد(٢٠٢١): الوعي بجوانب الأمن السيبراني في التعليم عن بُعد لدى معلمات العلوم، المجلة العلمية لجامعة الملك فيصل: العلوم الإنسانية والإدارية، ٢٢(٢)، ص ص ٢٩٩- ٣٠٧.

الاتحاد الدولي للاتصالات (٢٠١١): **تقرير الاتجاهات في مجال الاتصالات**: تمكين عالم الغد الرقمي http: itu.Int , (5-11-2020)

بروبست، لوران وآخرون (٢٠١٧): استشراف مستقبل المعرفة، **مؤشر المعرفة العالمي**، مؤسسة محمد بن راشد آل مكتوم للمعرفة والمكتب الإقليمي للدول العربية/ برنامج الأمم المتحدة الإنمائي، دبي، الإمارات العربية المتحدة.

بوابة الأهرام(٢٠٢١) http://gate.ahram.org.eg/News/2883919.aspx (3-8-2021)

جامعة بنها(٢٠٢١) http://bu.edu.eg/BUNews/24550

جبور، منى الأشقر(٢٠١٦): السيبرانية هاجس العصر، لبنان، جامعة الدول العربية، المركز العربي للبحوث القانونية والقضائية.

- الرفاعي، تغريد حميد (٢٠١٨): درجة ممارسة وتعرض كلية المرحلة المتوسطة في مدارس دولة الكويت للتنمر الإلكتروني وأثر متغير الجنس، مجلة العلوم التربوية، (٤)، ج ٣، أكتوبر، ص ص ١١٣- ١٤٥.

السالم، بندر(٢٠١٩): الأمن السيبراني، صوت الوطن.
www.okaz.com.sa/citizen-voice/na/1754249

السمحان، منى عبد الله(٢٠٢٠): متطلبات تحقيق الأمن السيبراني لأنظمة المعلومات الإدارية بجامعة الملك سعود، **مجلة كلية التربية**، (١١١)، جامعة المنصورة، يوليو، ص ص ١-٢٩.

السواط، حمد بن حمود بن حميد، الصانع، نورة عمر، أبو عيشة، زاهدة جميل نمر، سليمان، إيناس السيد محمد، عسران، عواطف سعد الدين (٢٠٢٠): العلاقة بين الوعي بالأمن السيبراني والقيم الوطنية والأخلاقية والدينية

لدى تلاميذ المرحلتين الابتدائية والمتوسطة بمدينة الطائف، مجلة البحث العلمي في التربية، (٢١)، ج ٤، كلية البنات للآداب والعلوم والتربية، جامعة عين شمس، ابريل، ص ص ٢٧٨- ٣٠٦.

الصائغ، وفاء بنت حسن عبد الوهاب (٢٠١٨): وعي أفراد الأسرة بمفهوم الأمن السيبراني وعلاقته باحتياطاتهم الأمنية من الجرائم الإلكترونية، المجلة العربية للعلوم الاجتماعية، المؤسسة العربية للاستشارات العلمية وتنمية الموارد البشرية، ١٤(٣)، ص ص ١٨-٧٠.

الصحفي، مصباح أحمد حامد، عسكول، سناء بنت صالح (٢٠١٩): مستوى الوعي بالأمن السيبراني لدى معلمات الحاسب الآلي للمرحلة الثانوية بمدينة جدة، **مجلة البحث العلمي في التربية**، (٢٠)، ج١٠، كلية البنات للآداب والعلوم والتربية، جامعة عين شمس، ص ص ٤٩٣- ٥٣٤.

الصيدلاني، بشائر(د.ت): أكاديمية وزارة التعليم في الأمن السيبراني، وزارة التعليم.

قاموس اكسفورد(٢٠٢١) http://en.oxforddictionaries.com/definition/cyber , (2\8\2020)

القحطاني، نوره بنت ناصر(٢٠١٩): مدى توافر الوعي بالأمن السيبراني لدى طلاب وطالبات الجامعات السعودية من منظور اجتماعي: دراسة ميدانية، **شؤون اجتماعية**، ٣٦(١٤٤)، جمعية الاجتماعيين في الشارقة، ص ص ٨٥- ١٢٠.

المبارك، عبد الله (٢٠١٦): ما الفرق بين information security وcyber security ؟ http://cut.us /Hq8uE, (3\5\2021)

المجلس الأعلى للأمن السيبراني: **الإستراتيجية الوطنية للأمن السيبراني (٢٠١٧-٢٠٢١)**، رئاسة مجلس الوزراء، جمهورية مصر العربية.

مركز الأمن السيبراني الأسترالي(٢٠٢١).

http://www.cyber.gov.au (2-5-2021)

مركز الأمن السيبراني الماليزي(٢٠٢١).

https://www.cybersecurity.my/en/index.html, (22-6-2021).

المركز الوطني المتكامل لأبحاث التعليم السيبراني(٢٠٢١).
http://nicerc.org (2-5-2021)

المنتشري، فاطمة يوسف، حريري، رندة (٢٠٢٠): درجة وعي معلمات المرحلة المتوسطة بالأمن السيبراني في المدارس العامة بمدينة جدة من وجهة نظر المعلمات، **المجلة العربية للتربية النوعية**، ٤(١٣)، يوليو، ص ص٩٥- ١٤٠.

موقع جامعة القاهرة(٢٠٢٠)
https://cu.edu.eg/ar/Cairo-University-News-13270.html, (5-7-2020)

الهيئة الوطنية للأمن السيبراني، السعودية(٢٠٢١).
https://nca.gov.sa/index.html, (22-5-2021)

وزارة الاتصالات وتكنولوجيا المعلومات(٢٠٢١)
https://mcit.gov.eg/ar (22-5-2021)

الوصابي، علي حميد (٢٠٢١): تحديات الأمن السيبراني على مستوى الهاتف النقال وشبكات المنظمات، المؤتمر الوطني الأول للأمن السيبراني المنعقد في الفترة من ٧-٩ يونيو، وزارة الاتصالات وتقنية المعلومات، صنعاء، اليمن.

ثانيًا: المراجع الأجنبية:

Coughlin, T.M. (2017): Cybersecurity Education for Adolescents and Non-Technical Adults. Master's Thesis.

Elmaghraby, Adel S. and Losavio, Michael M.(2014): Cyber security challenges in Smart Cities: Safety, security and privacy, Journal of advanced research, 5(4), pp 491-497.

International Telecommunications Union (ITU) (2009): series X: Data networks, open system communications and security: telecommunication security: Overview of Cyber security, ITU-TX.1205, 18 April 2008, p6.

International Telecommunications Union (ITU) (2008): series X: Data networks, open system communications and security: telecommunication security: Overview of Cyber security, ITU-TX.1205, 18 April 2008, p2.

ITU (2019): Measuring digital development, facts and figures, switzerland, Geneve, p1.
https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf, (2-4-2021)

Jansäter, Gustav & Olsson, Joel (2018): Cyber Security in Smart Cities - Not a primary concern, **Master thesis**, Lund School of Economics and Management, Lund University, June.

Kemmerer, Richard A. (2003): cyber security, **Proceedings of the 25th International Conference on Software Engineering (ICSE 03)**, computer society, IEEE.
https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.591.577&rep=rep1&type=pdf

Kritzinger, Elmarie, Bada, Maria and Nurse, Jason R.C. (2017): A study into the cybersecurity awareness initiatives for school learners in South Africa and the UK, **10 th world conference on information security education**, Rome, May29-31.

Moskal, Edward J. (2015): A Model for Establishing a Cybersecurity Center of Excellence, **Information Systems Education Journal (ISEDJ)**, 13 (6), Nov., pp 97- 108.

Nakama, Debra& Paullet, Karen (2018): The Urgency for Cybersecurity Education: The Impact of Early College Innovation in Hawaii Rural Communities, **Information Systems Education Journal (ISEDJ)**, 16(4), ISCAP, August, pp 41- 52.

Nyinkeu, Ngatchu Damen, Anye, Divine, Kwedeu, Leonnel & Buttler, William (2018): Cyber Education Outside the Cyberspace: The Case of the Catholic University

Institute of Buea, **International Journal of Technology in Teaching and Learning,** 14(2), pp 90-101.

Pusey, Portia and Sadera, William A. (2011): Cyberethics, Cybersafety, and Cybersecurity: Preservice Teacher Knowledge, Preparedness, and the Need for Teacher Education to Make a Difference, **Journal of Digital Learning in Teacher Education**, 28(2), pp 82-88.

Stewart, k. & shilingford, N.(2011): cyber girls sumer camp: exposing middle school females to internet security, Master thesis, university of Minnesota.

Von Solms, Rossouw & Van Niekerk ,Johan (2013): From information security to cyber security, **computer & security**, EL SEVIER, (38), pp 97- 102.