فعالية تكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والتحديات المرتبطة باستخدام الإنترنت وشبكات التواصل الاجتماعي

د/ سماح سيد أحمد محمد الدكروري
أستاذ مساعد تقنيات التعليم ـجامعة الملك خالد
مدرس تكنولوجيا التعليم ـجامعة أسيوط

المجلة العلمية المحكمة للجمعية المصرية للكمبيوتر التعليمى

معرف البحث الرقمي DOI: 10.21608/EAEC.2017.51848

المجلد الخامس ـ العدد الثاني – مسلسل العدد (10)- ديسمبر 2017

رقم الإيداع بدار الكتب 24388 لسنة 2019

ISSN-Print: 2682-2598 ISSN-Online: 2682-2601

موقع المجلة عبر بنك المعرفة المصري http://eaec.journals.ekb.eg

موقع الجمعية https://eaec-eg.com

العنوان البريدي: ص.ب 60 الأمين وروس 42311 بورسعيد – مصر

فعالية تكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والتحديات المرتبطة باستخدام الإنترنت وشبكات التواصل الاجتماعي

د/ سماح سيد أحمد محمد الدكروري

أستاذ مساعد تقنيات التعليم -جامعة الملك خالد

مدرس تكنولوجيا التعليم -جامعة أسيوط

الكلمات الرئيسية:

تكنولوجيا المعلومات- الإرهاب الإلكتروني- شبكات التواصل الاجتماعي.

مستخلص البحث

انتشر استخدام الإنترنت وشبكات التواصل الاجتماعي في مجال التعليم. وبسبب طبيعة هذه الشبكات وانفتاحها وعدم ارتباطها بدولة أو حدود معينة وصعوبة الرقابة على ما ينشر فيها؛ أصبح الإرهاب الإلكتروني عبر الإنترنت وشبكات التواصل أمرًا واقعًا . ويعد الإنترنت وشبكات التواصل الاجتماعي بيئة مناسبة لممارسات إرهابية وتهديدات حقيقية، ويرجع ذلك إلى ضعف بنية شبكات المعلومات وقابليتها للاختراق وغياب الحدود الجغرافية وتدني مستوى المخاطرة، سهولة الاستخدام وقلة التكلفة بالإضافة إلى صعوبة إثبات الإرهاب والجريمة الإلكترونية. والبحث الحالي يهدف الي دراسة فعالية تكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والتحديات المرتبطة باستخدام الإنترنت وشبكات التواصل الاجتماعي لحماية أمن المعلومات والبرمجيات والأجهزة والبنى التحتية. وقد قامت الباحثة بتصميم استبيان لتحديد أشكال وصور الإرهاب الإلكتروني والتهديدات التي تواجه مستخدمي الإنترنت وشبكات التواصل الاجتماعي لحماية أمن المعلومات والبرمجيات والأجهزة والبنى التحتية. واستبيان آخر لتحديد مدى فعالية تكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والتحديات المرتبطة باستخدام الإنترنت وشبكات التواصل الاجتماعي، وإيجاد حلول لمواجهة الإرهاب الإلكتروني والتهديدات التي تواجه المستخدمين لحماية أمن المعلومات والبرمجيات والاجهزة لديهم. وطُبقت الاستبانات على عينة البحث من أعضاء هيئة التدريس تخصص الحاسب الآلي، وتوصلت النتائج إلى فعالية تكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني وكيفية حماية مستخدم الإنترنت وشبكات التواصل الاجتماعي، وذلك من خلال إيجاد حلول منها، تأمين حسابات المستخدمين للإنترنت وشبكات التواصل وكذلك نظم التحقق الدقيق من الهوية، وتأمين خطوط الدفاع الأمامية واستخدام الجدران النارية، استخدام بصمة العين والصوت والتوقيع الإلكتروني، بالإضافة إلي استخدم

أنظمة الحوسبة السحابية المدعومة بتشفير كامل لمعلومات وبيانات المستخدمين، أنظمة اكتشاف الدخلاء والشبكات الافتراضية الخاصة. لكن هذه الحلول ليست نهائية لأنها تحتاج باستمرار إلى استحداث آليات وبرامج لحماية أمن المعلومات والبرمجيات والأنظمة والبنى التحتية، كلما طور المخترقين والإرهابيين الإلكترونيين برامجهم.

الكلمات المفتاحية: تكنولوجيا المعلومات، الإرهاب الإلكتروني، حماية أمن المعلومات، المنصات التعليمية، الإنترنت وشبكات التواصل الاجتماعي.

مدخل البحث:

يعيش العالم عصر المعلومات، حيث الاعتماد المتزايد على الحاسبات الآلية وشبكات الحاسب الآلي المتطورة في جميع مناحي الحياه وخاصة في مجال التعليم، مما جعلها أكثر عرضه لهجمات القرصنة والفيروسات والاختراق وما إلى ذلك من المخاطر، مما يؤثر سلباً على أنظمة التشغيل وأمن المعلومات **(Zhiyong Li & Suling Jia, 2014 p 4541-4544)** وتعد التطورات التي تحدث باستمرار في مجال تكنولوجيا المعلومات وما تبلغه من أهمية من ناحية توفير خدمات الاتصال بمختلف أنواعها، وخدمات التعليم والتثقيف، وتوفير المعلومات اللازمة للأشخاص والمنظمات ذات أهمية عالية. ولا يخفى أن قوة الدول تقاس الآن بما لديها من تكنولوجيا معلومات. (عيسى العسافين، 2007، 264-286). وتعود أهمية تكنولوجيا المعلومات إلى الخصائص التي تميزها حيث الانتشار الواسع وسعة التحمل لعدد الأشخاص المشاركين وحجم المعلومات المنقولة، كما أنها تتسم بسرعة الأداء وسهولة استعمالها وتنوع الخدمات التي تقدمها. (مؤتمر القمة العالمي لمجتمع المعلومات، 2003، ص2). إن المؤسسات الكبيرة مثل غوغل فيسبوك وأبل ويوتيوب وياهو وهوت ميل، حققت نجاحاً بالغا في أغلب المجتمعات، مع ذلك فقد تعرض بعضها لهجوم وقرصنة إلكترونية أدى إلى توقفها لمدة 24 ساعة. وبالتالي كم كبير من المخاطر المعلوماتية لاستخدامها والاعتماد عليها من الباحثين والطلاب حول العالم (اريك شميدت وجارين كوين، 2013، 14). ومن خلال دراسة الحالة يتضح أن خرق أمن المعلومات ليس ظاهرة جديدة، ولكن تغيرت وسائل ارتكاب الانتهاكات بمرور الوقت، وقد زاد حجم الضرر مع زيادة استخدام الحواسيب **(Michael Krousz, 2010, p196)**.

ويعتبر الإنترنت ووسائل التواصل الاجتماعي من الوسائل المهمة للإرهاب الإلكتروني، ومن ثمَّ يولي المخترقين اهتماما متزايداً لحساباتهم على الإنترنت ومواقع التواصل الاجتماعي عبر مبرمجين متخصصين لحثهم على تنفيذ أشكال للإرهاب الإلكتروني كسرقة المعلومات ونشر الفيروسات. وقد أصبح توظيف الإنترنت ووسائل التواصل الاجتماعي مكثفاً من قبل أفراد وجماعات الإرهاب الإلكتروني، لتجاوزها حاجز الزمان والمكان والرقابة الأمنية وتوفير الوقت والجهد. وقد تعددت أساليب توظيف تلك الجماعات لهذه الوسائل ما بين الحصول على الدعم، ونشر الفيروسات، حتى أصبحت هناك حروب غير تقليدية تدار عبر الإنترنت وشبكات التواصل الاجتماعي، وكل فترة يتم ضرب العالم بأحد الفيروسات المدمرة للأنظمة وللمنظمات الحكومية

والخاصة، مما يحدث كثير من الفوضى والإضرار بالأنظمة والمؤسسات التعليمية. ومع ذلك فإن مواقع التواصل الاجتماعي والإنترنت تلعب دوراً متزايد الأهمية في مجتمع اليوم والمعلمون يقومون باستخدامها كأداة للتعليم والتعلم وكمستودع للمعلومات، وللاستفادة من خدمات المدونات ومنتديات المناقشة، كما عززت أساليب التفكير واستعراض نتائج أعمال الطلاب. وشمل ذلك أيضاً نتائج إيجابية مقصودة وغير مقصودة لبناء مجتمع المعرفة **(Nike & Trea, 2010, p 188-196) .**

وقد دفعت شعبية تكنولوجيا الإنترنت وشبكات التواصل الاجتماعي مؤخرا المحاضرين الجامعيين لاستخدامها في الأنشطة التعليمية. ويرجع ذلك إلى ما لهذه التكنولوجيات من إمكانات هائلة لتعزيز تجربة التعليم والتعلم. ومع ذلك كانت هناك دراسات محدودة تقيم كيفية استخدام هذه التكنولوجيات الاجتماعية بفعالية وما هي التأثيرات السلبية على تجربة تعلم الطلاب، لا سيما فيما يتعلق بقيمتها في الحفاظ على أمن المعلومات **(Suraya & others, 2015, p 1-9) .**

وقد حذر رئيس الاستخبارات الهولندية "روب بيرتولي" أن العالم قد يكون على حافة عمل تخريبي رقمي جدي يزرع الفوضى والاضطراب. وقال "بيرتولي" أمام مؤتمر بشأن الأمن الإلكتروني عقد في لاهاي أن تخريب شبكات البنية التحتية "هو أمر قد يبقيك مستيقظا طوال الليل،" في وقت يحاول فيه خبراء حول العالم التعامل مع هجمات معلوماتية ضخمة ضربت عشرات الدول، وأشار بيرتولي إلى الهجوم الذي اخترق حواسيب أكبر شركة نفط سعودية عام 2012، وكيف تمت قرصنة شركات الكهرباء الاوكرانية مما تسبب في انقطاع الخدمة كلياً لعدة ساعات، ورغم فوائد الارتباط الكبير في البنى التحتية حول العالم، إلا أن لذلك "نقاط ضعف". وأوضح أن على الدول أن تكون مستعدة لمواجهة التهديدات المستقبلية في المجال الرقمي. كما أوضح باحثون أن الهجمات الإلكترونية الضخمة التي تحصل خلال فترات، أنها أسوأ الأعمال التخريبية في العالم. ومن ناحيتها أشارت الشرطة الأوروبية "يوروبول" إلى أن عدد عناوين بروتوكول إنترنت أو المعرّف الرقمي لأجهزة الكمبيوتر التي تأثرت حول العالم بلغ 163745، حالة التي تم تسجيلها في عام 2017 **Agence France-Presse (AFP), May 16, (2017, p3).**

ومن المؤكد أن فيروسات الحاسب الآلي التي تضرب كثير من دول العالم في نفس الوقت من التحديات وأحد أشكال الإرهاب الإلكتروني التي تواجه تكنولوجيا المعلومات حول العالم، وفي سابقة بأبريل 2017، تعرضت أكثر من 74 بلداً في العالم إلى هجمات إلكترونية متزامنة خطيرة أدت إلى تعطيل أنظمة معظم المستشفيات والجامعات البريطانية كما أصابت دولاً عظمى مثل الصين وروسيا.

ونقلت وكالات الأنباء الروسية عن المتحدثة باسم الوزارة "إيرينا فولك" أنه تم رصد هجوم فيروسي على الحاسبات الآلية الشخصية التابعة للوزارة والعاملة على نظام تشغيل ويندوز.

وأضاف الخبراء أن الفيروس ضرب نحو 45 ألف موقع حول العالم، وربما ضرب عددا أكبر، ووصف بعض الخبراء تلك الهجمات بالخطيرة لأنها قادرة على تعطيل الحياة في كثير من دول العالم. ويتفق رأي هؤلاء الخبراء جزئيا مع تصريح رئيسة الوزراء البريطانية " تيريزا ماي" التي قالت إن الهجوم الإلكتروني استهدف عددا من الدول والهيئات، وقد تم التصدي للمشكلة ومعالجتها . **(www skynewsarabia.com,. 2010, p1)**

ويُعد تقرير الشرق الأوسط بتاريخ 19 أكتوبر 2014 من التقارير التي أولت اهتماما بالغاً بأمن المعلومات، ودعت لإجراء تفعيل لتكنولوجيا ونظم أمن المعلومات وصيانتها، لرصد الأنظمة الأمنية المتكاملة لحماية أمن المعلومات ومكافحة الإرهاب الإلكتروني (**MENA Report;London,2014,p 16**).

وقد ظهر في مقابل الإرهاب الإلكتروني الرقابة من قبل تكنولوجيا المعلومات، وأصبح هناك نوع من الحروب غير التقليدية بين هؤلاء المخترقين والأجهزة التقنية للأفراد والدول، التي أصبح لديها متخصصون في التعامل مع تلك المشكلات ولذلك أصبح جانب أمن المعلومات أكثر تغلغلاً في المجالات التكنولوجية والمعلوماتية، وذلك من أجل التعامل مع المستجدات التكنولوجية التي تهدد أمن المعلومات في جميع المؤسسات الخدمية والتعليمية حول العالم، ويسعي البحث الحالي لدراسة فعالية تكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والتحديات المرتبطة باستخدام الإنترنت وشبكات التواصل الاجتماعي.

مشكلة البحث:

انتشر استخدام الإنترنت وشبكات التواصل الاجتماعي انتشارًا واسعًا في التعليم، ويرجع ذلك إلى أنه لا يوجد حصر للخدمات التي يمكن أن يقدمه الإنترنت وشبكات التواصل الاجتماعي في مجال التعليم. فكل ما يصب في مجال الاتصال متوفر كخدمة مركزية فيه، يوفر الخدمات التقنية كالتدريس والاتصال المرئي والبريد الإلكتروني، يتسم بالانفتاح على المعلومات، كما تتوفر فيه مميزات التعلم التفاعلي والبحث ودعم لكثير من اللغات المعروفة حول العالم (مضر عدنان زهران، 2011، ص 45). وقد ذكرت "كاترين **Katrin**" وآخرون أيضاً أن وسائل التواصل الاجتماعي تفتح خيارات متعددة لإضافة بعُد جديد إلى عمليات التعلم والمعرفة. وعلى وجه الخصوص تقوم بربط التعلم الرسمي وغير الرسمي كما يمكن للطلاب العثور على المعرفة وتنظيمها وتبادلها للأغراض التعليمية، إن الطلاب يستخدمون مواقع الإنترنت وشبكات التواصل الاجتماعي أساساً للتفاعل الاجتماعي والتكامل. وتشير نتائج دراستها أيضا إلى أن التواصل حلول للقضايا الاجتماعية على مواقع الشبكات الاجتماعية يسير جنبا إلى جنب مع تبادل المعرفة ذات الصلة بالدراسة **(Katrin& Others, 2012, p 9-14)**. وأكد محمد مراياتي في دراسة سعت إلى تحديد تأثير تكنولوجيا المعلومات على تعلم الطلاب للعلوم والتكنولوجيا، والبحث العلمي والتطوير والتكنولوجي ونشر العلم، وعرض بعض المشروعات الناجحة، ووضح أثرها على التعليم. وتوصلت الدراسة لمشروع يناسب طلاب التعليم العالي (محمد مراياتي، 2006، 201-217).

لكن بسبب طبيعة هذه الشبكات وانفتاحها، وعدم ارتباطها بدولة أو حدود معينة، وانعدام الخصوصية الذي يُعد تحدي كبير للمؤسسات التعليمية لحفظ أمن معلومات الطلاب وبياناتهم من الإرهاب الإلكتروني، أثناء التعلم من خلال الإنترنت وشبكات التواصل الاجتماعي، وصعوبة الرقابة على ما ينشر فيها أيضاً كتحدي ثاني؛ أصبح الإرهاب الإلكتروني عبر الإنترنت وشبكات التواصل امرًا واقعًا. ويعد الإنترنت وشبكات التواصل الاجتماعي بيئة مناسبة لممارسات إرهابية وتهديدات إلكترونية لتحقيق مآرب خاصة تتعارض ومصلحة الفرد والمجتمع أو القيام بأعمال تقنية تخريبية بشكل يُخفي هوية منفذها، ويرجع ذلك إلى ضعف بنية شبكات المعلومات وقابليتها للاختراق، وغياب الحدود الجغرافية، وتدني مستوى المخاطرة، سهولة الاستخدام وقلة التكلفة بالإضافة إلى صعوبة اثبات الإرهاب والجريمة الإلكترونية، وغياب جهة الرقابة بشكل كبير. ويرجع ذلك إلى أن الإنترنت عند ابتكاره وتصميمه لم يؤخذ بعين الاعتبار القضية الأمنية، لأنه أسس لأغراض البحث العلمي، ومثالاً على ذلك بروتوكول الإنترنت الأساسي **ICP/IP** يستخدم كوسيلة لإجراء عمليات نقل المعلومات بين مختلف أنواع الأجهزة وأنظمة التشغيل والشبكات مما يسهل على الإرهابيين استخدامه للوصول إلى المعلومات بسهولة (عطا الله أحمد سويلم الحسبان، 2009، ص 29).

إذا كانت المعلومات هي المقياس الذي تُقاس به قوة الشعوب، فمن يمتلك المعلومات يمتلك القوة التي توصل الشعوب إلى الريادة. لقد تغير العالم وأصبحت جرائم المعلوماتية من أهم ما يؤرق الأفراد والمنظمات، حيث أصبح يمكن سرقة المعلومات وغيرها من خلال أفراد جالسين خلف أجهزتهم، ومن الصعب أن يتم حماية المؤسسات التعليمية إذا لم يكن هناك وعي لمواجهة أعداء مسلحون بالعلم والبرامج التقنية (خضرالطيطي، 2010، ص17). وقد أعلنت عواصم غربية كثيرة التعبئة العامة لمواجهة الهجمات المعلوماتية وحملات التضليل التي تسبب كثير من المشكلات، مع اقتراب مواعيد استحقاقات هامة في أكثر من بلد أوروبي. وقد طلب الرئيس الفرنسي "فرنسوا هولاند" رفع اقتراحات اليه بشأن اجراءات خاصة لليقظة والحماية في مجال المعلوماتية. كذلك حذر وزير خارجيته "جان مارك ايرولت" أنه يجب إبراز الحدود بوضوح لكل من يحاول انتهاك مبدأ عدم التدخل واتخاذ اجراءات رد عند اللزوم. في اواخر 2016 قالت المستشارة الالمانية "انغلا ميركل" أن مؤسسات تطلق تسمية "نزاعات هجينة" على العمليات التي تشمل اختراقاً معلوماتياً وحملات تضليل، وذلك بعد تعرض ألمانيا لأضخم هجوم معلوماتي طال مؤسسات هامة منها تقنية للاتصالات. وأضافت "ميركل" بات ذلك حدثا يوميا وعلينا تعلم الرد عليه. كما اعتبر الباحث في مؤسسة العلاقات الدولية "جوليان نوسيتي" أن ما حدث في الولايات المتحدة من إرهاب إلكتروني كشف للجميع فداحة التهديد. ولم يجذب هذا الملف هذا القدر من الاهتمام سواء في المجال العام او الخاص قبل 2016.

يتضح مما سبق أن المشكلة لا تختص بدولة أو مؤسسة، لكنها مشكلة عالمية، إن الإرهاب الإلكتروني يعتمد على استخدام الإمكانيات العلمية والتقنية، واستغلال وسائل الاتصال والشبكات المعلوماتية، من أجل الإضرار بالأخرين حيث تستهدف معلومات أو بيانات المستخدمين أو نظم الحاسب الآلي (محمد طوالبية، 2017، ص ص 55-67).

وتتعدد أشـــكال الإرهاب الإلكتروني ما بين فيروســـات البرمجيات المعلوماتية منها "الدودة" وهي قادرة على التوغل في شـبكة بأكملها انطلاقاً من كمبيوتر واحد مصـــاب إلى شـبكة أجهزة حاسبات مؤسسة أو دولة أو مجموعة دول، وفيروس "الفدية" وهو برنامج خبيث لطلب فدية من كل جهة أصـــابها، فدية مالية بعملة "بتكوين" الافتراضـــية مقابل فك الشـــيفرة للنظام، والفيروس المســـمى "واناكراي" الذي يجمع بين فيروســـات وبرمجيات الدودة والفدية. ونظراً لخطورة الموضـــوع، تعددت الجهود لحماية أمن المعلومات، منها ما قام به الحلف الأطلســـي والاتحاد الأوروبي خلال عام 2017، حيث دعا إلى تشـــكيل مركز أوروبي رفيع لمكافحة التهديدات "الهجينة" في فنلندا، يجيز لشبكة خبراء اوروبيين تبادل المعلومات واطلاع الدول الأعضاء (في الاتحاد الأوربي وفي الحلف) على أي هجمات او تهديدات إلكترونية جديدة لحماية الأنظمة ومواجهة الهجمات الإلكترونية **(Gregory Daniel, 2017, p1)**.

وقد تعددت الجهود العربية في مجال حماية أمن المعلومات ومواجهة الإرهاب الإلكتروني، ومن هذه الجهود: مؤتمر حماية أمن المعلومات والحد من التهديدات والمخاطر الإلكترونية للشـرق الأوسـط وشـمال أفريقيا مؤتمر أمن المعلومات يوم 21 تشـرين الثاني/ نوفمبر 2017، وقد حذر القائمون على المؤتمر من أنه على الرغم من النمو السنوي لاقتصاد الإنترنت المعروف أيضًا باسم "الاقتصاد الرقمي" في جميع أنحاء العالم، إلا أن المنطقة تواجه تحديات شديدة الأهمية تتعلق بتأمين المعلومات من الهجمات الإلكترونية (مؤتمر أمن المعلومات، 2017، ص1).

والمؤتمر الدولي الثاني لمكافحة الجرائم المعلوماتية حيث تم فيه التوصـــل إلى توصـــيات أهمها التأكيد على زيادة دور قطاع الاتصـــالات وتقنية المعلومات في مكافحة الجرائم المعلوماتية والتوعية بالمخاطر، وإصـــدار لائحة تنفيذية لنظام مكافحة الجرائم المعلوماتية، وتضـــمين النصـوص اللازمة لمواجهة الصـور المتنوعة والمسـتحدثة للجريمة المعلوماتية (مؤتمر الدولي الثاني لمكافحة الجرائم لمعلوماتية، جامعة الملك خالد، ص3).

ومؤتمر أمن المعلومات الإلكترونية بأبو ظبي لبناء اســـتراتيجية دفاعية فعالة لتكنولوجيا المعلومات، كســـياج واقي لحماية أمن المعلومات والحد من القرصـــنة الإلكترونية، وقد شـــهد المؤتمر اهتماماً كبيراً بمجال أمن المعلومات والأمن الإلكتروني والحروب الإلكترونية ومخاطر البرمجيات (مؤتمر أمن المعلومات بأبو ظبي، 2017، ص9).

كما عُقد بالقاهرة مؤتمر شـــركاء الأعمال الدولي، للإعلان عن حزمة جديدة لعدد من الحلول الرقمية لأمن الشبكات والمعلومات بمصر والشرق الأوسط، وتم التأكيد في التوصيات على أن سـوء الاسـتغلال المتنامي للشـبكات الإلكترونية لأهداف إجرامية يؤثر سـلبًا على سـلامة البنية التحتية للمعلومات، لاسيما على المعلومات الشـخصـية، والقطاعات الحكومية والخدمية والتعليم، كما تم تقديم برامج لتطوير النظم والمعايير المتبعة في أمن المعلومات والشـبكات والوقوف على التجارب والممارســـات المتميزة في بنـاء أنظمـة حمـايـة المعلومـات (مؤتمر أمن المعلومـات والتكنولوجيا، 2017، ص1)

نظراً للتحدي الذي تواجهه الأنظمة التعليمية، ما بين المميزات الغير محدودة لاستخدام الإنترنت وشبكات التواصل الاجتماعي في التعليم، ومواجهة الإرهاب الإلكتروني لحماية معلومات الطلاب داخل المؤسسات التعليمية، ويعد هذا مشكلة حقيقية، حيث أن حماية أمن هذه المعلومات والأجهزة والبرمجيات والبنى التحتية لمؤسساتنا التعليمية أمر حتمي عليها توفيره للطلاب، فكيف يمكن حمايتها؟ وهل تكنولوجيا المعلومات تستطيع تقديم حلول بل وخطوات استباقية لحماية مؤسساتنا التعليمية من الإرهاب الإلكتروني؟

ويسعى البحث الحالي إلى التوصل لمعرفة مدى فعالية تكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والتحديات المرتبطة باستخدام الإنترنت وشبكات التواصل الاجتماعي. وقد تحددت مشكلة البحث الحالي في الإجابة على السؤال الرئيس التالي: " ما دور تكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والتهديدات الأمنية المرتبطة باستخدام الإنترنت وشبكات التواصل الاجتماعي؟

أسئلة البحث:

يحاول البحث الحالي الإجابة عن الأسئلة الآتية:

1- ما الصعوبات والتحديات الإلكترونية المرتبطة باستخدام الإنترنت وشبكات التواصل الاجتماعي والتي تواجه مستخدم الإنترنت وشبكات التواصل الاجتماعي لحماية أمن المعلومات والبرمجيات؟

2- ما فعالية تكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني الصعوبات والتحديات المرتبطة باستخدام الإنترنت وشبكات التواصل الاجتماعي من وجهة نظر أعضاء هيئة التدريس؟

أهداف البحث:

يهدف البحث الحالي للتوصل إلى:

مدى فعالية تكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والصعوبات والتحديات المرتبطة باستخدام شبكات التواصل الاجتماعي من وجهة نظر أعضاء هيئة التدريس تخصص الحاسب الآلي.

أهمية البحث:

يمكن أن يستفيد من هذا البحث كلاً مما يأتي:

1-الافراد والمؤسسات لحماية أمن معلوماتهم على الإنترنت وشبكات التواصل الاجتماعي.

2-المؤسسات التعليمية أثناء استخدامها الإنترنت وشبكات التواصل الاجتماعي لنشر خدماتها التعليمية.

3-الباحثون في مجال أمن المعلومات ومواجهة الإرهاب الإلكتروني.

منهج البحث:

اعتمد البحث الحالي على المنهج الوصفي التحليلي.

عينة البحث:

تكونت عينة البحث من مجموعة من أعضاء هيئة التدريس تخصص الحاسب الآلي في جامعة الملك خالد.

حدود البحث:

اقتصر البحث الحالي علي:

- الإرهاب الإلكتروني والصعوبات والتحديات في البحث الحالي على تلك المرتبطة بالإنترنت وشبكات التواصل الاجتماعي.
- مدى فعالية تكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والصعوبات والتحديات من وجهة نظر أعضاء هيئة التدريس تخصص الحاسب الآلي.

متغيرات البحث:

المتغير المستقل: تكنولوجيا المعلومات

المتغيرات التابعة: مواجهة الإرهاب الإلكتروني والصعوبات والتحديات المرتبطة باستخدام الإنترنت وشبكات التواصل الاجتماعي من وجهة نظر أعضاء هيئة التدريس تخصص الحاسب الآلي.

أدوات البحث:

تطلب البحث إعداد الاستبانات التالية:

- استبيان بالتهديدات وصور الإرهاب الإلكتروني والصعوبات والتحديات التي تواجه مستخدمي الإنترنت وشبكات التواصل الاجتماعي لحماية أمن معلومات.
- استبيان لفعالية تكنولوجيا المعلومات في مواجهة التهديدات والإرهاب الإلكتروني المرتبطة باستخدام الإنترنت وشبكات التواصل الاجتماعي والحلول التي تقدمها تكنولوجيا المعلومات لحماية أمن المعلومات والبرمجيات.

مواد المعالجة الإحصائية

تمثلت مواد المعالجات الإحصائية في الآتي:

- حساب التكرارات والنسب المئوية والمتوسط الوزني والانحراف المعياري لكل عبارة من عبارات استبانة التهديدات الأمنية والصعوبات والتحديات التي تواجه مستخدم الإنترنت وشبكات التواصل الاجتماعي لحماية أمن المعلومات والبرمجيات والأجهزة والتي تتكون من (24) تهديداً أو صعوبة أو تحدياً، وذلك بهدف ترتيب هذه التهديدات الأمنية والصعوبات والتحديات التي تواجه مستخدم الإنترنت وشبكات التواصل الاجتماعي لحماية أمن المعلومات والبرمجيات والأجهزة لمعرفة أكثرها خطورة.
- حساب التكرارات والنسب المئوية والمتوسط الوزني والانحراف المعياري لكل عبارة من عبارات استبانة دور تكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والتهديدات الأمنية

المرتبطة باستخدام الإنترنت وشبكات ا لحماية أمن المعلومات والبرمجيات والأجهزة، والتي تتكون من (35) دوراً، وذلك بهدف ترتيب أدوار تكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والتهديدات الأمنية المرتبطة باستخدام الإنترنت وشبكات التواصل الاجتماعي لحماية أمن المعلومات والبرمجيات والأجهزة لمعرفة أكثرها قوة.

الإطار النظري للبحث:

إن العصر الذي نعيش فيه يمتاز باستخدام تكنولوجيا المعلومات من حاسبات وإنترنت وهواتف نقالة وتقنية اتصال لاسلكية، في جمع البيانات ومعالجتها وبثها، ليتم انجاز كثير من الأعمال بشكل أسرع وأكثر فعالية لشتى مناحي الحياة. وقد استفاد التعليم التقليدي والإلكتروني من تكنولوجيا الإنترنت وشبكات التواصل الاجتماعي في تنظيم وتنسيق المصادر والأعمال والأنشطة التعليمية، لكنه في المقابل فتح باباً للمتطفلين وقراصنة الحاسوب (الإرهاب الإلكتروني) للقيام بعمليات تدمير للبيانات والبرامج وأجهزة الحاسوب والأجهزة الخلوية والبنى التحتية، لذلك يجب معرفة طرق حماية أنفسنا ومصادرنا من هذه الأخطار، من خلال التقنيات الحديثة لتكنولوجيا المعلومات لصد ومنع التهديدات والأخطار.

ويذكر "خضر الطيطي" أن الحل الأمني الذي تقدمه التقنيات الحديثة يعتمد على عوامل أهمها:

- مدى التهديدات التي تواجه النظام الحالي للمؤسسات والأفراد.
- الحالة التقنية المتوفرة لحماية النظام ومدى قوتها لصد ومنع الهجوم الإلكتروني.
- قيمة معلومات ومصادر معلومات المؤسسة.
- تشابه التهديدات على الأنظمة المختلفة المفعلة بالمؤسسة (خضر الطيطي، 2010، ص20).

إن الهدف الرئيس لأمن المعلومات هو عملية حماية المعلومات، وكشف الاختراق أو الهجوم وغيرها من عمليات الإرهاب الإلكتروني، وهي عملية معقدة تحتاج برمجيات ذكية تعتمد على أنظمة التشفير المتقدمة، وأجهزة حاسبات آلية تُستخدم كسياج لصد وكشف الخروقات الأمنية قبل أن تحقق أهدافها. ومن الدراسات التي تناولت لجوانب الحرية والمسؤولية المرتبطة باستخدام تكنولوجيا المعلومات دراسة (عبد المجيد بو عزة، 1991، ص ص 306-313) التي اهتمت بالجوانب الاجتماعية المرتبطة بتطوير واستغلال تكنولوجيا المعلومات، واهتمام المجتمعات بها وتأثير ذلك على حرية الانسان. وأكدت الدراسة على أهمية توافر المسئولية عن حماية المعلومات مقابل الحرية التي توفرها تكنولوجيا المعلومات. والبحث الحالي يدعم الحفاظ على أمن المعلومات، مع ضمان استفادة الطلاب من الإنترنت وشبكات التواصل الاجتماعي في التعليم.

تكنولوجيا المعلومات

تكنولوجيا المعلومات هي تقنية القرن الواحد والعشرين وما بعده، فهي أنظمة بالغة الدقة تتكون من مجموعة أدوات. وتسمى تكنولوجيا المعلومات وتقنية تكنولوجيا المعلومات، ويعبر عنها

اختصاراً **.IT**، وتسمى أيضاً: قسم خدمات المعلومات **(IS)** ونظم المعلومات الإدارية **(MSP)** ، أو مزود خدمة المنظمة **(MSP)** .
وقد عرّفتها (مجموعة المعلومات الأمريكية) بأنها: "دراسة، تصميم، تطوير، تفعيل، دعم أو تسيير أنظمة المعلومات التي تعتمد على الحواسيب"، ويتم استخدامها وتطبيقها على الحواسيب والتطبيقات البرمجية، وتعمل هذه التطبيقات على تحويل، وتخزين، ومعالجة وإرسال، واسترجاع آمن للمعلومات (تكنولوجيا المعلومات،2016، ص1)

تكنولوجيا المعلومات تطلق على جميع ما يتصل بمعدات الاتصالات والبرمجيات التي تساعد الحاسوب للتعامل في إطارٍ مستقلٍ أو شبكي مع عدة أجهزةٍ أخرى. وعرفتها " نتاشا عيسى" على أنها البحث عن أفضل وأسرع الطرق التي تعمل على تسهيل الحصول على المعلومات والبيانات وجعلها متاحة ومتوفرة لطالبيها بأقصى سرعة وفعالية (نتاشا عيسى، 2014، ص1). وقد ركزت مدينة الملك عبد العزيز للعلوم والتكنولوجيا على مجال تكنولوجيا المعلومات الواسع، حيث يضم بحوثاً وتطبيقات مختلفة. وقد أصبحت محركاً أساسياً للإنتاج والنمو الاقتصادي في كثير من البلدان، فالعمل على تطوير تكنولوجيا المعلومات يساهم في تعزيز الإنتاجية في جميع المجالات وذلك بتسريع نشر المعرفة، وإعادة توجيه القوى العاملة، وتطوير خدمات جديدة، ودعم التعليم. إن تقنية المعلومات -وبخاصة النمذجة الحاسوبية، وتحليل البيانات، وبناء قواعد البيانات -تساهم في تقدم جميع مجالات العلوم والتقنيات التعليمية والاجتماعية. (مدينة الملك عبد العزيز للعلوم والتقنية، 2016، ص1). وعرفت تكنولوجيا المعلومات بأنها "مجموع التقنيات أو الأدوات أو الوسائل أو النظم المختلفة التي يتم توظيفها لمعالجة المضمون أو المحتوى الذي يراد توصيله من خلال عملية الاتصال الجماهيري أو الشخصي أو التنظيمي ، والتي يتم من خلالها جمع المعلومات والبيانات الرقمية (من خلال الحاسبات الإلكترونية) وتخزينها واسترجاعها في الوقت المناسب، ثم نشر هذه المواد الاتصالية والرسائل الرقمية، ونقلها ومبادلتها. (محي محمد مسعى،1999، ص26). وقدمت منظمة اليونسكو تعريفا لمفهوم تكنولوجيا المعلومات جاء فيه أن تكنولوجيا المعلومات هي تطبيق التكنولوجيات الإلكترونية ومنها الحاسب الآلي والاقمار الصناعية وغيرها من التكنولوجيات المتقدمة لإنتاج المعلومات التناظرية والرقمية وتخزينها واسترجاعها، وتوزيعها ونقلها من مكان إلى آخر. ومن الدراسات التي تناولت تكنولوجيا المعلومات كحلقة وصل بين مراحل التعليم دراسة (مجدي عزيز إبراهيم 2009، ص ص 120-133) هدفت لمعرفة هل تكنولوجيا المعلومات تمثل حلقة وصل في مراحل التعليم؟ وتكونت عينة الدراسة من مجموعة من طلاب المرحلة الثانوية والجامعية، وتوصلت الدراسة إلى أهمية استخدام تكنولوجيا المعلومات كحلقة وصل بين المراحل التعليمية.
وقد أورد معجم ما كميلان **(Macmillan)** تعريف مختصر لتكنولوجيا المعلومات أنها "حيازة معلومات لفظية ونصية ورقمية وتجهيزها واختزانها وبثها الكترونياً **Longley, D. Shain, M.,1985 ,P164)**). كما أشار جنيفر**(Jennifer)** إلى وجود ثلاث نماذج لتعريفها كما يلي:

1- حيازة المعلومات اللفظية والمرئية والنصية والرقمية بواسطة إلكترونيات مصغرة.

2- الأنظمة العلمية والتكنولوجيا والهندسية وطرق الإدارة المستخدمة لهذه المعلومات ومعالجتها واستخدامها والجوانب الاجتماعية والثقافية والاقتصادية المتعلقة بذلك.
3- جمع المعلومات وتخزينها وبثها واستخدامها، والتعرف على أهداف الإنسان من استخدام التكنولوجيا والقيم والمبادئ التي يأخذ بها لتحقيق غاياته، وحماية الانسان أثناء العمل مع التكنولوجيا. (**Rowley, J.E., 1988, p1**).

وقد تم اعتماد تعريف جنيفر **Jennifer** النموذج الثاني والثالث في البحث الحالي لربط تكنولوجيا المعلومات بالجوانب الاجتماعية والمبادئ والقيم وحماية الخصوصية أثناء استخدام الأشخاص تكنولوجيا المعلومات المتمثلة في الإنترنت وشبكات التواصل الاجتماعي.

مما سبق يتضح أن تكنولوجيا المعلومات تطلق على جميع معدات الاتصالات والبرمجيات التي تساعد الحاسوب من التعامل في إطار مستقل أو شبكي مع عدة أجهزة أخرى، أي أنه اختصاص واسع يهتم بالتقنية ونواحيها المتعلقة بمعالجة وإدارة المعلومات، وتهتم أيضاً بالجوانب الاجتماعية والثقافية والاقتصادية. وتتعامل تكنولوجيا المعلومات مع الحواسيب الإلكترونية والبرمجيات، للعمل على تخزين وتحويل البيانات وحمايتها ونقلها واستعادتها في أيّ وقت لذلك تعمل وفق معايير مطبقة على أجهزة الحاسوب للحصول على معلومات يعجز الإنسان عن تجهيزها وعملها بالطرق التقليدية، وخاصة في المجتمعات ذات الكم الكبير من المعلومات والبيانات مثل الإنترنت وشبكات التواصل الاجتماعي، الذي يفقد السيطرة عليها وعلى معالجتها بشكلٍ دقيق وسريع إلا باستخدام تكنولوجيا المعلومات الحديثة التي تعمل في مجالاتٍ كثيرة منها: الأبحاث العلمية، والمال والأعمال، والاقتصاد.

تتميز تقنية تكنولوجيا المعلومات:
بتكلفة اقتصادية منخفضة، وقدرة على القيام بأعمال كثيرة ومتعددة المجالات في وقتٍ قليل وبجهد أقل وذلك من خلال قواعد ونظم المعلومات المختلفة وباستخدام برامجها المتنوعة. لذلك يظهر واضحاً دور تكنولوجيا المعلومات في تعزيز التنمية البشرية والاقتصادية التقليدية، فهي تتخطى الحدود الجغرافية والسياسية للدول لتصل إلى أي نقطة من العالم كما أنها تمتاز بكثرة وتنوع المعلومات والبرامج التثقيفية والتعليمية، لذلك تعد مصدر هام للمعلومات للأشخاص والمنظمات والحكومات، كما أنها تلعب دورا هاما في تنمية العنصر البشري من خلال البرامج التي تعرضها كبرامج التدريب وبرامج التعليم وبرامج التعلم وغيرها. لهذا كان من الضروري الاهتمام بها وتطوير استخدامها بشكل فعال مع تدريب وتعليم الطلاب والمؤسسات التعليمية على استعمالها، وتوعيتهم بأهميتها في التنمية والتطور.

مكونات تكنولوجيا المعلومات: تتكون تكنولوجيا المعلومات من ثلاثة عناصر أساسية كالتالي:
أولاً: الكيان المادي كالحاسوب وما يتصل به من أجهزة ومعدات.
ثانياً: البرمجيات التي تعمل على الحاسوب، والبرمجيات التي تعمل على تشغيل الحاسوب والقيام بمهام مختلفة.

ثالثا: الموارد المعرفية 1437/11/1(**https://ar.wikipedia.org/wiki**/)

الإنترنت وشبكات التواصل الاجتماعي وعلاقته بالإرهاب الإلكتروني:
نظراً للتطور التكنولوجي الكبير وخاصة في مجال التكنولوجيا والعالم الافتراضي الإلكتروني "الإنترنت وشبكات التواصل الاجتماعي" ظهرت العديد من الظواهر التي لم يُتعارف عليها من قبل. وقد جاءت بالإيجاب في كثير من الجوانب وبالسلب أيضاً في جوانب أخرى، منها ما يخدم أهدافاً سليمة وبطرق مشروعة والآخر يحقق أغراضاً خاصة لأفراد ومؤسسات. ومن أبرز سلبيات هذا التطور الجرائم المعلوماتية، والتي يأتي في مقدمتها الإرهاب الإلكتروني" **Cyber-Terrorism**" والذي يمثل تهديداً على الأفراد والأمن القومي للدول. وقد لوحظ تزايد الهجمات الإلكترونية في الآونة الأخيرة (ولاء البحيري، 2012، 189-192).

وقد عَرف الاتحاد الأوربي الإرهاب الإلكتروني أنه "أعمال ترتكب بغرض ترويع الأهالي أو اجبار الهيئات على القيام بعمل أو الامتناع عن القيام بعمل. أو تدمير الهياكل الاقتصادية والاجتماعية وزعزعة الاستقرار" (هشام بشير، 2012، 76). ومن الدراسات التي تناولت الإرهاب الإلكتروني والصعوبات المرتبطة بذلك دراسة (بدرة هويمل الزبن، 2012، 1-246) والتي هدفت إلى البحث في طرق مكافحة الإرهاب الإلكتروني والصعوبات القائمة التي تظهر في مجال مكافحته، وتوصلت إلى بعض التدابير القانونية والجهود الوطنية والإقليمية في مجال مكافحة الإرهاب التقليدي والإلكتروني، والاتفاقيات الدولية والتشريعات لحد من الإرهاب. ودراسة (عبد الله عبد العزيز العجلان، 2015، 50-65) التي سعت لتحليل جريمة الإرهاب المعلوماتي وتحديد معالم هذه الظاهرة الإجرامية المستحدثة التي تعتمد على استخدام الإمكانات التقنية، وبيان أسبابها ودوافعها، وتحديد مفهوم هذه الجريمة، وإبراز مظاهرها وأشكالها.

وفي البحث الحالي يمكن تعريف الإرهاب الإلكتروني "بالتهديد المادي والمعنوي على الانسان في نفسه بغير حق، باستخدام الموارد المعلوماتية من خلال الإنترنت وشبكات التواصل الاجتماعي".

يعتمد المتخصصون والأكاديميون عدة مسميات للتعبير عن التوسع في ظاهرة استخدام الإنترنت وشبكات التواصل الاجتماعي من قبل المخترقين، منها: الإرهاب "الإلكتروني" أو "الرقمي" أو "الافتراضي" أو "الشبكي". فقد تمكنت معظم التنظيمات الإرهابية شبه المنظمة من امتلاك أدوات المعرفة والتقنية اللازمة لاختراق العالم الافتراضي بدرجة كبيرة. (سماح عبد الصبور، 2014، 2) وتكفي الإشارة إلى زيادة عدد المواقع المحسوبة لجماعات إرهابية عالمية. كما ذكر" فليب سيب ودانا جانبك، **Philip Seib and Dana M."** في كتابة "الإرهاب العالمي والإعلام الجديد" فإن عدد المواقع المحسوبة لجماعات الإرهاب الإلكتروني العالمي ارتفع من نحو 12 موقعاً إلكترونياً عام 1997، إلى 4,350 موقعاً في أوائل عام 2005، ثم 4,800 موقع عام 2006، وتجاوز أكثر من 6 آلاف موقع إلكتروني في نهاية عام 2008، والعدد

في تزايد، ومن الملحوظ أن هذه التنظيمات كان لها السبق في الاعتماد على المواقع الإلكترونية حول العالم (فليب سيب ودانا جانبك، **Philip Seib and Dana M. Janbek**، 2011، 41). وتُعرف شبكات التواصل الاجتماعي بأنها "شبكات تفاعلية تتيح لمستخدميها التواصل في أي وقت وفي أي مكان في العالم"، وقد انتشرت على الشبكة الدولية للمعلومات (الإنترنت) في السنوات الأخيرة ومن أبرزها "فيسبوك" "تويتر" و"يوتيوب"، لتحدث في زمن قياسي تأثيراً عابراً للحدود، وتزيد من كثافة وسرعة "العولمة" والتأثيرات المتبادلة على المستويات المختلفة، بحيث أضحى أي تفاعل يحدث في أي منطقة في العالم يترك تأثيره في المناطق الأخرى في ظل ما يطلق عليه جوزيف ناي "تأثير النظام" **System Effect**. (**Joseph Nye, 2002, 85-86**). ومع تزايد اعتماد الإرهابيين الإلكترونيين في تحركاتهم الخارجية على الجمع بين أدوات القوة، لذلك ارتفع الاعتماد على هذه الشبكات. حتى الحركات المسلحة لم تعد تعتمد على القوة العسكرية فقط في تحقيق أهدافها، بل تلجأ إلى استخدام وسائل التواصل وشبكة الإنترنت بشكل واسع ودعائي لأفكارها وتحركاتها، وأيضاً للحصول على الدعم المادي والمعنوي، وكأداة جديدة لنشر أفكارها ومعتقداتها وزيادة عدد المنتمين لها عبر تجنيدهم باستخدام تلك المواقع العابرة للحدود القومية، ومن دون استخدام تلك الأدوات لم يكن بمقدور هذه التنظيمات أن تحقق أهدافها مع توفير ذلك الوقت والجهد، بالإضافة لميزة الابتعاد والتخفي بعيداً عن قبضة الأجهزة الأمنية للدول المستهدفة. وتقوم وسائل التواصل الاجتماعي بدوراً كبيراً ومؤثراً في المنطقة العربية وخارجها كما أضحت تلك الشبكات الأداة الأهم في يد الجماعات الإرهابية لوضع خططها وتنفيذ أهدافها.**(Joseph Nye, 2008, 11)**

دور الإنترنت وشبكات التواصل الاجتماعي في الإرهاب الإلكتروني

للإنترنت وشبكات التواصل الاجتماعي دور كبير في الإرهاب الإلكتروني حيث تقليل العبء المادي، والاعتماد على آلية منخفضة التكلفة يتيح نشر المعلومات غير الصحيحة وتضليل الآخرين، ونشر الفيروسات، وتغيير هيئة المعلومات بطريقة لا يمكن التعامل معها، بالإضافة إلى إتاحة تدفق المعلومات وتسهيل تشكيل المجموعات وتقليل تكلفة تجنيد الأعضاء وإيجاد حوافز حماسية للمشاركة، كما انها تدعم وتعزز وجود هوية جماعية ووجود إحساس وانتماء بين أفراد المجموعة الواحدة، حيث تربطهم قضية واحدة، وهدف مشترك، وقيم متماثلة، وإيجاد مجتمعات للتواصل الإلكتروني يتشارك أعضاؤها الأفكار والنقاش، وتتيح تأسيس علاقات واسعة، وتُمكن من قيام علاقات وجهاً لوجه، رغم من بعد المسافات الجغرافية **(Garrett, R. K, 2006, 5-6)**.كل هذه المميزات وبإمكانات تقنية بسيطة يمكن تعلمها، وسيتم فيما يلي توضيح أهم لغات برمجة الإنترنت .

لغات برمجة الإنترنت:

يعتمد الإنترنت على عدة لغات برمجية أهمها كما ذكر مضر عدنان:(مضر عدنان زهران، 2011، ص ص 19-31)

1-لغة **HT ML (Hyper Text Markup Language)**

لغة على درجة كبيرة من البساطة بحيث يمكن اتقانها في فترة بسيطة، وتتميز بسهولة تعديلها وإعادة برمجتها، وهي على بدائيتها قادرة على انتاج صفحات إنترنت ومواقع شاملة وعالية الجودة.

2-لغة **Dynamic HTML**

وهي امتداد للغة **HTML** إلا أنها أكثر ذكاءاً، حيث أن كل المعلومات متوفرة في الموقع الذي تم بناؤه، حيث يتم تنزيل برنامج المستخدم بمجرد دخول الموقع، وتكون المعلومات سريعة التحميل ومتحركة أيضاً.

3-لغة **Java Script**

وتُعد لغة البرمجة الأكثر رواجاً، وتعتمد بشكل أساسي على العمليات الحسابية، وهي من أفضل ما تم ابتكاره في عالم لغات برمجة الإنترنت منذ فترة.

4-لغة **XML**

لغة مبنية على لغة **Java**، وآخذه في الانتشار لسهولة التعامل معها، وتطابق نتائجها مع **Java**.

5-لغة **XTML**

خليط بين لغتي **HTML** و**XML** وأخذت في الانتشار إلا أنها لا تغني عن اللغات الأخرى.

6-برنامج **Front Page**

تطوير لبرامج فرونت بيج السابقة لبناء مواقع الإنترنت، ويمتاز بإدخال الكود أوتوماتيكياً، وما على المبرمج إلا إدخال النص ورسم الشكل الذي يريد الحصول عليه، وتحميله على الموقع الذي يريد.

ونظراً لسهولة البرمجة والأهمية المتزايدة للإنترنت وشبكات التواصل الاجتماعي، فقد لجأ الارهابيون لتوظيفها على أربعة أهداف رئيسية أو مستويات كالتالي:

التنسيق عبر وسائل التواصل الاجتماعي: يعتبر "تويتر" أحد أهم وسائل التواصل الاجتماعي التي تستخدم للتفاعل والتنسيق أثناء عمليات الاختراق والإرهاب الإلكتروني، وتكمن الميزة الأساسية في "تويتر" بالنسبة إليهم في أنه يوفر مجتمعات افتراضية متغيرة، تتكون بصورة تلقائية خلال الأحداث الكبرى، إلى جانب استخدام الإنترنت كوسيلة لتنسيق العمليات الإرهابية التي تتم على أرض الواقع، فإنها تستخدم كذلك لتنفيذ هجمات إرهابية افتراضية على المواقع الإلكترونية المهمة، ولسرقة أرقام بطاقات الائتمان أو استهداف البنية التحتية للدول التي تعتمد على أجهزة الحاسوب الرقمي بهدف تعطيلها أو مهاجمة أهداف اقتصادية لإيقافها عن العمل. **(James A. Lewis, 2002, 193-194)**

نشر الأفكار والمعتقدات الارهابية: يعتبر "فيسبوك" من أكثر وسائل التواصل الاجتماعي استخداماً في نشر الأفكار والمعتقدات الارهابية، وغالباً ما تقوم الجماعات الإرهابية بإنشاء "مجموعة" (**Group**) على "فيسبوك"، حيث تركز المجموعة في أطروحاتها على فكرة إنسانية بالأساس، ومع زيادة عدد الأعضاء المنتمين لهذه المجموعة، فإن المواد الجهادية يتم وضعها تدريجياً بطريقة لا تستهجن الأفعال الجهادية أو تدينها في الوقت نفسه، حتى لا تنتهك سياسة

"فيسبوك"، ثم يتم بعد ذلك توجيه أعضاء المجموعة مباشرة إلى المواقع أو المنتديات المرتبطة بالجماعة الإرهابية. ويُمكِّن "فيسبوك" بهذه الطريقة من تجنيد الأعضاء من أنحاء العالم كافة من دون أن يمثل ذلك تهديداً لأمن المنظمة. **(Geoff Dean, Peter Bell, Jack Newan, 2012, 194-195)**

ساحة افتراضية للتدريب: وعلى سبيل المثال تستخدم الجماعات المسلحة "فيسبوك" لنشر رسائلها، كما تستخدم الجماعات المسلحة "يوتيوب" من أجل شرح كيفية القيام بهجمات أو استخدام الأسلحة.

الحصول على الدعم المادي والمعنوي: استخدمت الجماعات الإرهابية مواقع التواصل الاجتماعي لتسهيل التحويلات الماليّة فيما بينها، بجانب الحصول على الدعم المادي، في ظل سهولة استخدام تلك المواقع لتحويل التبرعات والدعم المالي، مع عدم إمكانية التحقق من هوية متلقى تلك التبرعات في بعض الأحيان. (فيفيان عقيقي، 2014, 1)

أسباب اهتمام تلك التنظيمات الإرهابية بوسائل التواصل الاجتماعي:

- البعد عن سيادة الدول، كما هي الحال في وسائل التواصل التقليدية التقليدي.
- إتاحتها للجميع وصعوبة السيطرة عليها عبر أجهزة محددة، إضافة إلى القدرة على التحايل على المراقبة الأمنية وفتح مواقع وحسابات أخرى بسهولة.
- تقدم هذه الشبكات خدمة الاتصال والتواصل السريع بين الأعضاء والمؤيدين بطرق شتى.
- توفر مواقع التواصل لهذه التنظيمات منصات إعلامية دعائية لأنشطتها وأفكارها.
- إمكانية النشر المكثف للصور والأفلام والوثائق التي تدعم الأفكار التي تروج لها لجذب المؤيدين. (سامي التتر، سعيد الحميداني، 2014، 2)

أمن المعلومات

أمن المعلومات هو العلم الذي يبحث في نظريات واستراتيجيات توفير حماية المعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء عليها. وعُرف تقنياً بمجموعة الوسائل والأدوات والإجراءات اللازم توفيرها لضمان حماية المعلومات من الأخطار الداخلية والخارجية. وتدابير حماية سرية وسلامة المحتوى وتوفر المعلومات ومكافحة أنشطة الاعتداء عليها او استغلال نظمها في ارتكاب الجريمة (الجرائم الإلكترونية). واستخدام اصطلاح أمن المعلومات **Information Security** في نطاق انشطة معالجة ونقل البيانات بواسطة وسائل الحوسبة والاتصال، اذ مع شيوع الوسائل التقنية لمعالجة وخزن البيانات وتداولها والتفاعل معها عبر شبكات المعلومات-وتحديدا الإنترنت – احتلت ابحاث ودراسات أمن المعلومات مساحة رحبة آخذة في النماء من بين أبحاث تقنية المعلومات المختلفة، بل ربما أمست أحد الهواجس التي تؤرق مختلف الجهات.

المخاطر والاعتداءات في بيئة المعلومات ؟؟

إن التقدم الكبير في تقنية المعلومات وعبر الإنترنت أدى إلى زيادة أعداد الأماكن والمنافذ، التي يمكن التسلل من خلالها واختراق الأنظمة، وإلى زيادة تعقيدات عمليات إدارة هذه الأنظمة والحفاظ عليها، حيث ظهرت تحسينات على أدوت التطفل والاختراق. وقد صنف الخبراء المختصين بالقضايا الأمنية عبر الشبكات والإنترنت أنواع التهديدات الهجوم المحتمل إلى: الهجوم التقني والهجوم غير التقني. ويختص البحث بالهجوم التقني الذي يتم عبر الشبكات، حيث يستخدم المهاجم طريقة الحيلة والدهاء لخداع العاملين بالمؤسسة التعليمية أو غير التعليمية، للحصول على تصاريح وأذونات استخدام الخدمات، والحصول على المعلومات واختراق أمن الشبكات وهو ما يسمى "الهجوم الاجتماعي"(خضر الطيطي، 2010، ص ص 45-43)

وتظهر المخاطر والاعتداءات في بيئة المعلومات في أربعة مواطن أساسية هي مكونات تقنية المعلومات:

1-الأجهـــــــــزة: وهي كافة المعدات والأدوات المادية التي تتكون منها النظم، كالشاشات والطابعات ومكوناتها الداخلية ووسائط التخزين المادية وغيرها.

2-البرامـج: وهي الأوامر المرتبة في نسق معين لإنجاز الأعمال، وهي إما مستقلة عن النظام أو مخزنة.

3-المعطيـــات: انها العقل الحي للأنظمة، وما سيكون محلاً لجرائم الكمبيوتر، وتشمل كافة البيانات المدخلة والمعلومات المستخرجة عقب معالجتها، وتمتد بمعناها الواسع للبرمجيات المخزنة داخل النظم. والمعطيات قد تكون في طور الإدخال أو الإخراج او التخزين أو التبادل بين النظم عبر الشبكات، وقد تخزن داخل النظم أو على وسائط التخزين خارجه.

4-الاتصـــالات: وتشمل شبكات الاتصال التي تربط اجهزة التقنية بعضها بعض محلياً ونطاقاً ودولياً وتتيح فرصة اختراق النظم عبر ها، كما أنها بذاتها محل للاعتداء وموطن من مواطن الخطر الحقيقي.

ومحور الخطر الانسان (طالب-أستاذ-مسئول تقني)، سواء المستخدم أو الشخص المناط به مهام تقنية معينة تتصل بالنظام والمواقع التعليمية على الإنترنت وشبكات التواصل الاجتماعي، حيث أنه من خلال اختراق حساب واحد فقط يمكن الدخول على جميع الحسابات لإجراء عمليات إرهاب إلكتروني، فإدراك هذا الشخص حدود صلاحياته، وادراكه آليات التعامل مع الخطر، وسلامة الرقابة على أنشطته في حدود احترام حقوقه القانونية، مسائل رئيسة يعنى بها نظام أمن المعلومات الشامل ضد الإرهاب الإلكتروني. تحديدا في بيئة العمل التعليمية المرتكزة على نظم الكمبيوتر وقواعد البيانات.

إجراءات البحث:

للإجابة عن السؤال الأول الذي نص على " ما التهديدات وأشكال الإرهاب الإلكتروني والصعوبات والتحديات التي تواجه مستخدم الإنترنت وشبكات التواصل الاجتماعي لحماية أمن المعلومات والبرمجيات"؟

تم الإجابة عن السؤال البحثي كالآتي:

على الرغم من الآفاق الواسعة التي فتحتها شبكة الإنترنت وخدماتها المتنوعة وشبكات التواصل الاجتماعي، وعلى الرغم من المتعة التي يعيشها المتعلم عند استخدامه لخدماتها أو ابحاره في صفحاتها، تبقى المشكلة العالقة هي كيفية تأمين الحماية الشخصية التي باتت هاجساً يشغل بال المستخدمين ومطوري صناعة خدمات تكنولوجيا المعلومات والإنترنت على حد سواء.

لقد أصبح الاعتماد على الإنترنت وشبكات التواصل الاجتماعي كبيراً كواحدة من وسائل الاتصال الهامة في مختلف حقول التعليم بشكل أبرز أهمية التركيز على المخاطر التي قد تنتج جراء ذلك الاستخدام. وقد نتج عن ذلك مخاطر وتهديدات أمنية، وقد توصل البحث الحالي إلى أهم هذه التهديدات كما يلي:

1-الاصابة بالفيروسات المدمرة للبيانات والمعلومات المخزنة على الحاسوب.

2-الاختراق للعبث بملفات المستخدمين.

3-اختراق حاسوب الأشخاص واستغلال ذلك بقصد الإساءة إلى آخرين.

4-سرقة البيانات الشخصية بقصد الانتحال أو الابتزاز.

5-سرقة بطاقات الائتمان.

6-نشر الخوف والفزع والرعب وبث الكراهية.

7-نشر فيروسات الحاسب الآلي بين مستخدمي شبكة الإنترنت.

8-هجمات الشفرات البرمجية على برامج التواصل الاجتماعي وخاصة فيس بوك **Face Book**

9-الاختراق بإجراء تغييرات في البرامج أو في البيئة التي تعمل فيها.

10-فقد الملفات المخزنة وتحطم نظام التشغيل على الجهاز.

11-اختراق المواقع الإلكترونية لتغيير محتوياتها.

12-سرقة معلومات سرية من مستخدمي الشبكة.

13-تعطيل الموقع عن العمل والسيطرة عليه بشكل كامل.

14-المواقع الإلكترونية التي تنشر وتروج أفكارها الغير سليمة في مختلف أنحاء العالم.

15-تقنيات التجسس المتطورة داخل الشبكة العنكبوتية لمراقبة معلومات المستخدمين حول العالم.

16-التهديد الإلكتروني بأساليبه المتنوعة ما بين تهديدات بتفجيرات، أو التهديد بإطلاق الفيروسات التي من شأنها تدمير أنظمة معلومات بالكامل.

17-القصف الإلكتروني من خلال توجيه مئات الآلاف من الرسائل الإلكترونية الى مواقع هذه الشبكات لتسبب ضغط كبير عليها المواقع، وتفقدها قدرتها ويوقفها عن العمل.

18-تدمير أنظمة المعلومات باختراق شبكة المعلومات الخاصة بالشركات العالمية أو بالأفراد بهدف تخريب نقطة الاتصال، وتخليق أنواع جديده من الفيروسات تسبب الدمار لأجهزة الكمبيوتر وللمعلومات.

19-فشل عام في شبكة الاتصالات في الدولة المستهدفة والتي تعتمد بنيتها التحتية أو شبكات اتصالاتها على الكمبيوتر.

20-تهديد الديدان كبرامج مستقلة، تتكاثر عن طريق نسخ نفسها عن طريق الشبكات وإذا لم تتمكن من تدمير البيانات فإنها تقوم بقطع الاتصالات وتغيير شكل المعلومات.

21-أحصنة طروادة كبرامج صغيرة مختبئة في برنامج أكبر، بإرسال البيانات عن الثغرات الموجودة في النظام وإرسال كلمات المرور السرية.

22-القنابل المنطقية التي يزرعها المبرمج داخل النظام الذي يطوره أو أن تكون برامج مستقله.

23-الأبواب الخلفية وهي ثغرة تترك عن عمد من مصمم النظام للتسلل اليه عند الحاجة، والجدير بالذكر أن الكثير من البرامج والنظم التي تطورها الولايات المتحدة الأمريكية تحتوي على أبواب خلفية تستخدمها عند الحاجة.

24-الإرهابيين الذين يستخدمون الفضاء الإلكتروني في جمع المعلومات والتجنيد والتخطيط للأعمال الإرهابية.

للإجابة عن السؤال الثاني والذي نص على " ما دور تكنولوجيا المعلومات في مواجهة الصعوبات والتحديات والإرهاب الإلكتروني والتهديدات المرتبطة باستخدام الإنترنت وشبكات التواصل الاجتماعي؟

تم الإجابة عن السؤال البحثي كالاتي:

رغم الدور الحيوي الذي تقوم به تكنولوجيا المعلومات لمنع وصد أي هجوم إلكتروني محتمل، إلا إنه ليست هناك ضمانات كاملة للحماية من الإرهاب الإلكتروني والتهديدات المرتبطة باستخدام الإنترنت وشبكات التواصل الاجتماعي إلا إذا أدرك والتزم كل مستخدم ومسئول في المواقع التعليمية بدوره المنوط به. في هذه الحالة فقط هناك إجراءات وقائية تحمي المستخدم من خطر الإصابة، وإجراءات علاجية في حالة الإصابة، توفرها تكنولوجيا المعلومات لحماية المواقع التعليمية والمستخدمين حول العالم. وقد أكد على ذلك "دانيال مكارثي **Daniel R. McCarthy**" حيث ذكر أنه يجب معاملة تكنولوجيا المعلومات في عالمنا العصري كمؤسسات دولية، وذلك لدورها الهام في حل مشكلات الإرهاب الإلكتروني والتهديدات الأمنية. **(Daniel R. McCarthy, 2015, 124)**

أيضاً توفير تكنولوجيا المعلومات الأمن والسلامة لضمان سلامة المستخدم نفسه من التعرض للاستغلال أو الابتزاز أو الانتهاك والإساءة، بالإضافة إلى أنها اصطلاح يستخدم للإشارة إلى حماية الأشخاص والمجتمعات المؤسسات التعليمية أثناء استخدامهم لشبكة الإنترنت وشبكات التواصل الاجتماعي، وتوفير الحماية لضمان أمن المعلومات والبيانات والخصوصية الشخصية. وهي بذلك تشمل حماية الملفات والعتاد والبنى التحتية وقد تم التوصل إلى أهم أدوار تكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني، بغرض حماية المستخدم أثناء العمل على الانترنت ووسائل التواصل الاجتماعي كما يلي:

1-استخدام برامج مكافحة الفيروسات والجدران النارية **(firewalls)** لتأمين جهاز الحاسوب وتحديثها باستمرار.

2-استخدام برامج الكشف عن الملفات الخبيثة كملفات التجسس والملفات الدعائية والملفات التي تسيطر على متصفح الإنترنت.

3-فحص الملفات المحملة من المواقع غير المعروفة أو خدمات مشاركة الملفات.

4-فحص الملفات الواردة عن طريق البريد الإلكتروني.

5-استخدام برامج تشفير الملفات.**(files encryption)**

7-استخدام مرشحات رسائل البريد الإلكتروني **(filters)** وخدمات مكافحة البريد غير المرغوب فيه.**(anti-spam)**

8-عمل نسخ احتياطي للملفات المهمة بشكل دوري.

9-الحذر أثناء استخدام برامج المحادثة الفورية، وفحص الملفات التي ترد قبل فتحها.

10-استخدام مواقع فحص المنافذ **(ports)** للتأكد من عدم وجود منافذ مفتوحة للمخترقين، وتعرف تلك المواقع باسم.**(online port scanners)**

10-اجراء عمليات التحديث الضرورية والدورية لبيئة التشغيل المستخدمة لسد الثغرات الأمنية.

11-تجنب فتح الحسابات المصرفية على الشبكة أو ارسال أرقام بطاقات الائتمان عبر الشبكات اللاسلكية **(Wi-Fi)** غير الآمنة.

12-في حالة الاستعانة بخبراء تعليميين خارج المؤسسة التعليمية، يجب معرفة مع من تتعامل قبل الكشف عن أية معلومات.

13-تجنب الافصاح عن أية معلومات شخصية في خدمات المشاركة الحية كغرف المحادثة والمنتديات التعليمية.

14-استخدام التقنيات البصرية والصوتية الحديثة وبصمة العين للدخول على الحسابات الشخصية.

15- عدم ارسال أية معلومات مهمة مثل كلمات السر وأرقام بطاقات الائتمان عبر البريد الإلكتروني.

16-استخدم كلمات سر صعبة التخمين وتجنب المعلومات العامة كتواريخ الميلاد وأرقام الهواتف، واستخدم المزج بين الأحرف الصغيرة والكبيرة والأرقام والرموز.

17-تجنب خاصية التخزين التلقائي للمعلومات الشخصية على الحواسيب التي تخصك والتي لا تخصك في حال استخدامها.

18-القيام بعملية مسح ملفات **(cookies)** بين فترة وأخرى.

19- استخدام أنظمة مراقبة الشبكة للتنبيه عن نقاط الضعف التأمينية.

20 -فصل كاميرا الويب في حال عدم استخدامها.

21-استخدم كلمات سر للملفات الهامة.

22-تجنب الرد على رسائل البريد الإلكتروني غير المعروفة.

عند القيام بعملية الشراء الإلكتروني للمواد التعليمية عبر مواقع الإنترنت، يتم التأكد من الآتي:

23-استخدم المواقع العلمية والمكتبات الرقمية المعروفة، وتأكد من أن الموقع يمتلك عنواناً فعلياً وأرقام اتصال واطلع على سياسة الموقع العلمي وشروط الخدمة.

24-عند الشروع في علمية الدفع بواسطة بطاقة الائتمان، تأكد من ظهور صورة القفل **(padlock)**في أسفل الصفحة أو نافذة العنوان.

25-اضـغط على القفل لتظهر لك معلومات الشـهادة الإلكترونية، وتأكد أن الشـهادة منحت لنفس عنوان الموقع. وتأكد من أن بادئة عنوان الموقع قد تغيرت من **(http)** الى**(https)** .

26-يمكنك الاسـتعانة بميزة الدفع عن طريق طرف ثالث، كتلك التي توفرها شـركات مثل **(PayPal)**و**.(money bookers)**

27-استخدم بطاقات الائتمان الافتراضية بدلاً من استخدام البطاقات التقليدية.

28-استخدام ميزة الخصوصية في المتصفح لحظر المواقع غير المرغوبة.

29-استخدام جهازاً منفصلاً للأطفال، وقم باستخدام حساب منفصل لهم على نفس الجهاز لتقليل مخاطر الإصابة بالإرهاب الإلكتروني والتهديدات.

30-استخدام أنظمة مراقبة الشبكة.

31- استخدام الشهادات الرقمية وأنظمة كشف الاختراق وتحديثها.

32-دعم أجهزة عدم انقطاع التيار.

33-استخدام أنظمة الحوسبة السحابية المدعومة بتشفير كامل لمعلومات وبيانات المستخدمين.

34-أنظمة الكشف عن الدخلاء والشبكات الافتراضية الخاصة.

35-استخدام أنظمة الدفاع ضد الكود التخريبي.

نتائج البحث:

قامت الباحثة بالتوصـل إلى نتائج البحث الحالي من خلال الإجابة عن أسـئلة البحث، وهي كما يلي:

أولاً: للإجابة عن السـؤال الأول للبحث ينص السـؤال الأول للبحث على: "ما التهديدات الأمنية والصعوبات والتحديات التي تواجه مستخدم الإنترنت وشبكات التواصل الاجتماعي لحماية أمن المعلومات والبرمجيات والأجهزة؟

قامت الباحثة بحساب التكرارات والنسب المئوية والمتوسط الوزني والانحراف المعياري لكل عبارة من عبارات استبانة التهديدات الأمنية والصعوبات والتحديات التي تواجه مستخدم الإنترنت وشـبكات التواصـل الاجتماعي لحماية أمن المعلومات والبرمجيات والأجهزة والتي تتكون من (24) تهديداً أو صـعوبة أو تحدياً، وذلك بهدف ترتيب هذه التهديدات الأمنية والصـعوبات والتحديات التي تواجه مستخدم الإنترنت وشـبكات التواصـل الاجتماعي لحماية أمن المعلومات والبرمجيات والأجهزة لمعرفة أكثرها خطورة، والجدول التالي يوضح النتائج:-

جدول (1) التكرارات والنسب المئوية والمتوسط الوزني والانحراف المعياري لكل عبارة من عبارات استبانة التهديدات الأمنية والصعوبات والتحديات التي تواجه مستخدم الإنترنت وشبكات التواصل الاجتماعي

رقم العبارة	مضمون العبارة	الإحصاء	الاستجابة						المتوسط الوزني*	الانحراف المعياري	درجة التحقق والترتيب
			أوافق بشدة	أوافق	لا أوافق ولا أختلف	لا أوافق	أختلف بشدة	غير قابل للتطبيق			
1	الإصابة بالفيروسات المدمرة للبيانات والمعلومات المخزنة على الحاسوب	التكرار	16	13	1	10	6	1	4.43	1.6	مرتفعة 1
		النسبة	34.0	27.7	2.1	21.3	12.8	2.1			
2	اختراق جهاز الحاسب الآلي للعبث بملفات المستخدم	التكرار	14	10	3	11	8	1	4.17	1.5	متوسطة 13
		النسبة	29.8	21.3	6.4	23.4	12.8	2.1			
3	استغلال الحاسب الآلي للأشخاص بقصد الإساءة إلى آخرين	التكرار	12	9	6	10	10	0	4.06	1.5	متوسطة 20
		النسبة	25.5	19.1	12.8	21.3	21.3	0			
4	سرقة البيانات الشخصية بقصد الانتحال أو الابتزاز	التكرار	16	11	1	9	9	1	4.28	1.7	متوسطة 5
		النسبة	34.0	23.4	2.1	19.1	19.1	2.1			
5	سرقة الحسابات الشخصية وبطاقات الائتمان	التكرار	10	16	3	8	10	0	4.17	1.4	متوسطة 12
		النسبة	21.3	34.0	6.4	12.8	21.3	0			
6	نشر الخوف والفزع والرعب وبث الكراهية	التكرار	8	12	7	10	9	1	3.94	1.5	متوسطة 24
		النسبة	12.8	25.5	14.9	21.3	19.1	2.1			
7	نشر فيروسات الحاسب الآلي بين مستخدمي شبكة الإنترنت	التكرار	10	14	5	10	8	0	4.17	1.3	متوسطة 11
		النسبة	21.3	29.8	10.6	21.3	12.8	0			
8	هجمات الشفرات البرمجية على برامج التواصل الاجتماعي وخاصة Face Bookفيس بوك	التكرار	9	12	7	10	9	0	4.04	1.4	متوسطة 21
		النسبة	19.1	25.5	14.9	21.3	19.1	0			
9	الاختراق بإجراء تغييرات في البرامج أو في البيئة التي تعمل فيها	التكرار	8	15	8	8	5	3	4.09	1.5	متوسطة 19
		النسبة	12.8	31.9	12.8	12.8	10.6	6.4			
10	فقد الملفات المخزنة وتحطم نظام التشغيل على جهاز لحاسب الآلي	التكرار	7	16	6	14	4	0	4.17	1.2	متوسطة 10
		النسبة	14.9	34.0	12.8	29.8	8.5	0			
11	اختراق المواقع الإلكترونية لتغيير محتوياتها	التكرار	7	17	7	11	5	0	4.21	1.3	متوسطة 7
		النسبة	14.9	36.2	14.9	23.4	10.6	0			
12	سرقة معلومات سرية من مستخدمي الشبكة	التكرار	7	19	2	10	9	0	4.11	1.4	متوسطة 17
		النسبة	14.9	40.4	4.3	21.3	19.1	0			
13	تعطيل الموقع عن العمل أو السيطرة	التكرار	10	10	9	10	8	0	4.09	1.4	متوسطة 18
		النسبة	21.3	21.3	19.1	21.3	12.8	0			
14		التكرار	12	12	5	10	6	2	4.17	1.6	متوسطة 14

				4.3	12.8	21.3	10.6	25.5	25.5	النسبة	المواقع الإلكترونية التى تنشر وتروج افكارها الغير سليمة فى مختلف أنحاء العالم
15	تقنيات التجسس المتطورة داخل الشبكة العنكبوتية لمراقبة معلومات المستخدمين حول العالم	التكرار	10	16	9	6	6	0	4.38	1.3	مرتفعة 2
		النسبة	21.3	34.0	19.1	12.8	12.8	0			
16	التهديد الإلكترونى بأساليبه المتنوعة ما بين تهديد بالاغتيال أو التهديد بإطلاق الفيروسات التى من شأنها تدمير أنظمة معلومات بالكامل	التكرار	10	15	5	9	8	0	4.21	1.4	متوسطة 8
		النسبة	21.3	31.9	10.6	19.1	12.8	0			
17	القصف الإلكتروني من خلال توجيه مئات الالاف من الرسائل الإلكترونية إلي المواقع لتفقدها قدرتها على العمل	التكرار	8	17	4	12	6	0	4.19	1.3	متوسطة 9
		النسبة	12.8	36.2	8.5	25.5	12.8	0			
18	تدمير أنظمة المعلومات باختراق شبكة المعلومات العالمية أو بالأفراد بهدف تخريب نقطة الاتصال	التكرار	8	12	8	11	7	1	4.00	1.4	متوسطة 22
		النسبة	12.8	25.5	12.8	23.4	14.9	2.1			
19	فشل عام فى شبكة الاتصالات فى الدولة المستهدفة والتى تعتمد بنيتها التحتية أو شبكات اتصالاتها على الكمبيوتر	التكرار	8	12	5	15	6	1	3.96	1.4	متوسطة 23
		النسبة	12.8	25.5	10.6	31.9	12.8	2.1			
20	تهديد الديدان كبرامج مستقلة، تتكاثر عن طريق نسخ نفسها لتدمير البيانات وقطع الاتصالات وتغيير شكلها	التكرار	7	14	9	12	4	1	4.11	1.3	متوسطة 16
		النسبة	14.9	29.8	19.1	25.5	8.5	2.1			
21	أحصنة طروادة كبرامج صغيرة مختبئة في برامج أكبر	التكرار	6	17	10	9	5	0	4.21	1.2	متوسطة 6
		النسبة	12.8	36.2	21.3	19.1	10.6	0			
22	القنابل المنطقية التى يزرعها المبرمجين داخل الأنظمة	التكرار	5	17	10	10	4	1	4.13	1.2	متوسطة 15
		النسبة	10.6	36.2	21.3	21.3	8.5	2.1			
23	الأبواب الخلفية كثغرة للتسلل إلى المستخدمين	التكرار	8	15	10	10	4	0	4.28	1.2	متوسطة 4
		النسبة	12.8	31.9	21.3	21.3	8.5	0			
24	الإرهابيين الذين يستخدمون الفضاء الإلكتروني في جمع المعلومات والاعمال الإرهابية	التكرار	15	10	4	11	7	0	4.32	1.5	متوسطة 3
		النسبة	31.9	21.3	8.5	23.4	14.9	0			

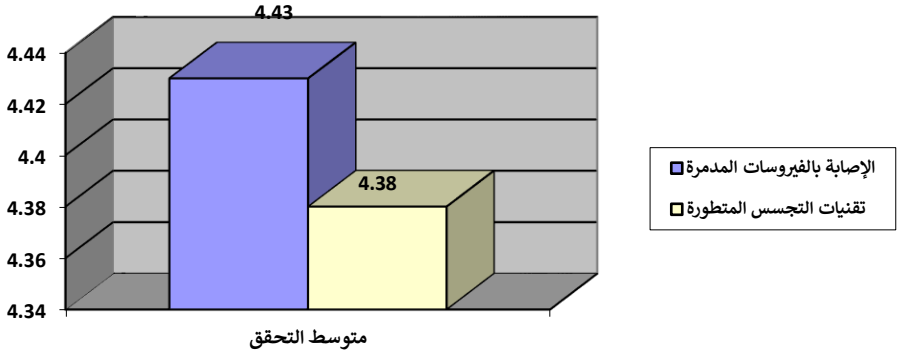
***من (1) حتى أقل من (2.67) تعني أن التهديد منخفض.**
من (2.67) حتى أقل من (4.34) تعني أن التهديد متوسط.
من (4.34) حتى (6.00) تعني أن التهديد مرتفع.

يتضح من نتائج الجدول السابق أن جميع التهديدات الأمنية والصعوبات والتحديات التي تواجه مستخدم الإنترنت وشبكات التواصل الاجتماعي لحماية أمن المعلومات والبرمجيات والأجهزة، تحققت بدرجة متوسطة، ما عدا تهديدين تحققا بدرجة مرتفعة وهما كما يلي:-

- تهديد "الإصابة بالفيروسات المدمرة للبيانات والمعلومات المخزنة على الحاسوب"، وتحقق بدرجة مرتفعة بمتوسط بلغت قيمته (4.43) وكان أكثر التهديدات تحققاً من وجهة نظر عينة البحث.

- تهديد "تقنيات التجسس المتطورة داخل الشبكة العنكبوتية لمراقبة معلومات المستخدمين حول العالم"، وتحقق بدرجة مرتفعة بمتوسط بلغت قيمته (4.38) وكان في الترتيب الثاني من حيث أكثر التهديدات تحققاً من وجهة نظر عينة البحث.

والشكل التالي يوضح التهديدات التي تحققت بدرجة مرتفعة.



شكل رقم (1) التهديدات الأمنية والصعوبات والتحديات التي تواجه مستخدم الإنترنت وشبكات التواصل الاجتماعي التي تحققت بدرجة مرتفعة.

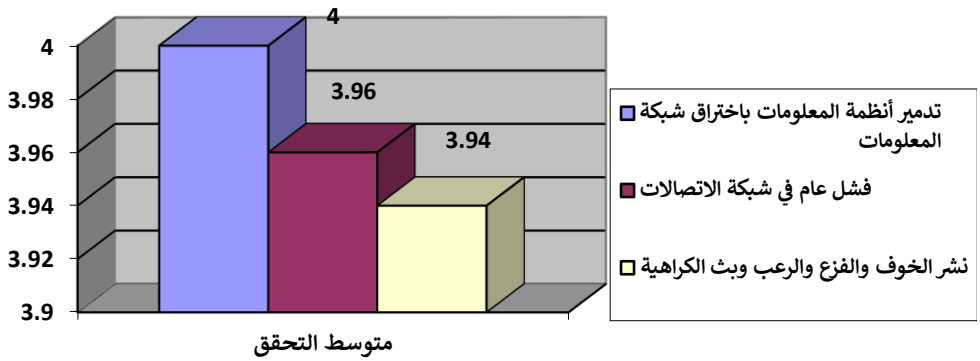
كما يتضح من نتائج الجدول السابق أن أقل ثلاث تهديدات أمنية وصعوبات وتحديات تواجه مستخدم الإنترنت وشبكات التواصل الاجتماعي لحماية أمن المعلومات والبرمجيات والأجهزة، وتحققت بدرجة متوسطة هي كما يلي:-

- تهديد "تدمير أنظمة المعلومات باختراق شبكة المعلومات العالمية أو بالأفراد بهدف تخريب نقطة الاتصال"، وتحقق بدرجة متوسطة بمتوسط بلغت قيمته (4.00) وكان في الترتيب الثاني والعشرين من حيث أكثر التهديدات تحققاً من وجهة نظر عينة البحث.

- تهديد "فشل عام في شبكة الاتصالات في الدولة المستهدفة والتي تعتمد بنيتها التحتية أو شبكات اتصالاتها على الكمبيوتر"، وتحقق بدرجة متوسطة بمتوسط بلغت قيمته (3.96) وكان في الترتيب الثالث والعشرين وقبل الأخير من حيث أكثر التهديدات تحققاً من وجهة نظر عينة البحث.

- تهديد "نشر الخوف والفزع والرعب وبث الكراهية"، وتحقق بدرجة متوسطة بمتوسط بلغت قيمته (3.94) وكان في الترتيب الرابع والعشـــرين والأخير من حيث أكثر التهديدات تحققاً من وجهة نظر عينة البحث.

والشكل التالي يوضح أقل ثلاثة تهديدات والتي تحققت بدرجة متوسطة.



شكل رقم (2) أقل ثلاث تهديدات أمنية وصعوبات وتحديات تواجه مستخدم الإنترنت وشبكات التواصل الاجتماعي التي تحققت بدرجة متوسطة.

ويتضح إجمالاً أن أعلى التهديدات الأمنية والصعوبات والتحديات التي تواجه مستخدم الإنترنت وشبكات التواصل الاجتماعي لحماية أمن المعلومات والبرمجيات والأجهزة هو تهديد "الإصابة بالفيروسات المدمرة للبيانات والمعلومات المخزنة على الحاسوب"، وتحقق بدرجة مرتفعة بمتوسط بلغت قيمته (4.43)، بينما كان أقلها هو تهديد "نشر الخوف والفزع والرعب وبث الكراهية"، وتحقق بدرجة متوسطة بمتوسط بلغت قيمته (3.94) وكان في الترتيب الرابع والعشرين والأخير.

ثانياً:- الإجابة عن السؤال الثاني للبحث:-

ينص السؤال الثاني للبحث على:- "ما دور تكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والتهديدات الأمنية المرتبطة باستخدام الإنترنت وشبكات التواصل الاجتماعي لحماية أمن المعلومات والبرمجيات والأجهزة؟.

وللإجابة عن هذا السؤال قامت الباحثة بحساب التكرارات والنسب المئوية والمتوسط الوزني والانحراف المعياري لكل عبارة من عبارات استبانة دور تكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والتهديدات الأمنية المرتبطة باستخدام الإنترنت وشبكات التواصل الاجتماعي لحماية أمن المعلومات والبرمجيات والأجهزة، والتي تتكون من (35) دوراً، وذلك بهدف ترتيب أدوار تكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والتهديدات الأمنية المرتبطة باستخدام الإنترنت وشبكات التواصل الاجتماعي لحماية أمن المعلومات والبرمجيات والأجهزة لمعرفة أكثرها قوة، والجدول التالي يوضح النتائج:-

جدول (2) التكرارات والنسب المئوية والمتوسط الوزني والانحراف المعياري لكل عبارة من عبارات استبانة دور تكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والتهديدات الأمنية المرتبطة باستخدام الإنترنت وشبكات التواصل الاجتماعي

رقم العبارة	مضمون العبارة	الإحصاء	الاستجابة						المتوسط الوزني*	الانحراف المعياري	درجة التحقق والترتيب
			أوافق بشدة	أوافق	لا أوافق ولا أختلف	لا أوافق	أختلف بشدة	غير قابل للتطبيق			
1	اتباع سياسات محددة منها استخدام برامج مكافحة الفيروسات والجدران النارية لتأمين الحاسب وتحديثها باستمرار	التكرار	35	11	1	0	0	0	5.72	0.5	مرتفعة 1
		النسبة	74.5	23.4	2.1	0	0	0			
2	استخدام برامج الكشف عن الملفات الخبيثة كملفات التجسس	التكرار	26	19	1	1	0	0	5.48	0.7	مرتفعة 9
		النسبة	55.3	40.4	2.1	2.1	0	0			
3	فحص الملفات التي تم تنزيلها من مواقع غير معروفة"	التكرار	29	16	2	0	0	0	5.57	0.6	مرتفعة 5
		النسبة	61.7	34.0	4.3	0	0	0			
4	فحص الملفات الواردة عن طريق البريد الإلكتروني"	التكرار	29	18	0	0	0	0	5.62	0.5	مرتفعة 3
		النسبة	61.7	38.3	0	0	0	0			
5	استخدام برامج تشفير الملفات (files encryption)	التكرار	28	18	1	0	0	0	5.57	0.5	مرتفعة 4
		النسبة	59.6	38.3	2.1	0	0	0			
6	استخدام مرشحات رسائل البريد الإلكتروني (filters)وخدمات مكافحة البريد غير المرغوب فيه (anti-spam).	التكرار	13	19	11	2	0	2	4.79	1.16	مرتفعة 31
		النسبة	27.7	40.4	23.4	4.3	0	4.3			
7	استخدم ميزة الخصوصية في (privacy) المتصفح لحظر المواقع غير المرغوبة والموجودة في خيارات الإنترنت (internet options) في قائمة الأدوات (tools).	التكرار	17	20	7	2	0	1	5.04	1.0	مرتفعة 25
		النسبة	36.2	42.6	14.9	4.3	0	2.1			
8	اجراء نسخ احتياطي للملفات بشكل دوري	التكرار	25	14	8	0	0	0	5.4	0.8	مرتفعة 24
		النسبة	53.2	29.8	17.0	0	0	0			
9	الحذر في حال استخدام برامج المحادثة الفورية	التكرار	17	21	7	2	0	0	5.13	0.8	مرتفعة 22
		النسبة	36.2	44.7	14.9	4.3	0	0			
10	استخدام مواقع فحص المنافذ للتأكد من عدم	التكرار	22	23	2	0	0	0	5.42	0.6	مرتفعة 13
		النسبة	46.8	48.9	4.3	0	0	0			

رقم العبارة	مضمون العبارة	الإحصاء	الاستجابة						المتوسط الوزني*	الانحراف المعياري	درجة التحقق والترتيب
			أوافق بشدة	أوافق	لا أوافق ولا أختلف	لا أوافق	أختلف بشدة	غير قابل للتطبيق			
	وجود منافذ مفتوحة للمخترقين										
11	القيام بالتحديثات الضرورية والدورية لبيئة التشغيل لسد الثغرات الأمنية	التكرار	20	24	1	2	0	0	5.32	0.7	مرتفعة 17
		النسبة	42.6	51.1	2.1	4.3	0	0			
12	تجنب فتح الحسابات المصرفية أو ارسال أرقام بطاقات الائتمان عبر الشبكة اللاسلكية غير الامنة مثل المطارات	التكرار	22	20	4	1	0	0	5.34	0.7	مرتفعة 15
		النسبة	46.8	42.6	8.5	2.1	0	0			
13	معرفة مع من تتعامل قبل الكشف عن أي معلومات شخصية	التكرار	34	12	1	0	0	0	5.70	0.5	مرتفعة 2
		النسبة	72.3	25.5	2.1	0	0	0			
14	استخدام التقنيات البصرية الحديثة وبصمة العين للدخول على الحسابات الشخصية	التكرار	26	14	7	0	0	0	5.40	0.7	مرتفعة 14
		النسبة	55.3	29.8	14.9	0	0	0			
15	عدم ارسال أية معلومات مهمة مثل كلمات السر وأرقام بطاقات الائتمان عبر البريد الإلكتروني	التكرار	18	17	11	1	0	0	5.11	0.8	مرتفعة 23
		النسبة	38.3	36.2	23.4	2.1	0	0			
16	استخدام كلمات مرور صعبة التخمين	التكرار	28	17	1	1	0	0	5.53	0.7	مرتفعة 6
		النسبة	59.6	36.2	2.1	2.1	0	0			
17	تجنب خاصية التخزين التلقائى للمعلومات الشخصية علي الحاسب	التكرار	18	17	9	2	0	1	5.02	1.1	مرتفعة 27
		النسبة	38.3	36.2	19.1	4.3	0	2.1			
18	مسح ملفات Cookies كل فترة	التكرار	15	23	7	1	0	1	5.04	1.1	مرتفعة 26
		النسبة	31.9	48.9	14.9	2.1	0	2.1			
19	فصل كاميرا الويب فى حال عدم استخدامها	التكرار	10	7	23	1	0	6	4.17	1.5	متوسطة 34
		النسبة	21.3	14.9	48.9	2.1	0	12.8			
20	استخدام أنظمة مراقبة الشبكة للتنبيه عن نقاط الضعف التأمينية وعمل سياسة للنسخ الاحتياطي.	التكرار	27	17	3	0	0	0	5.51	0.6	مرتفعة 7
		النسبة	57.4	36.2	6.4	0	0	0			
21	استخدام كلمات سر للملفات الهامة	التكرار	25	18	4	0	0	0	5.45	0.7	مرتفعة 11
		النسبة	53.2	38.3	8.5	0	0	0			
22	تجنب الرد علي رسائل البريد غير المعروفة	التكرار	21	20	6	0	0	0	5.32	0.6	مرتفعة 16
		النسبة	44.7	42.6	12.8	0	0	0			
23	الاطلاع على سياسة المواقع التجارية وشروط خدماتها قبل استخدامها	التكرار	20	21	4	2	0	0	5.26	0.8	مرتفعة 19
		النسبة	42.6	44.7	8.5	4.3	0	0			
24		التكرار	26	16	4	1	0	0	5.43	0.7	مرتفعة

رقم العبارة	مضمون العبارة	الإحصاء	الاستجابة						المتوسط الوزني*	الانحراف المعياري	درجة التحقق والترتيب
			أوافق بشدة	أوافق	لا أوافق ولا أختلف	لا أوافق	أختلف بشدة	غير قابل للتطبيق			
	استخدام المواقع التجارية المعروفة	النسبة	55.3	34.0	8.5	2.1	0	0			12
25	التأكد من ظهور صورة القفل في أسفل الصفحة أو نافذة العنوان قبل الشروع في استخدام بطاقات الائتمان	التكرار	16	25	5	1	0	0	5.19	0.7	مرتفعة 20
		النسبة	34.0	53.2	10.6	2.1	0	0			
26	الاستعانة بميزة الدفع عن طريق طرف ثالث التي توفرها بعض الشركات"	التكرار	13	11	14	4	1	4	4.40	1.5	مرتفعة 33
		النسبة	27.7	23.4	29.8	8.5	2.1	8.5			
27	استخدام بطاقات الائتمان الافتراضية بدل البطاقات التقليدية	التكرار	13	17	14	3	0	0	4.85	0.9	مرتفعة 30
		النسبة	27.7	36.2	29.8	6.4	0	0			
28	استخدام ميزة الخصوصية في المتصفح لحظر المواقع غير المرغوبة	التكرار	22	24	1	0	0	0	5.45	0.5	مرتفعة 10
		النسبة	46.8	51.1	2.1	0	0	0			
29	توفير جهاز منفصل لاستخدام الاطفال، أو استخدام حساب منفصل لهم "	التكرار	23	18	4	1	1	0	5.30	0.9	مرتفعة 18
		النسبة	48.9	38.3	8.5	2.1	2.1	0			
30	استخدام أنظمة مراقبة الشبكة للتنبيه عن نقاط الضعف التأمينية	التكرار	17	24	5	0	0	1	5.17	0.9	مرتفعة 21
		النسبة	36.2	51.1	10.6	0	0	2.1			
31	استخدام أنظمة كشف الاختراق وتحديثها	التكرار	26	19	2	0	0	0	5.51	0.7	مرتفعة 8
		النسبة	55.3	40.4	4.3	0	0	0			
32	دعم أجهزة عدم انقطاع التيار الكهربي"	التكرار	10	19	14	1	1	2	4.64	1.2	مرتفعة 32
		النسبة	21.3	40.4	29.8	2.1	2.1	4.3			
33	استخدام أنظمة الحوسبة السحابية المدعومة بتشفير كامل لمعلومات وبيانات المستخدمين	التكرار	16	18	9	2	1	1	4.91	1.1	مرتفعة 29
		النسبة	34.0	38.3	19.1	4.3	2.1	2.1			
34	استخدام الشبكات الافتراضية الخاصة	التكرار	12	24	10	1	0	0	5.00	0.8	مرتفعة 28
		النسبة	25.5	51.5	21.3	2.1	0	0			
35	استخدام أنظمة الدفاع ضد الكود التخريبي.	التكرار	10	19	14	1	1	2	4.64	1.2	مرتفعة 32
		النسبة	21.3	40.4	29.8	2.1	2.1	4.3			

***من (1) حتى أقل من (2.67) تعني أن دور تكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والتهديدات الأمنية منخفض.**

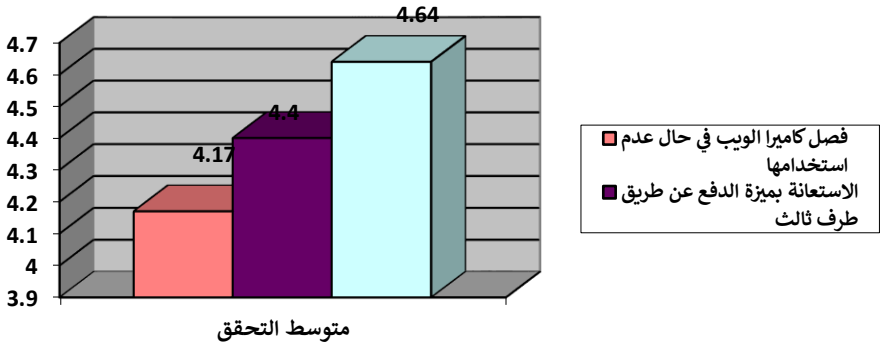
***من (2.67) حتى أقل من (4.34) تعني أن دور تكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والتهديدات الأمنية متوسط.**

***من (4.34) حتى (6.00) تعني أن دور تكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والتهديدات الأمنية مرتفع.**

يتضـــح من نتائج الجدول الســـابق أن جميع أدوار تكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والتهديدات الأمنية المرتبطة باستخدام الإنترنت وشبكات التواصل الاجتماعي لحماية أمن المعلومات والبرمجيات والأجهزة، تحققت بدرجة مرتفعة، ما عدا دور واحد لتكنولوجيا المعلومات تحقق بدرجة متوسطة وهو كما يلي:-

- "فصل كاميرا الويب في حال عدم استخدامها"، وتحقق بدرجة متوسطة بمتوسط بلغت قيمته (4.17) وكان أقل أدوار تكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والتهديدات الأمنية المرتبطة باســتخدام الإنترنت وشــبكات التواصــل الاجتماعي لحماية أمن المعلومات والبرمجيات والأجهزة من وجهة نظر عينة البحث.

والشــكل التالي يوضــح أقل ثلاث أدوار لتكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والتهديدات الأمنية.



شكل رقم (3) أقل ثلاث أدوار لتكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والتهديدات الأمنية.

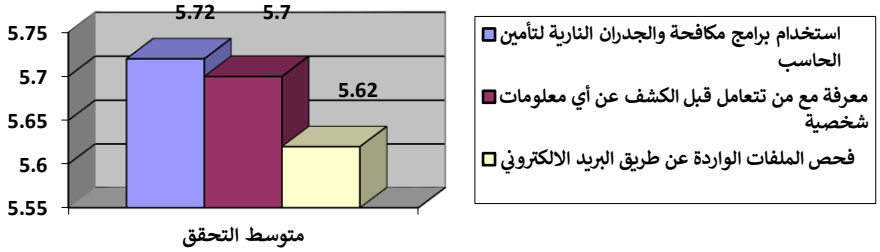
كما يتضـــح من نتائج الجدول الســـابق أن أكثر ثلاث أدوار لتكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والتهديدات الأمنية المرتبطة باســتخدام الإنترنت وشــبكات التواصــل الاجتماعي لحماية أمن المعلومات والبرمجيات والأجهزة، وتحققت بدرجة مرتفعة، هي كما يلي:-

- دور تكنولوجيا المعلومات في "اتباع ســياســات محددة مثل اســتخدام برامج مكافحة الفيروســات والجدران النارية لتأمين الحاســب وتحديثها باســتمرار"، وتحقق بدرجة مرتفعة بمتوســط بلغت قيمته (5.72) وكان في الترتيب الأول من حيث أكثر أدوار تكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والتهديدات الأمنية المرتبطة باســتخدام الإنترنت وشــبكات التواصــل الاجتماعي لحماية أمن المعلومات والبرمجيات والأجهزة تحققاً من وجهة نظر عينة البحث. لذلك يجب إتباع سياسات محددة لحماية أمن المعلومات.

وهذا ما أكدت علية دراسة " هرس وآخرون Hearth & others "على أهمية الالتزام التنظيمي في حماية أمن المعلومات ووضع سياسات أمن للكمبيوتر لضمان أمن المعلومات وذلك لمستخدمي نظم المعلومات التنظيمية، وإلا ضاعت الجهود سدى، كما اكدت على أهمية إتباع المستخدمين لهذه السياسات، حيث قام البحث على فرضية أن ممارسات أمن المعلومات والسياسات تتأثر بالعوامل التنظيمية والبيئية والسلوكية وتطوير الحافز والردع. واعتمدت الدراسة أداة استطلاع الرأي (Hearth & others, 2009,p2-18).

- دور تكنولوجيا المعلومات في "معرفة مع من تتعامل قبل الكشف عن أي معلومات شخصية"، وتحقق بدرجة مرتفعة بمتوسط بلغت قيمته (5.70) وكان في الترتيب الثاني من حيث أكثر أدوار تكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والتهديدات الأمنية المرتبطة باستخدام الإنترنت وشبكات التواصل الاجتماعي لحماية أمن المعلومات والبرمجيات والأجهزة تحققاً من وجهة نظر عينة البحث.
- دور تكنولوجيا المعلومات في "فحص الملفات الواردة عن طريق البريد الإلكتروني"، وتحقق بدرجة مرتفعة بمتوسط بلغت قيمته (5.62) وكان في الترتيب الثالث من حيث أكثر أدوار تكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والتهديدات الأمنية المرتبطة باستخدام الإنترنت وشبكات التواصل الاجتماعي لحماية أمن المعلومات والبرمجيات والأجهزة تحققاً من وجهة نظر عينة البحث.

والشكل التالي يوضح أكثر ثلاث أدوار لتكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والتهديدات الأمنية المرتبطة باستخدام الإنترنت وشبكات التواصل الاجتماعي لحماية أمن المعلومات والبرمجيات والأجهزة والتي تحققت بدرجة مرتفعة.



شكل رقم (4) أكثر ثلاث أدوار لتكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والتهديدات الأمنية.

ويتضح إجمالاً أن أكثر أدوار لتكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني والتهديدات الأمنية المرتبطة باستخدام الإنترنت وشبكات التواصل الاجتماعي لحماية أمن المعلومات والبرمجيات والأجهزة هو دورها في "استخدام برامج مكافحة الفيروسات والجدران النارية

لتأمين الحاسب وتحديثها باستمرار"، وتحقق بدرجة مرتفعة بمتوسط بلغت قيمته (5.72)، بينما كان أقلها هو دورها في "فصل كاميرا الويب في حال عدم استخدامها"، وتحقق بدرجة متوسطة بمتوسط بلغت قيمته (4.17) وكان في الترتيب الرابع والثلاثين والأخير.

توصل البحث إلى التهديدات الأمنية والصعوبات والتحديات التي تواجه مستخدمي شبكة الإنترنت وشبكات التواصل الاجتماعي لحماية أمن المعلومات والبرمجيات" من خلال وضع قائمة تحتوي تلك الصعوبات والتهديدات الإلكترونية الأمنية التي تواجه مستخدمي الإنترنت وشبكات التواصل الاجتماعي، تحتوي22 معياراً. وقد أثبت البحث أهمية دور تكنولوجيا المعلومات في مواجهة الإرهاب الإلكتروني وحماية أمن المعلومات والبرمجيات والأجهزة ، والحد من التهديدات الأمنية أثناء استخدام الإنترنت وشبكات التواصل الاجتماعي وذلك من خلال إيجاد قائمة من الحلول شملت54 معيارا أو حلاً، لعلاج مشكلات أمن المعلومات والبرمجيات والأجهزة، والحد من الإرهاب الإلكتروني والتهديدات الأمنية منها، تأمين حسابات المستخدمين للإنترنت وشبكات التواصل وكذلك نظم التحقق الدقيق من الهوية، وتأمين خطوط الدفاع الامامية واستخدام الجدران النارية، بالإضافة إلي استخدم أنظمة الحوسبة السحابية المدعومة بتشفير كامل لمعلومات وبيانات المستخدمين، واستخدام الشبكات الافتراضية الخاصة.

وقد اتفقت دراسة ميشيل كروز "Michael Krousz" مع الدراسة الحالية حيث أكد على أهمية أن يُعتمد في حفظ أمن المعلومات على تكنولوجيا المعلومات للحفاظ على أنظمة أمنة ومأمونة، ولتوفير إطاراً مناسباً للتنفيذ الفعال والتدابير المضادة لحماية المعلومات في جميع أشكالها. (Michael Krousz, 2010, p196)، لكن هذه الحلول ليست نهائية لأنها تحتاج باستمرار إلى استحداث آليات وبرامج لحماية أمن المعلومات والبرمجيات والأنظمة والبنى التحتية، كلما طور المخترقين والقراصنة الإلكترونيين برامجهم.

توصيات البحث:

بناءً على ما تم التوصل اليه من نتائج يوصي البحث بالآتي:

-إتباع الإجراءات الوقائية التي تحمي المستخدم من خطر الإصابة بالإرهاب الإلكتروني والإجراءات العلاجية في حالة الإصابة، توفر ها تكنولوجيا المعلومات لحماية لمستخدمي الإنترنت وشبكات التواصل الاجتماعي، والتي تم التوصل اليها بالبحث الحالي.

-وضع سياسات مع ضرورة إلزام مستخدمي نظم المعلومات إتباع تلك السياسات لضمان أمن المعلومات.

- ضرورة السعي إلى عقد مؤتمر دولي بإشراف هيئة الأمم المتحدة يتم من خلاله تحديد تعريف الإرهاب الإلكتروني والتهديدات الأمنية الإلكترونية، وتحديد خطة عملية دولية لمكافحته.

- الدعوة إلى زيادة التعاون على المستوى الوطني والعربي والدولي للتنسيق بين الأجهزة المختصة بمكافحة الإرهاب الإلكتروني، لتبادل الخبرات والتجارب، بما في ذلك التدريب لضمان الفعالية في محاربة الإرهابيين والجريمة المنظمة الكترونياً.

-السعي إلى إنشاء منظمة عربية لتنسيق أعمال مكافحة الإرهاب عبر الشبكات المعلوماتية والأنظمة الإلكترونية وتشجيع قيام اتحادات عربية تسعي للتصدي لجرائم الإرهاب الإلكتروني.

-حث الدول إلى الإسراع والانضمام إلى الاتفاقيات الدولية الخاصة بمكافحة جرائم الإرهاب وخاصة المعاهدة الدولية لمكافحة جرائم المعلوماتية.

المراجع :

1. إبراهيم، مجدي عزيز. (2009). **المؤتمر القومي السنوي السادس عشر (التعليم الجامعي العربي ودوره في تطوير التعليم قبل الجامعي "تكنولوجيا المعلومات كيف تكون حلقة وصل بين التعليم الجامعي وقبل الجامعي"**، مركز تطوير التعليم الجامعي. جامعة عين شمس، القاهرة
2. اريك شميدت، جارين كوين. (2013). **العصر الرقمي الجديد**، الدار العربية ناشرون، ط1.
3. بشير، هشام. (2012). **"الإرهاب الإلكتروني في ظل ثورة المعلومات"**، دورية آراء عن مركز الخليج للأبحاث -الإمارات
4. بو عزة، عبد المجيد. (1991). **الندوة العربية الثانية للمعلومات (تقنيات المعلومات والاتصالات في الوطن العربي -تحديات المستقبل)**، تكنولوجيا المعلومات: أداة قوة أم وسيلة تهديد لحرية الإنسان؟، تونس.
5. زهران، مضر عدنان. زهران، عمر عدنان. (2011). **التعليم عن طريق الإنترنت**، دار زهران للنشر والتوزيع، عمان.
6. عبد الصبور، سماح. (2014). **المستقبل للأبحاث والدراسات المتقدمة، "الإرهاب الرقمي، أنماط استخدام الجماعات المسلحة للإرهاب الشبكي"**، دورية (اتجاهات الأحداث) الصادرة عن مركز المستقبل، العدد الثاني، كلية الاقتصاد والعلوم السياسية - جامعة القاهرة
7. التتر، سامي، الحميداني، سعيد. (2014) **الإرهاب يغزو شبكات التواصل الاجتماعي: تحريض. تجنيد. ودعاية سوداء**، موقع مجلة اليمامة، 2016/7/24، موجود على الرابط التالي: http://www.alriyadh.com/alyamamah/article/955131
8. عيسى، نتاشا. (2014). **"تعريف تقنية المعلومات"**، من موقع موضوع أكبر موقع عربي بالعالم بتاريخ 1437/11/1 http://mawdoo3.com/
9. عقيقي، فيفيان. (2014). **"الإرهاب على مواقع التواصل الاجتماعي: كل ما يجب أن تعرفه"**، جريدة النهار، 24 يوليو 2014، موجود على الموقع التالي: http://www.annahar.com
10. البحيري، ولاء. (2012). **مستقبل الإرهاب الإلكتروني-تحديات وأساليب المواجهة**، المركز الدولي للدراسات المستقبلية والاستراتيجية، مجلة النهضة، القاهرة.
11. الحسبان، عطا الله أحمد سويلم. (2009). **الرقابة الداخلية والتدقيق في بيئة تكنولوجيا المعلومات**، دار الراية للنشر والتوزيع، عمان، الأردن.
12. الزبن، بدرة هويمل. (2012). **الإرهاب في الفضاء الإلكتروني-دراسة مقارنة**، رسالة دكتوراه غير منشورة، جامعة عمان العربية، كلية الحقوق، الأردن

13. الطيطي، خضر مصباح اسماعيل. (2010). **"أساسيات أمن المعلومات والحاسوب"**، الحامد للنشر والتوزيع، الأردن.
14. العجلان، عبد الله عبد العزيز فهد. (1015). **"الإرهاب المعلوماتي"** المؤتمر الدولي الأول لمكافحة الجرائم المعلوماتية، جامعة الإمام محمد بن سعود الإسلامية، كلية علوم الحاسب والمعلومات
15. العسافين، عيسى. (2007). **تكنولوجيا المعلومات دراسة في مفهومها وأبعادها ومشاكل نقلها الى الدول العربية**، مجلة مكتبة الملك فهد الوطنية –السعودية مجلد 12، العدد 7 المملكة العربية السعودية
16. المري، عايض. (2016). **" امن المعلومات ماهيتها واستراتيجياتها "** من موقع الدليل للدراسات والاستشارات القانونية بتاريخ 1437/11/2 http://www.dralmarri.com/Contact_A.asp
17. المؤتمر العلمي الثاني لمكافحة الجرائم المعلوماتية. (2017). **"مكافحة الجرائم المعلوماتية"**، جامعة الملك خالد، أبها، المملكة العربية السعودية.
18. طوالبية، محمد. (2017). **" الامن في العالم الافتراضي دراسة في سيكولوجية الإرهاب الإلكتروني"**، كلية العلوم الإنسانية والاجتماعية، جامعة حسيبة بو علي بالشلف، مجلة الأكاديمية للدراسات الاجتماعية والإنسانية، العدد 18، يناير 2017.
19. مدينة الملك عبد العزيز للعلوم والتكنولوجيا. (2016). من موقع مدينة الملك عبد العزيز للعلوم التكنولوجيا، بتاريخ 1437/10/29 http://www.kacst.edu.sa/ar/research/pages/it.aspx
20. مسعى، محي محمد. (1999). **" ظاهرة العولمة الأوهام والحقائق"**، ط1، مطبعة ومكتبة الشعاع، جمهورية مصر العربية.
21. مؤتمر القمة العالمي لمجتمع المعلومات. (2003). "توصيات مؤتمر القمة العالمي لمجتمع المعلومات جنيف 2003 وتونس العاصمة، من موقع – بتاريخ 2016/6/20 http://www.un.org/arabic/conferences/wsis/fact6.
22. مؤتمر أمن المعلومات لمنطقة الشرق الأوسط وشمال افريقيا. (2017). **"اقتصاد الإنترنت يواجه مخاطر اختراقات القراصنة**، البوابة العربية للتقنية، الرياض، المملكة العربية السعودية.
23. مؤتمر أمن المعلومات والتكنولوجيا. (2017). **"أمن الشبكات والمعلومات"**، القاهرة، جمهورية مصر العربية.
24. Amold, Nike; Paulus, Trena. (2010)**."Using a Social networking site for experiential learning Appropriating**, lurking, modeling and community building, The Internet and Higher Education, Vol.13, Issue 4, Journal Article: https://doi- org.sdl.idm.oclc.org/10.1016/j.iheduc.2010.04.002

25. Copyright Agence France-Presse (AFP), (2017). **All content is provided by AFP on an "AS IS" and "AS AVAILABLE" basis without any warranty of any kind**. Users assume the risk of use of the content and any information contained therein, including any losses and charges incurred by AFP related to user's misuse
26. Daniel R. McCarthy. (2015). **"Power, Information Technology, and International Relations**, Theory The Power and of us foreign policy and Internet, pol grave Macmillan
27. Garrett, R. K. (2009) "**Protest in an Information Society: A Review of Literature on Social Movements and New ICTs Information ,"Communication and Society ,**Vol. 9, No. 2
28. Geoff Dean, Peter Bell, Jack Newan. (2012).**The Dark Side of Social Media: Review of Online Terrorism** ,Pakistan Journal of Criminology ,Vol. 3, No. 4, April – July
29. Gregory Daniel. (2017). "**AFP International Text Wire in Arabic**", Agence France-Presse, ProQuist Central, Washington, United States. https://search-proquest com.sdl.idm.oclc.org/publisherlinkhandler/sng/jsu/General+Interest+Periodicals--United+States/$N?accountid=142908,
30. Herath, Tejaswini; Rao, H Raghav. (2009). **Protection motivation and deterrence: a framework for security policy compliance in organizations**, European Journal of Information Systems.
31. James A. lewis , Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats ,Center for Strategic and International Studies ,December 2002 , available at: http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf
32. Joseph ،Nye(2002**). "The Paradox of American Power: Why the World's Only Super Power Cannot Go It Alone** ",(Oxford University Press)
33. Joseph ،Nye.(2008)"**Smart Power and The War on Terror**", Asia Pacific Review, Vol. 15, no1.
34. Wodzicki, Katrin; Schwammlein, Eva; Moskaliuk, Johannes. (2012). **"Actually I Wanted to Learned": Study-related knowledge exchange on Social networking sites**, The Internet and Higher Education, Journal Article, Vol 15, Issue1
35. https://doi-org.sdl.idm.oclc.org/10.1016/j.iheduc.2011.05.008
36. Longley, D. Shain, M. (1985). **Macmillan Dictionary of Information Technology**, London, Macmillan press
37. MENA Report; London (2014). **Information Technology and Information Security information System** {Tender de Cuments: T24346624}

38. Michael Krousz. (2010). **Managing Information Security Breaches: Studies From Real Life**, IT Governane LTD.
39. Philip ,Sei & Dana M. Janbek.(2011). **Global Terrorism and New Media: The Post-Al Qaeda Generation** ,(New York: Rutledge)
40. http://www.skynewsarabia.com/web/article/948200
41. Rowley, J. E. (1988). **The Basic of in information Technology**. London: Clive Bingley
42. Hamid, Suraya; Waycott, Jenny; Kurnia, Sherah; More. (2015). **Understanding Students of the benefits of Online Social networking use for Teaching and Learning**, Vol. 26,
43. Journal article https://doi-org.sdl.idm.oclc.org/10.1016/j.iheduc.2015.02.004
44. Zhiyong Li & Suling Jia. (2014). **Application of Information Security Technology in Risk Assessment of insurance Companies**, Zhongrong Life insurance co., LTD., pacific Mansion, Beijing ,China.

The effectiveness of information technology in the face of cyber terrorism and the challenges associated with the use of the Internet and social networks

Dr. Samah Sayed Ahmed Mohamed Dakroury

Assistant Professor of Educational Technology - King Khalid University

Instructor of educational technology - Assiut University

ORCID:

Keywords:

Information technology, cyber terrorism, information security, education platforms, the Internet and social networking.

Abstract:

The use of the Internet and social networking in education. The reason for the nature of these networks and their openness and lack of connection to a particular state or undaries and the difficulty of controlling what is published in them; electronic terrorism on the Internet and communication networks become a reality. Weillers & Others is a professor of the Oberation of the Oberating. The current research aims to study the effectiveness of information technology in the face of terrorism and Internet control. The researcher has designed a questionnaire to identify forms and images of cyber terrorism and the threats used by the Internet and social networks to protect the security of information, software and devices. And another questionnaire to determine the effectiveness of information technology in the face of terrorism and control the use of the Internet, and solutions to address electronic terrorism and threats facing users on the Internet and social networks, to protect the security of information and software and devices to them. Excellent English teacher. The results relate to the effectiveness of information technology in the face of terrorism and protection from the use of the Internet, through solutions such as securing Internet user accounts and networks as well as identity verification systems, securing defense lines and using firewalls, using an eye print, Other.