كلية التربية

تفعيل دور التربية لمواجهة الإرهاب الإلكتروني

إعداد

أ.م.د/ أماني محمد شريف عبد السلام

أستاذ التخطيط التربوي المساعد

كلية التربية – جامعة أسيوط

أكتوبر 2020

تفعيل دور التربية لمواجهة الإرهاب الإلكتروني

المستخلص

في ظل ما يشهده العالم اليوم من تطور هائل في تكنولوجيا الاتصالات والمعلومات ، وفى ظل الاستخدام السلبي لها، ظهرت صور وأشكال جديدة من الإرهاب أطلق عليها الإرهاب الإلكتروني ، الذي ظهر وشاع استخدامه عقب الطفرة الكبيرة التي حققتها تكنولوجيا المعلومات واستخدامات الحواسب الآلية بصفة عامة ، والإنترنت بصفة خاصة في إدارة معظم الأنشطة الحياتية.

وتناولت الدراسة الحالية مفهوم الإرهاب الإلكتروني ، وسماته، وأسباب انتشاره ، وأضراره. كما تناولت الاتجاهات الحديثة لمواجهة الإرهاب الإلكتروني ، والمتمثلة في تجارب بعض الدول، والهيئات الدولية والحقوقية ، ودور التربية في التصدي لآثاره المدمرة على المجتمعات والأفراد.

وقد توصلت الدراسة إلى أن مواجهة الإرهاب الإلكتروني تتطلب من المؤسسات التربوية تبني أدوار جديدة في إعداد النشء للحياة في العصر الرقمي ، ووضع تصور شامل تتبناه المؤسسات التربوية ، وذلك من خلال تدعيم ثقافة الاستخدام الرشيد للمواقع الإلكترونية ، وتنمية الوعي بمخاطر الإرهاب الإلكتروني، والتأصيل لثقافة الحوار والتفكير الناقد وقبول الآخر.

Abstract

In light of the tremendous development of ICT in the world today, and in the negative use of it, new forms of terrorism have emerged, called cyber terrorism, which emerged and became popular following the great boom in information technology and the use of computers in general, Especially in the management of most life activities.

The current study dealt with the concept of cyber terrorism, its characteristics, the causes of its spread and its damage. And recent trends in countering cyber terrorism, represented by the experiences of some States, international and human rights bodies, and the role of education in addressing its devastating effects on societies and individuals.

The study concluded that countering cyber terrorism requires educational institutions to adopt new roles in the preparation of youth for life in the digital age, and to develop a comprehensive vision adopted by educational institutions through the promotion of a culture of rational use of websites and to raise awareness of the dangers of cyber terrorism and acceptance of the other.

مقدمة

يشكل الإرهاب خطراً كبيراً على سلام وأمن المجتمعات. وعادة ما تكون الأفعال الإرهابية هي الناتج النهائي للتشدد الفكري، والايمان بأفكار متطرفة وتبني العنف كوسيلة لمحاولة التغيير. ويأخذ الإرهاب أشكالاً مختلفة تشمل الجرائم المتعلقة باستخدام العنف لأغراض سياسية، مثل خطف الطائرات واستهداف السفن البحرية واستخدام الأسلحة الكيميائية أو النووية ضد المدنيين، واختطاف الأشخاص وغير ذلك من أشكال استهداف المدنيين.

ونتيجة لما يشهده العالم المعاصر من ثورة كبيرة وطفرة هائلة جلبتها حضارة التقنية في عصر المعلومات، برز مصطلح الإرهاب الإلكتروني أو الإرهاب الرقمي, وشاع استخدامه، مما ترتب عليه زيادة خطورة الجرائم الإرهابية وتعقيدها، سواء من حيث استخدام التكنولوجيا في تسهيل الاتصال بين الجماعات الإرهابية وتنسيق عملياتها، أو من حيث المساعدة على ابتكار أساليب وطرق إجرامية متقدمة باستخدام الانترنت.

ويعتمد الإرهاب الإلكتروني على استخدام الإمكانيات العلمية والتقنية ، واستغلال وسائل الاتصال والشبكات المعلوماتية ، من أجل تخويف وترويع الآخرين ، وإلحاق الضرر بهم, أو بممتلكاتهم، وتهديدهم، والأخطر أن الإرهاب الإلكتروني لم يقتصر خطره فقط على ممارسة الأعمال التخريبية لشبكات الحاسب الآلي والإنترنت، بل امتد ليشمل أنشطة أكثر خطورة، تمثلت في الاستخدام اليومي للإنترنت من قبل المنظمات الإرهابية لتنظيم وتنسيق عملياتهم المتفرقة والمنتشرة حول العالم.

فالجماعات الإرهابية أصبح لها انتشار كبير على الانترنت، تمثل في آلاف الصفحات والمواقع والتي تستخدمها في استقطاب الشباب من مختلف دول العالم، والترويج لأهدافها وللدعاية الخاصة بها، فتنظيم القاعدة على سبيل المثال له العديد من المواقع والصحف الإلكترونية والتي تصدر بلغات مختلفة، ومؤخراً ظهور تنظيم الدولة الاسلامية "داعش" والذى يستخدم الفضاء الإلكتروني بشكل واسع، وله العديد من المواقع الإلكترونية والصحف التي تصدر بلغات مختلفة، ويستخدمها للترويج لأفكاره، حيث يقوم بنشر الأعمال الإرهابية التي يرتكبها والمصورة بتقنية عالية الجودة، وكذلك الترويج لنمط حياة الأفراد في المناطق التي يسيطر عليها التنظيم، لتشكيل صورة ذهنية عنهم بأنهم الأقوى والأخطر عالمياً.

وإذا كان الإرهاب يُعرف بأنه اعتداء على شخص وإصابته بأذى فعلي أو ذعر أو تهديد نفسي فإنه بدخول الحاسب الآلي والانترنت في كل مجالات الحياة اندثرت الحدود بين الإرهاب بمفهومه القديم والإرهاب الإلكتروني الذي أضحى يمثل تهديدا كبيرا في كل مكان، فمن الممكن اقتحام صفحة لمستشفى ما وتهديد حياة المرضى عن طريق تغيير برامج العلاج، ومن الممكن تهديد الاقتصاد باقتحام مواقع البورصة العالمية كما يمكن أيضا التدخل في نظام الاتصالات، والكهرباء أو المياه بل والسيطرة على نظام المواصلات والطائرات وتهديد الأمن القومي بشكل كامل، فقد يصل الأمر إلى التحكم في الشبكات الحكومية وشبكات الأمن وإغلاقها تماما وبذلك تتم السيطرة التامة على الدول من جانب منفذي الهجمات الإلكترونية ويحظى هذه النوع من الإرهاب الرقمي بجاذبية خاصة عند جماعات عديدة وذلك لأن الانترنت مجال مفتوح ليس له حدود، كما يمكن لهذه المجموعات تنفيذ هجمات في بلدان أخرى دون الحاجة إلى أوراق أو تفتيش أو قيود فكل ما يحتاجونه هو بعض المعلومات لتسطيع اقتحام الحوائط الالكترونية كما أن تكاليف القيام بها لا تتجاوز أكثر من حاسب آلي واتصال بشبكة الانترنت فضلا عن صعوبة تعقب الجناة والوصول إليهم. (الرومي، 2008، 86)

وانطلاقاً من أن الإرهاب الإلكتروني أصبح من أخطر أنواع الإرهاب في العصر الحاضر، نظرًا لاتساع نطاق استخدام التكنولوجيا الحديثة في العالم ، لذا فمن المهم دراسة أسبابه، وطرق مكافحته، ولذلك فقد عقدت العديد من المؤتمرات والندوات وأجريت العديد من الدراسات والبحوث حول تلك الظاهرة، من أبرزها على المستوى العربى، الملتقى العلمي الدولي والذى نظمه مركز الملك عبدالله بن عبدالعزيز للدراسات الإسلامية المعاصرة وحوار الحضارات تحت عنوان "الإرهاب الإلكتروني: خطره وطرق مكافحته" وذلك يوم الثلاثاء 1436/1/25هـ الموافق 2014/11/18م ، وندوة "الإرهاب الإلكتروني: المخاطر والمواجهة الأمنية"، والتي نظمتها أكاديمية الشرطة بوزارة الداخلية المصرية في 27 ديسمبر 2015، بهدف إبراز مخاطر الإرهاب الإلكتروني ووضع استراتيجية فاعلة للمواجهة الأمنية له، وكذلك مؤتمر ليبيا الدولي لمكافحة الإرهاب الإلكتروني والذى عقد في مدينة بنغازي خلال الفترة من 9- 11فبراير 2016، ومؤتمر جامعة الامام محمد بن سعود الإسلامية في 17 نوفمبر 2016 الذى عقد تحت عنوان "الإرهاب الإلكتروني: خططه ووسائل مكافحته"، ومؤتمر "الإرهاب الإلكتروني" والذى عقد في

العاصمة اللبنانية بيروت ونظمه معهد التنمية الإدارية خلال الفترة من 12 – 15 فبراير 2017، وأخيرا المؤتمر الدولي لتجريم الإرهاب الإلكتروني والذى عقد بأبي ظبى خلال الفترة من 15 – 16 مايو 2017 بهدف إيجاد أرضية مشتركة، لصياغة منظومة من القوانين الدولية، للتصدي لجذور وامتدادات ظاهرة الإرهاب في الفضاء الرقمي، والذى شارك فيه على مدى يومين، نخبة من أصحاب القرار والخبراء في القانون والجرائم الإلكترونية ومكافحة الإرهاب، من مختلف دول العالم. (الدهشان، 2018، 88)

مما سبق يتضح أن مخاطر ظاهرة الإرهاب بصفة عامة والإرهاب الإلكتروني بصفة خاصة وانتشارها، تتطلب ضرورة دراستها وبحثها من كافة جوانبها وتوعية أفراد المجتمع ومستخدمي شبكات الانترنت والمعلومات بتلك الظاهرة وصورها ومخاطرها وأساليب الوقاية منها ومواجهتها، وتوجيه البحوث والدراسات إلى بحث ودراسة كافة جوانبها بطريقة علمية، وتقديم المقترحات المناسبة لمواجهتها.

مشكلة الدراسة

يعد الإرهاب الإلكتروني هو إرهاب المستقبل، وهو الخطر القادم؛ نظراً لتعدد أشكاله وتنوع أساليبه واتساع مجال الأهداف التي يمكن مهاجمتها بطرق سهلة من خلال وسائل الاتصالات وتقنية المعلومات.

وتتمثل خطورة الإرهاب الإلكتروني بشكل أساسي في سهولته بمعنى القدرة على القيام بالهجمات الإرهابية من أي مكان، وتعدد أشكاله، وتنوع أساليبه وأدواته، وقدرته الهائلة على التخريب والتدمير، وتوفير قدر كبير من الأمان والسلامة للإرهابيين.

وتستخدم الجماعات الإرهابية المواقع الإلكترونية في تحقيق أهدافها، ومخاطبة المجتمعات التي تقوم بترويعها وإرهابها، كما تعتبر المواقع الإلكترونية بمثابة مكتبة إلكترونية هائلة الحجم ، تكتظ بالمعلومات الحساسة التي يسعى الإرهابيون للحصول عليها، وتستخدم أيضاً المواقع الإلكترونية في التخطيط والتنظيم بين الخلايا الإرهابية ، وتبادل المعلومات والحصول على التمويل (Weimann, 2006, 49).

وفي ضوء ما سبق يتبين أن خطورة الإرهاب الإلكتروني وأثاره المدمرة على الأمن الإنساني والقومي تستوجب دراسة هذه الظاهرة ومحاولة توعية أفراد المجتمع الرقمي بصورها ومظاهرها وطرق مواجهتها وكذلك التأكيد على الدور المحوري والمهم الذي يمكن أن تلعبه التربية في مواجهة هذه الظاهرة الغير مسبوقة، وهو ما تسعى هذه الدراسة إلى مناقشته .

أهداف الدراسة :

هدفت الدراسة الحالية إلى التعرف على:

1- الإطار المفاهيمي والنظري لمفهوم الإرهاب الإلكتروني وخصائصه وأسبابه وأشكاله.
2- الاتجاهات الحديثة لمواجهة الإرهاب الإلكتروني.
3- دور التربية في التصدي للإرهاب الإلكتروني.

أسئلة الدراسة:

سعت الدراسة الحالية إلى الإجابة عن الأسئلة التالية :

1- ما مفهوم الإرهاب الإلكتروني، وما خصائصه، وما أسبابه، وأشكاله؟
2- ما الاتجاهات الحديثة التي يأخذ بها العالم لمواجهة الإرهاب الإلكتروني؟
ما دور التربية في التصدي للإرهاب الإلكتروني؟

أهمية الدراسة

تتمثل أهمية الدراسة الحالية في ما يلي:

1- قد تفيد الدراسة الحالية في إلقاء الضوء على أهم مخاطر الإرهاب الإلكتروني وأشكاله المختلفة.
2- تؤكد الدراسة الحالية على أهمية دور التربية في التوعية بالقضايا الحديثة والمخاطر التي تهدد الأمن القومي ، والوقاية منها.
3- قد تفيد الدراسة الحالية القائمين على المؤسسات التربوية في اتخاذ الإجراءات المناسبة لتفعيل دور التربية في مواجهة الإرهاب الإلكتروني ، وحماية الشباب من الوقوع ضحية لهذا النوع من الإرهاب.
4- قد تفيد الدراسة الحالية في توجيه نظر القيادات السياسية وصانعي القرار إلى الدور الحيوي والفعال الذي يمكن أن تقوم به المؤسسات التربوية في مواجهة الأشكال الحديثة

والمستحدثة من الإرهاب وحماية الوطن والشباب منها ، وبالتالي العمل على دعم دور التربية في هذا المجال.

الدراسات السابقة:

أولاً: الدراسات العربية

استهدفت دراسة محمد (2016) التعرف على ماهية ظاهرة الإرهاب الإلكتروني ، وتوضيح التحديات المجتمعية المسببة لظاهرة الإرهاب الإلكتروني، وبيان الدور المأمول للمؤسسات التربوية لمواجهة ظاهرة الإرهاب الإلكتروني. ولتحقيق أهداف الدراسة تم تحليل العديد من الأدبيات والدراسات السابقة حول الإرهاب الإلكتروني ، وتوصلت الدراسة لعدد من النتائج ، أهمها: خطورة هذه الظاهرة على استقرار الوطن وأمنه؛ لما لها من خصائص ووسائل وأشكال متعددة. وأن هناك العديد من التحديات السياسية والاقتصادية والاجتماعية والثقافية والإعلامية وغيرها داخل المجتمع هي الأساس في تنامي وتصاعد خطورة ظاهرة الإرهاب الإلكتروني. وأنه لابد من تعاون العديد من المؤسسات التربوية والمتمثلة في الأسرة، والمدرسة، والجامعة، والمسجد، والإعلام ومراكز الشباب في مواجهة ظاهرة الإرهاب الإلكتروني.

هدفت دراسة سليمان (2016) لوضع رؤية لتعزيز وتفعيل دور وسائل الإعلام الجديد لمواجهة تأثيرات الشائعات المرتبطة بالإرهاب الالكتروني باستخدام استراتيجية معلوماتية تعتمد على المنصات المتعددة، عبر مواقع التواصل الاجتماعي والإعلام الكتروني، ووضع تصور لضبط استخدام المواقع، والمبادرة بالمعلومات الوقائية، التي تعد بناء على اتجاهات "التنقيب على المعلومات عبر الإنترنت Web Mining لدى الجمهور"، سواء على الحواسب الشخصية أو الهواتف الذكية، وتوفير نظام معلوماتي يمتلك القدرة على رصد الشائعات في توقيت مبكر لحظة إطلاقها على تلك المواقع، واستخدمت الدراسة المنهج المسحي، وتم تطبيق الدراسة على عينة قدرها 400 أربعمائة من السعوديين المستخدمين لمواقع التواصل الاجتماعي ووسائل الإعلام الجديد، وتكونت الاستبانة من ستة محاور رئيسة. وتوصلت الدراسة إلى أن تطبيق واتس أب What'sApp هو الاكثر استخداما لدى عينة الدراسة؛ ومتوسط استخدامه (دائما)، يليه في الترتيب موقع التواصل الاجتماعي لتطبيق تويتر Twitter، يليه في الترتيب الثالث تطبيق انستجرام Instagram، ثم استخدام BlackBerry Messenger BBM، وفي الترتيب الاخير

(لأكثر خمس تطبيقات للتواصل الاجتماعي انتشارا لدى العينة) يأتي موقع التواصل الاجتماعي فيسبوك، وكذلك يتضح أن أول هذه الأهداف وأكثرها انتشارا لدى عينة الدراسة هو التواصل والحديث مع الأصدقاء Chating، وتبين أن التفقه في الدين والحصول على المعلومات الدينية. هو المجال الاول الذي يهتم به المستخدمون للإعلام الجديد ومواقع التواصل الاجتماعي، ثم المجال الرياضي ثم الاهتمام بالتراث الحضاري يليه الاهتمام بالجوانب السياسية.

وهدفت دراسة آل علي (2019) إلى توعية المجتمع بخطورة استخدام الجهات والتنظيمات الإرهابية للوسائل الإلكترونية، من خلال دراستها المعنونة "الإرهاب الإلكتروني: دراسة مقارنة"، إذ سعت لاكتشاف وتحديد معالم هذه الظاهرة الخطرة، وتوضيح الدور الذي تؤديه الشبكة العنكبوتية ووسائل التواصل الاجتماعي في نشر أفكار التنظيمات الإرهابية، وتسليط الضوء على أساليب التعامل مع هذه الجرائم شكلاً وموضوعاً من قبل الأجهزة المعنية بما يتناسب مع مخاطرها وآثارها المترتبة عليها. وأوصت الدراسة بضرورة التصدي لأوجه الإرهاب الإلكتروني كحالة سلوكية، ومجابهتها بالطرق العلمية من خلال الوسائل القانونية، وضرورة حجب كل المواقع التي تدعو إلى نشر الأفكار العدوانية، وتشجع على اعتناق الأفكار المحرضة على الكراهية.

وهدفت دراسة خليل (2019) إلى تقديم آليات تربوية مقترحة لمواجهة الإرهاب الإلكتروني لدي طلاب المرحلة الجامعية من وجهة نظر أعضاء هيئة التدريس بجامعة أسوان. واعتمدت الدراسة على المنهج الوصفي. وجاءت الأدوات متمثلة في المقابلات الشخصية واستبانة لمعرفة أسباب سهولة تجنيد الشباب في الإرهاب الإلكتروني، وتم تطبيقهم على عينة من أعضاء هيئة التدريس ومعاونيهم بجامعة أسوان بلغ عددهم (310) عضواً من أربع كليات (كلية التربية–كلية الآداب – كلية الخدمة الاجتماعية–كلية الحقوق) باعتبارها كليات مهتمة بالعلوم والقضايا الاجتماعية. وتوصلت الدراسة إلى مجموعة من النتائج ، أهمها أن البطالة من أهم الأسباب الاقتصادية لتجنيد طلاب المرحلة الجامعية وهي من أقوي العوامل المساهمة في امتهان الجريمة والسرقة وتفشى ظاهرة الإرهاب. كما أشارت النتائج إلى أن التفكك الأسري بكافة أنواعه يعد أحد الأسباب الاجتماعية الرئيسة المؤدية لسهولة تجنيد طلاب المرحلة الجامعية من قبل التنظيمات الإرهابية. وتنوعت الآليات التربوية المقترحة لمواجهة الإرهاب الإلكتروني لدي طلاب

المرحلة الجامعية ما بين الدور التربوي للجامعة، والدور التربوي للأسرة، ودور الحكومة والمجتمع والتي تتمثل في المشاركة السياسية للشباب من مختلف البيئات والطبقات في اتخاذ جميع القرارات التي تمس حياة المواطنين ومبادرة الحكومة بإقامة مشروعات قومية عملاقة تستوعب أعداد كبيرة من الشباب للحد من البطالة

أجرى السبيعي (2020) دراسة ميدانية على مراكز المعلومات والتقنية في الجامعات السعودية بمدينة الرياض، هدفت إلى تحديد دور مراكز المعلومات والتقنية في التوعية من خطر الإرهاب السيبراني في الجامعات السعودية بمدينة الرياض، واستخدمت الدراسة المنهج الوصفي بشقيه التحليلي والمسحي، واعتمدت على الاستبانة كأداة للدراسة، حيث وزعت على (150) من المختصين بمراكز المعلومات والتقنية بالجامعات السعودية في مدينة الرياض. وتوصلت نتائج الدراسة إلى أن أهم صور وأشكال الإرهاب السيبراني، تتلخص فيما يلي: معلومات مضللة– تجنيد أشخاص من قبل أجهزة لاختراق المواقع المهمة– نشر إشاعات تهدد أمن المجتمع عن طريق وسائل التقنية المختلفة– الابتزاز من خلال منصات التواصل الاجتماعي ووسائل التقنية). وأن أهم أدوار مراكز المعلومات والتقنية في التوعية من خطر الإرهاب السيبراني تتلخص فيما يلي:(سن قوانين رادعة لكل مخترق للأمن السيبراني– توعية الأسرة للأبناء من خطر التهديدات الإلكترونية– تنظم المدارس ورش عمل عن الإرهاب السيبراني لتوعية الطلاب– تنسيق الجهود بين الأنظمة المختلفة داخل الدولة للتوعية من خطر الإرهاب السيبراني– تفعيل دور المكافحة الوقائية ضد خطر الإرهاب السيبراني من خلال المؤسسات المجتمعية– اعتماد الهيئة الوطنية للأمن السيبراني على برامج توعوية للتصدي للإرهاب السيبراني)

ثانياً: الدراسات الأجنبية

هدفت دراسة Lester (2018) إلى تحديد كيفية فهم المعلمين وأولياء الأمور وتثقيفهم بشأن سلامة استخدام الإنترنت وحماية الأطفال والطلاب من الإرهاب الالكتروني. واستخدمت الدراسة استطلاع رأي ومقابلات عبر الإنترنت ، وتوصلت الدراسة إلى أن العديد من المعلمين وأولياء الأمور يعملون لمعرفة المزيد عن السلامة على الإنترنت ومراقبة الطلاب والأطفال ولكنهم يشعرون بالإحباط لأن التكنولوجيا تتغير بسرعة كبيرة لدرجة أن جهودهم في بعض الأحيان تبدو غير كافية، وأن إضافة الموارد المجانية للمعلمين وأولياء الأمور إلى قاعدة المعرفة

قد تساعد في هذا الشأن. وأن القنوات الإخبارية وبعض مديري المدارس تبذل بالفعل جهودًا لتثقيف مجتمعاتهم حول التغييرات التكنولوجية حيثما أمكن لإبقاء المعلمين وأولياء الأمور على اطلاع ومساعدة المجتمع على اتخاذ قرارات أفضل لحماية الطلاب والأطفال.

وسعت دراسة Lucas(2018) إلى التعرف على مدى التنمر عبر الإنترنت بين طلاب الجامعات ومدى تنبؤ نظرية التعلم الاجتماعي لرونالد أكيرز بارتكاب التنمر عبر الإنترنت. بالإضافة إلى ذلك ، استكشفت هذه الدراسة استخدام الطلاب لوسائل الإعلام والخصائص المرتبطة بالمشاركة في سلوكيات التسلط عبر الإنترنت كضحايا وجناة ومراقبين. وتوصلت الدراسة إلى أن ما يقرب من 10 ٪ و 37 ٪ و 53 ٪ من عينة الدراسة (ن = 296) تعرضوا للتنمر عبر الإنترنت والإيذاء والملاحظة على التوالي. كما كشفت تحليلات الانحدار السلبي ذي الحدين أن متغيرات التعلم الاجتماعي لم تكن مرتبطة بارتكاب التنمر الإلكتروني أو مراقبته ؛ ومع ذلك ، قدمت النظرية بعض الدعم للتنبؤ بإيذاء الارهاب الالكتروني. بالإضافة إلى ذلك ، كان الوضع الاجتماعي والاقتصادي والعرق مرتبطين إحصائيًا بارتكاب التسلط والارهاب عبر الإنترنت ، بينما ارتبط العمر والإيذاء السابق بإيذاء التنمر عبر الإنترنت.

أجرى(2020) Alshawareb; Alnasraween دراسة هدفت إلى التعرف على مستوى التنمر الإلكتروني من خلال وسائل التواصل الاجتماعي لدى طلاب المرحلة الأساسية في مديرية التربية والتعليم بمنطقة الجامعة ، وتكونت عينة الدراسة من 388 طالب وطالبة من الصفين السابع والعاشر . ولتحقيق هدف الدراسة تم تطوير استبيان للتنمر الإلكتروني والذي يتكون من 30 فقرة في شكله النهائي ، وتم التحقق من صدقه وثباته ، وأظهرت نتائج الدراسة وجود مستوى معتدل من التنمر الإلكتروني في عينة الدراسة. ولا توجد فروق بين المتوسطات الإحصائية حسب الجنس. ولكن توجد فروق ذات دلالة إحصائية تعزى إلى الدرجة ولصالح الصف العاشر.

هدفت دراسة Haseski (2020) إلى تحديد تأثير مهارات الأمن السيبراني الفردية لمعلمي ما قبل الخدمة على مواقفهم تجاه التعليم بمساعدة الحاسوب. وهكذا ، تم تصميم البحث كدراسة ارتباطية. شمل المشاركون في الدراسة 241 من كبار المعلمين قبل الخدمة في أقسام مختلفة في جامعة مانيسا جلال بايار ، كلية التربية خلال العام الدراسي 2019–2020 في

فصل الخريف. تم جمع البيانات باستخدام "مقياس توفير الأمن الإلكتروني الشخصي" و"مقياس الاتجاه نحو التعليم بمساعدة الكمبيوتر". بناءً على نتائج الدراسة ، يجب على المعلمين قبل الخدمة تحسين كفاءاتهم في مجال الأمن السيبراني. علاوة على ذلك ، حصل مدرسو ما قبل الخدمة الذين يمتلكون جهاز كمبيوتر شخصي على درجات أعلى في الحفاظ على الأمن السيبراني الشخصي ولديهم مواقف أفضل تجاه التعليم بمساعدة الكمبيوتر. إلى جانب ذلك ، لوحظ وجود اختلافات بين درجات الأمن السيبراني الشخصية لمعلمي ما قبل الخدمة ومواقفهم تجاه التعليم بمساعدة الكمبيوتر بناءً على أقسامهم. علاوة على ذلك ، تم تحديد أن درجة الإنجاز الشخصي للأمن السيبراني كانت مؤشرا هاما على الموقف تجاه التعليم بمساعدة الكمبيوتر.

جاءت دراسة Touloupis & Athanasiades,(2020) بهدف التعرف على تصورات معلمي تكنولوجيا المعلومات والاتصالات بالمدارس الابتدائية فيما يتعلق بسلوكيات الطلاب المحفوفة بالمخاطر عبر الإنترنت واستجاباتهم للسيناريوهات الافتراضية ذات الصلة. وشارك في الدراسة مائة وثمانية وثلاثون (138) مدرسًا لتكنولوجيا المعلومات والاتصالات (60 رجلاً و 78 امرأة) ، تم اختيارهم عشوائيًا من المدارس في جميع أنحاء اليونان. أكملت العينة مجموعة من استبيانات الإبلاغ الذاتي عبر الإنترنت. وفقًا للنتائج ، أعلن معلمو تكنولوجيا المعلومات والاتصالات أنهم لا يشعرون بالثقة في إدارة سلوكيات الطلاب المحفوفة بالمخاطر عبر الإنترنت، بغض النظر عن وعيهم وتوعيتهم بشأن هذه القضية. وأوصت الدراسة بتصميم إجراءات تدريبية جديدة لمعلمي تكنولوجيا المعلومات والاتصالات فيما يتعلق بمنع الأطفال من مخاطر الملاحة الإلكترونية.

التعليق على الدراسات السابقة

تنوعت الدراسات السابقة من حيث الأهداف ومناهج البحث المستخدمة ، فهدف بعضها إلى تحديد ماهية ظاهرة الإرهاب الإلكتروني ، وتوضيح التحديات المجتمعية المسببة لهذه الظاهرة ، وهدف البعض الآخر لوضع رؤية لتعزيز وتفعيل دور وسائل الإعلام الجديد لمواجهة تأثيرات الشائعات المرتبطة بالإرهاب الالكتروني ، ووضع تصور لضبط استخدام المواقع الالكترونية، وجاء البعض الآخر بهدف توعية المجتمع بخطورة استخدام الجهات والتنظيمات الإرهابية وتقديم آليات تربوية مقترحة لمواجهة الإرهاب الإلكتروني لدي الطلاب . وقد استفادت

الدراسة الحالية من الدراسات السابقة في تناول المحاور الثلاثة للدراسة، وتحديد منهج البحث الملائم لهذه الدراسة.

مصطلحات الدراسة:

الإرهاب الالكتروني

ينطلق تعريف الإرهاب الإلكتروني من تعريف الإرهاب فهو يعرف على أنه نوع من الإرهاب الذي يعتمد على استخدام الإمكانيات العلمية والتكنولوجية، واستغلال الإنترنت ووسائل الاتصال؛ من أجل تهديد وترويع الآخرين، أو إلحاق الضرر بهم (الألفي، 2013، 5).

ويعرف الارهاب الالكتروني اجرائياً بأنه : الاستخدام السلبي للتقنية الحديثة للتهديد، أو لتنفيذ وتحقيق مكاسب ماديّة، أو معنويّة والتأثير على الآخرين باستخدام الإنترنت، والحاسبات، والقدرة على صناعة برامج التخريب والتدمير واستخدامها لإلحاق الضرر بأجهزة الحاسب والمواقع الإلكترونية والشبكات المستهدفة أو السيطرة عليها.

منهج الدراسة:

استخدمت الدراسة الحالية المنهج الوصفي التحليلي لدراسة ووصف دور التربية في مواجهة الإرهاب الإلكتروني، كما استخدمت المنهج التاريخي للوقوف على تطور مفهوم الإرهاب الإلكتروني وانتشار مخاطره.

إجراءات الدراسة:

تسير إجراءات الدراسة وفقا للمحاور الآتية:

المحور الأول: يتناول الإطار المفاهيمي والنظري لمفهوم الإرهاب الإلكتروني وخصائصه وأسبابه وأشكاله.

المحور الثاني: يتناول الاتجاهات الحديثة لمواجهة الإرهاب الإلكتروني.

المحور الثالث: يتناول دور التربية في التصدي للإرهاب الإلكتروني.

المحور الأول: إطار نظري ومفاهيمي عن الإرهاب الإلكتروني

مفهوم الإرهاب الإلكتروني

يعرف الإرهاب بصفة عامة بأنه: كل استخدام للقوة أو العنف أو التهديد أو الترويع يلجأ إليه الجاني تنفيذا لمشروع اجرامي فردي أو جماعي بهدف الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر إذا كان من شأن ذلك إيذاء الأشخاص أو إلقاء الرعب بينهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر أو إلحاق الضرر بالبيئة أو بالاتصالات أو بالمواصلات أو بالأموال أو المباني أو بالأملاك العامة أو احتلالها أو الاستيلاء عليها أو منع أو عرقلة ممارسة السلطات العامة أو دور العبادة أو معاهد العلم أو تعطيل تطبيق الدستور أو القوانين أو اللوائح (الألفي، 2013، 10).

ويعد الإرهاب الإلكتروني نوع جديد من أنواع القوة التكنولوجية الجديدة، حيث لم تعد القوة قاصرة على القوة التقليدية سواء العسكرية أم الاقتصادية والتي كانت محتكرة من قبل الدول الكبرى، فقد أدى ظهور القوة الافتراضية إلى إنهاء احتكار القوى التقليدية، وأصبح كل من لديه معرفة تكنولوجية ولديه قدرة على استخدامها يمتلك القوة والقدرة على التأثير في النظام العالمي (Wortham, 2012,26) (الألفي، 2016، 11).

كما يعرفه بريديلي كولن بأنه "التقاء ما بين الفضاء السبراني والإرهاب" ويعرفه مارك بولت وكيل مكتب التحقيقات الفيدرالي بأنه "هجوم متعمد ذو دوافع سياسية ضد المعلومات وأنظمة الكمبيوتر وبرامج الكمبيوتر وبيانات الأهداف الحيوية من جانب المجموعات المعادية للوطنية أو وكلائهم السريين.(Bradley, 2013, 52)

ويعرفه دينيج دورثي بأنه شن هجمات ضد أجهزة الكمبيوتر والشبكات والمعلومات المخزنة فيها بهدف ترهيب حكومة أو شعب ما بناء على أهداف سياسية واجتماعية غير مشروعة ولكن ينبغي أن يقترن ذلك بترويع وإكراه الحكومات والأشخاص والممتلكات والتسبب في إحداث الضرر أو الخوف وإحداث ضحايا بإيذاء بدني أو أضرار اقتصادية جسيمة أو هجوم على البنية الأساسية وإعاقة عمل الخدمات الأساسية. (عنترة، 2016، 172)

كما يمكن تعريفه بأنه استخدام أدوات وشبكات الحاسوب في تدمير أو تعطيل البنى التحتية الوطنية المهمة مثل الطاقة والنقل والعمليات الحكومية، أو بهدف ترهيب حكومة ما أو مدنيين. (Bradley, 2013, 52).

ويمكن تعريفه بأنه إرهاب السيبر (Cyber Terrorism)أو الهجمات التي تستهدف نظم الكمبيوتر والمعلومات لأغراض دينية أو سياسية أو فكرية أو عرقية بهدف اتلاف نظم

المعلومات أو تعطيل المواقع وعمل الأنظمة أو القيام بجرائم اقتصادية مثل غسيل الأموال وسرقة أموال المودعين في البنوك. (الألفي، 2013، 10)

فالإرهاب الإلكتروني نتج من التزاوج بين ظاهرة الإرهاب والثورة التكنولوجية والمعلوماتية والاتصالية الحديثة، وشاع استخدمه عقب الطفرة الكبيرة التي حققها استخدام تكنولوجيا المعلومات وتطبيقات الحاسبات الآلية والانترنت في إدارة معظم الأنشطة الحياتية، حيث أصبح الفضاء الإلكتروني يشكل بيئة استراتيجية جديدة لنمو وبروز أشكال جديدة من الصراع ولظهور فاعلين جدد على الساحة الدولية. (الدهشان، 2018، 93)

كما يعرف الإرهاب الإلكتروني بأنه: ذلك العدوان أو التخويف أو التهديد المادي أو المعنوي الصادر من بعض الدول، أو الجماعات أو الأفراد على الإنسان، في دينه أو نفسه، أو عرضه، أو عقله، أو ماله بغير حق، باستخدام مصادر المعلومات أو الوسائل الإلكترونية (Arquilla and Ronfeldtm 2011, 281).

ومما سبق يمكن تعريف الإرهاب الإلكتروني بأنه: العدوان أو التخويف أو التهديد ماديا أو معنويا باستخدام الوسائل الإلكترونية الصادر من الدول أو الجماعات أو الأفراد على الإنسان في دينه، أو نفسه، أو عرضه، أو عقله أو ماله، بكل أشكال العدوان وصور الفساد.

سمات وخصائص الإرهاب الإلكتروني:

هناك العديد من السمات التى يتسم بها الإرهاب الإلكتروني والتي تزيد من خطورته، وتتمثل أبرز هذه السمات فيما يلي(العباسي، 2016، 82)، (Bologna, 2013, 3):

1- صعوبة التنبؤ بآثاره المدمرة

ففى الهجمات التقليدية يكون الموقع المستهدف محدد والأضرار من الممكن توقعها كما أنه يمكن اصلاح تلك الأضرار بشكل سريع لأنه يسهل اكتشاف مصادر الخلل على عكس الهجمات الإلكترونية التي قد تترتب عليها مخاطر غير محدودة، ونتائج غير متوقعة، مع صعوبة تحديد مصدر هذه الهجمات، حيث يصعب التنبؤ بمقدار الخطر الناتج عن الهجمات الإلكترونية.

2- القدرة على التخفي وتجهيل مصادر المعلومات :

تتسم جرائم الإرهاب الإلكتروني بأنها صعبة الإثبات، حيث لا توجد أدلة مادية واضحة كما هو الحال في الهجمات التقليدية، ويرجع صعوبة اثباتها الى العديد من الأسباب: منها أن من يقوم بارتكابها شخص ذو درجة كفاءة عالية، وارتفاع درجة الخداع والتضليل، واختلاف الزمان والمكان والقانون المطبق في الدولة التي ارتكبت فيها.

3- سهولة استخدامه وتنوع أساليبه

تشكل الحاسبات وقواعد البيانات عمل العديد من المرافق المهمة مثل: "المستشفيات- المطارات- البنوك... وغيرها"، وبالتالي ففي حالة حدوث خلل فى الحاسبات الآلية قد يؤدى ذلك الى العديد من الكوارث، ومن ثم أصبحت الحاسبات الآلية مستهدفة بشكل كبير، كما أصبحت هدف حيوي للجماعات الإرهابية، فلم تعد تلك الجماعات بحاجة إلى اطلاق الصواريخ والتفجيرات لتدمير مدينة ما، وإنما يكفى تعطيل شبكة المواصلات الخاصة بتلك المدينة أو تعطيل الحاسبات الآلية الخاصة بالبورصة في تلك المدينة.

4- يمكن تنفيذه في بيئة آمنة:

تتميز هجمات الإرهاب الإلكتروني برخص التكلفة، ولا تحتاج إلا إلى شخص ذو كفاءة وخبرة فنية. والهجوم الإلكتروني نشاط عابر للحدود ومن ثم فهو نشاط عالمي، ويعتمد على الخداع والتضليل. وتتم الهجمات الإلكترونية في بيئة آمنة لا تحتاج إلى القوة والعنف واستعمال الأسلحة، ولذلك يطلق عليه الجرائم الناعمة، وكل ما تحتاجه هو جهاز حاسب آلي وشبكة انترنت.

5- الصبغة الدينية للإرهاب الإلكتروني

يتخذ الإرهاب الإلكتروني من الدين غطاء له، ومبرراً لتحقيق أهدافه غير المشروعة، ووسيلة لتضليل الشباب وغوايتهم للالتحاق بالجماعات الإرهابية والتكفيرية، والجماعات المتطرفة ذات الفكر المتشدد، فنجد أن اسم الموقع الإلكتروني اسم ديني. ونرى أن معظم المواد المنشورة عليه تتضمن بين ثناياها نصوصاً دينية قد تم حشرها قسراً، وتفسيرها تفسيراً مضللاً، لكي تناسب واقع الحال لهذه الجماعات، وتعبر عن أهدافها وأفكارها.

6- الإرهاب الإلكتروني أداة من أدوات إرهاب الدولة

حيث تقوده الدولة من خلال مجموعة أعمال أو سياسات حكومية والتي تستهدف نشر الرعب بين المواطنين، وفرض قيود على استخدام الفضاء الإلكتروني واخضاع الأفراد لرغبات الحكومة، وتستخدمه الدولة ضد الدول الأخرى لتحقيق أهداف يصعب عليها تحقيقها بالطرق السلمية أو تستخدمه للقيام بأعمال تخريبية ضد مؤسسات الدول الأخرى ومرافقها، كما تستخدمه في انتهاك الحرية والخصوصية في مواجهتها للمعارضين للنظام السياسي ويظهر في شكل حجب المواقع الإلكترونية واعتقال المدونين.

أسباب الإرهاب الإلكتروني ودوافع انتشاره

تتعدد أسباب الإرهاب الإلكتروني وتتنوع دوافع انتشاره، ويمكن بيان أهمها فيما يلي (لعلالمة، 2016، 201: 202، جريدة الشرق الأوسط، 2009):

1- أسباب دينية ومذهبية: وتمثل أبرز الأسباب الكامنة وراء ظهور هذا النوع من الإرهاب، إذ يعد الفهم الخاطئ بأصول العقيدة وقواعدها والجهل بمقاصد الشريعة عاملاً مساعداً على تطرف الشباب، فحفظ النصوص دون فقه وفهم، يعد سبباً مباشراً لبروز ظاهرة الغلو وانتشاره؛ فالجهل بأصول الدين الصحيحة من أهم أسباب الإرهاب، فترتكب الجرائم إما دفاعاً عن عقيدة دينية أو مذهب معين، أو لنشر فكر ما. ولعل ما نراه في هذه الأيام من تجسس على الهواتف الذكية، والمواقع الإلكترونية عموماً، ومواقع التواصل الاجتماعي خصوصاً من قبل العديد من الجماعات ذات التوجه المتشدد ليبين بجلاء جدية هذا الأمر وخطورته.
2- أسباب سياسية وتقنية: حيث تعد السياسة من أكبر وأقوى محفزات الإرهاب الإلكتروني المنتشر في هذا العصر، والمتمثل في التجسس وسرقة البيانات واختراق المواقع، وغيرها من الجرائم التي ترتكب باسم السياسة، والتي يكون الظلم السياسي والاستغلال الأجنبي والتبعية السياسية المفروضة على الأمم والشعوب وراءها غالبًا.
3- أسباب اقتصادية ومالية: فالذين يعمدون إلى اختراق المواقع الإلكترونية ذات العلامات التجارية المعروفة هدفهم ابتزاز أصحاب هذه المواقع والحصول على المال لا غير، والذين يسرقون باقات الائتمان هدفهم السرقة والاغتناء فحسب، وكذا الذين يتسللون للمؤسسات المالية من بورصات وبنوك وغيرها من المؤسسات التي تعتمد على الإنترنت في تجارتها مطمحهم الرئيس هو المال، أو تقويض اقتصاد الدول.
4- أسباب اجتماعية ونفسية: وهي كثيرة ومتنوعة، منها الفقر، مع ما يلازمه من البطالة، والتفكك الأسري، ووجود خلل في التربية والفراغ القاتل، وهي مشاكل اجتماعية تولد نتائج نفسية سلبية على الأفراد، يحركها الشعور العام بالاحتقار المهين الذي تعيشه أغلب شعوب

الدول النامية، الشيء الذي يولد الحقد ويسهل عملية ظهور وانتشار هذه الآفة الخطيرة، ويرسخ لدى القرصان مشروعية ما يقوم به من إرهاب وتخريب ونهب وسرقة رغم فظاعته.

وبالإضافة إلى ما سبق، هناك العديد من العوامل الأخرى التي قد تدفع الشباب للانضمام للجماعات المتطرفة أو المنظمات الإرهابية،المنتشره من خلال الأنترنت ومن أم تلك العوامل ما يأتي:

- الاضطهاد والظلم : إذ أنه حينما يشعر الفرد أنه مضطهد، وأن حقوقه مسلوبة في المجتمع، فإن ذلك يساعد الفرد على الانضمام لأي جهة أو فرد في إزالة ما وقع عليه من تعسف ومساعدته في الحصول على حقوقه، وهنا تكون الفرصة مواتية لأفراد التنظيمات المتطرفة لاحتواء مثل هؤلاء الأفراد، واستغلال هذه الدوافع والاستمرار في تضخيمها (الثقفي ، 2005، 4).
- نقص المستوى التعليمي: وهذا العامل من أهم العوامل التي تساعد على سرعة الانتماء للجماعات الإرهابية، حيث إن غالبية المتورطين في قضابات الإرهاب والتطرف كانوا قديما من الأميين، وهي نتيجة طبيعية ومتوقعة؛ إذ لا يتوقع من فرد متعلم ومستمر في الدراسة أن ينساق بسرعة للجماعات المتطرفة، بل إن هؤلاء أكثر عرضة للانضمام للجماعات المتطرفة، أما الإرهاب الحديث فهو يقوم على الفكر، والثقافة، والتخصصات النادرة، ومهارات الانترنت، أو ما يعرف بالإرهاب الإلكتروني (شومان، 2012).
- الانفتاح الإعلامي : تقوم وسائل الإعلام بدور كبير في جذب الشباب للانتماء للتنظيمات الإرهابية والمتطرفة بشكل مباشر وغير مباشر، إذ تستفيد التنظيمات المتطرفة من وسائل الإعلام المتعددة، المفتوحة جماهيرياً والمغلقة في بث أفكار التنظيم والترويج له؛ لتجنيد أكبر عدد ممكن من الشباب، خاصة من يتوافر لديهم دوافع تساعد على الانتماء للتنظيمات المتطرفة والإرهابية. فقد استطاع الإرهابيون استخدام شبكة الانترنت، وكانت لهم مواقع دعائية على شبكات التواصل الاجتماعي تنطق باسمهم وتدعو لأفكارهم، وتجند الأعضاء والأنصار الجدد (اليوسف، 2010، 4) .
- تنامي الفساد في المجتمع: يعد استفحال الفساد في المجتمع عامل هدم في بناء ووظائف المجتمعات، بل وبداية زوال ذلك المجتمع، وتتعدد صور وأشكال الفساد، فمنها: الفساد الإداري، والفساد السياسي، والعديد من الأنواع الأخرى، ويؤدي انتشار الفساد في مجتمع ما إلى تعطيل الحقوق، وسوء الأداء الخدمي، وتضخيم البيروقراطية، وانتشار الرشوة والمحسوبية، واستغلال الوظيفة، ومن ثم يتولد السخط لدى الرافضين لهذا الفساد مما

يدفعهم للالتحاق بالمنظمات الإرهابية ؛ رغبة في الحصول عل حقوقهم المسلوبة (جريدة الشرق الأوسط، 2005، 3).

أشكال الإرهاب الإلكتروني:

للإرهاب الإلكتروني عدداً من الأشكال، يمكن تحديدها في ما يلي (العباسي، 2016)، (الألفي، 2013، 7):

1- اختراق المواقع الإلكترونية

وغالباً ما يتم اختراق المواقع الإلكترونية لتغيير محتواها، أو سرقة معلومات سرية أو تعطيل الموقع عن العمل والسيطرة عليه بشكل كامل، وبعد نجاح اختراق الموقع يضع المهاجمون رسائل فى الموقع تعلن اختراقه وكأنه بمثابة رفع راية النصر .

2- الفيروسات

تنتشر فيروسات الحاسب الآلي بسرعة كبيرة عن طريق شبكة الانترنت، ويرجع ذلك إلى الكم الهائل من الملفات والبيانات التي يتم تبادلها بين مستخدمي الشبكة العنكبوتية، وهذه الفيروسات هي عبارة عن برامج تستنسخ نفسها فى الجهاز وعندما تنشط هذه الفيروسات تحدث تغييرات فى البرامج أو فى البيئة التى تعمل فيها، ولها أضرار مختلفة تتمثل فى فقد الملفات المخزنة وقد تصل تلك الأضرار الى تعطيل نظام التشغيل فى الجهاز.

3- الحرب الاعلامية

يؤثر الفضاء الإلكتروني بدرجة كبيرة على الرأى العام العالمى لأنه يخاطب ملايين المستخدمين للشبكة العنكبوتية من شتى أنحاء العالم وبوسائل مختلفة تتمثل في "الصوت- الصورة الثابتة والمتحركة- النص"، كما تستطيع أى جماعة أو منظمة إنشاء مواقع إلكترونية تروج أفكارها وتنشرها فى مختلف أنحاء العالم.

4- التجسس الإلكتروني

حيث تلجأ العديد من الحكومات إلى استخدام تقنيات متطورة من خلال الشبكة العنكبوتية للتجسس على الدول أو المنظمات ومراقبة المعلومات التى يتم تداولها حول العالم .

ومن أهم ما يندرج تحت مسمى جرائم التجسس الالكتروني ما يلي:

1- **جرائم التجسس الاقتصادية والتجارية:** هي الجرائم التي يكون الهدف منها الحصول على معلومات اقتصادية وتجارية.
2- **جرائم التجسس العسكرية والأمنية والسياسية:** وهي التي يكون الهدف منها الحصول على معلومات عسكرية أو أمنية أو سياسية.
3- **جرائم التجسس الثقافية والتعليمية:** وهي جرائم التجسس التي يكون الهدف منها الحصول على معلومات ثقافية وتعليمية ومن أمثلتها التجسس على الأبحاث والمخترعات والدراسات العلمية.
4- **الجرائم المالية والاقتصادية الالكترونية:** وتتمثل هذه الجرائم فيما يلي:

أ- الاحتيال والاستيلاء على المعلومات البنكية لعملاء البنوك عبر الانترنت واستغلالها في الشراء.

ب- إنشاء مواقع الكترونية وهمية بهدف الاستيلاء على أموال الشركات والكيانات الصناعية.

5- **غسيل الأموال عبر الانترنت:** وهي عبارة عن استغلال الأموال الغير مشروعة والمحرمة محلياً ودولياً وتمريرها واستبدالها بأموال مشروعة أو الاتجار بها في أنشطة غير مشروعة عبر الانترنت كالمخدرات والمواد الإباحية.

5- التهديد الإلكتروني

يوجد العديد من الأساليب التى تستخدم فى التهديد عبر الشبكة العنكبوتية، وتتنوع تلك الأساليب بين تهديدات باغتيال شخصيات سياسية، تهديدات بتفجيرات فى مراكز سياسية أو هيئات حكومية، أو التهديد باطلاق الفيروسات التى من شأنها تدمير أنظمة معلومات بالكامل.

6- القصف الإلكتروني

ويشير إلى الهجوم على شبكة المعلومات عن طريق توجيه مئات الآلاف من الرسائل الإلكترونية إلى مواقع هذه الشبكات، وبالتالى تسبب ضغط كبير على هذه المواقع، وتفقدها قدرتها على استقبال الرسائل من العملاء، ويؤدى ذلك الى التوقف عن العمل تماماً.

7- تدمير أنظمة المعلومات

ويتمثل ذلك في اختراق شبكة المعلومات الخاصة بالشركات العالمية أو بالأفراد بهدف تخريب نقطة الاتصال، وتخليق أنواع جديده من الفيروسات التى تسبب الدمار لأجهزة الكمبيوتر وللمعلومات .

مخاطر وتداعيات الإرهاب الإلكتروني

يمثل الإرهاب الإلكتروني خطراً كبيرا ، خاصة على الدول المتقدمة التي تعتمد حياة مجتمعاتها على شبكات الحاسب الآلي والمعلومات بصورة أساسية في إدارة بنيتها التحتية، وبالتالي فإن أى اختراق أو تدمير للبنى المعلوماتية قد يترتب عليه أضرار فائقة تتمثل على سبيل المثال في شل أنظمة القيادة والسيطرة والاتصالات، وقطع شبكة الاتصال بين الوحدات والقيادات المركزية، وتعطيل أنظمة الدفاع الجوي، والتحكم في خطوط الملاحة ، واختراق النظام المصرفي وإلحاق الضرر بأعمال البنوك وأسواق المال العالمية، كما يتم استخدام تقنية المعلومات لإصابة المرافق الحيوية مثل قطاعات الكهرباء والاتصالات والكمبيوتر والتي تعد ركائز الأمن القومي الجديد.(DE Franco, 2014, 40)

ولا يتوقف خطر الإرهاب الإلكتروني عند هذا الحد، إنما يترتب عليها عدد من التداعيات أهمها:

أ- تداعيات الإرهاب الإلكتروني على المستوى الأمني:

يتأثر الجانب الأمني بشكل مباشر من هذا النوع من الإرهاب نظراً لما يشكله من تهديد حقيقي على الفرد والمجتمع والدولة بكل مؤسساتها. ويظهر هذا جلياً في العديد من الأمور، مثل إلحاق الأضرار بالمواقع الحيوية والقطاعات الحساسة، والتسبب في الخراب والفوضى وإفزاع الآمنيين، والعمد إلى اختراق أنظمة الملاحة الجوية في أبراج المراقبة بالمطارات الكبيرة، والتسبب في اصطدام الطائرات وسقوطها، واختراق أنظمة إدارة معامل إنتاج الطاقة الكهربائية، والتسبب في انقطاع التيار الكهربائي عن الأحياء والمدن، وهو ما يستب في وفيات المرضى في

المستشفيات، إما في غرفة العمليات أو الذين هم تحت المراقبة الطبية . ليس هذا فحسب، بل إلحاق الضرر بكل شيء مرتبط بالأنترنت، بما في ذلك الحاسبات الآلية التي تدير معامل الطاقة الذرية، وتلك التي تدير محطات الكهرباء المحلية، بالإضافة إلى الحاسبات التي تستخدم في إدارة السدود الضخمة والتحكم في بواباتها(المحلاب، 2008، 86).

كما تستعين الجماعات المسلحة بشبكات التواصل لتوظيفها في عدة مهام من أبرزها، التنسيق فيما بينها، واستخدامها كأداة عابرة لقيود المكان، وذلك من أجل التدريب على تكوين خلايا تنظيمية، واستقطاب مزيد من الكوادر وتدريبهم على استخدام الأسلحة، وتقديم الوصفات الجاهزة لصناعة القنابل والمفرقعات، والتنسيق للعمليات المسلحة وتوقيتها، وتجنيد أتباع جدد ونشر الأفكار والمعتقدات، وغالباً ما تقوم الجماعات الإرهابية بإنشاء صفحات أو مجموعات على "تلك الشبكات" لاجتذاب المتوافقين فكرياً معها، ثم يتم بعد ذلك توجيه أعضاء المجموعة مباشرة إلى المواقع أو المنتديات المرتبطة بالجماعة الإرهابية. ويُمكن بهذه الطريقة تجنيد الأعضاء من كافة أنحاء العالم من دون أن يمثل ذلك تهديداً لهم. ولقد نشرت صحيفة النيويورك تايمز تقريراً يؤكد أن 90% من الهجمات الإرهابية استخدم فيها متفجرات صناعة يدوية من تلك التي توجد وصفاتها بكثرة على شبكة الانترنت. ولقد لعب البريد الإلكتروني دوراً مهماً في التواصل بين الإرهابيين وتبادل المعلومات بينهم. حتى إن كثيراً من الحوادث الإرهابية التي حدثت في الآونة الأخيرة كان فيها البريد الإلكتروني وسيلة من وسائل تبادل المعلومات وتناقلها بين القائمين بالعمليات الإرهابية والمخططين لها(الدهشان، 2018، 105) ,Lee, 2015) .225)

ب- تداعيات الإرهاب الإلكتروني على المستوى الاقتصادي:

أما تداعياته على المستوى الاقتصادي فهي كثيرة، رغم عدم وجود إحصائيات رسمية حول هذا الأمر، نظراً لأنه غالباً ما يتكتم على هذا النوع من الجرائم، لكن هذا لا يمنع من وجود بعض المؤشرات الدالة على الخسائر الفادحة التي بتكبدها الاقتصاد جراء هذا النوع الممنهج من الإرهاب. فالخسائر الناجمة عنه على المستوى الاقتصادي أكبر من الجرائم المعتادة، فمثلاً تقدر الخسائر اليومية لتدمير شبكة معلوماتية بما يعادل الأضعاف المضاعفة لانهيار مبنى، أو قصف منشأة، أو تفجير جسر، أو اختطاف طائرة (Ekpe, 2013, 38).

فعلى سبيل المثال، عندما انقطع خط الإنترنت البحري الذي يربط أوربا بالشرق الأوسط في نهاية شهر يناير عام 2008م، وأعقبه انقطاع آخر للخط القريب من ساحل دبي وخليج

عمان، قدرت الخسائر الناتجة عن ذلك والتي لحقت بقطاع الاتصالات والتعاملات الإلكترونية بمئات الملايين من الدولارات، وما تزال الأسباب مجهولة من وراء ذلك الانقطاع المفاجئ (المحلاب، 2008، 86).

وحسب الموقع الإلكتروني لهيئة الإمارات للهوية، فإن خسائر الإمارات العربية المتحدة في عام 2012م بلغ 420 مليون دولار بسبب هذه الجرائم، بينما أشارت مصادر أجنبية إلى أن تكلفة هذه الجرائم في المملكة العربية السعودية بلغت 2.6 مليار دولار في العام 2013، بحسب الموقع الإلكتروني لوزارة الاتصالات وتقنية المعلومات السعودية(سليمان، 2015، 10). بينما بينت إحصائية أجرتها FBI الأمريكية حول الخسائر الناجمة عن جرائم الإنترنت بأن الخسائر الاقتصادية المتعلقة بالضرر الناجم عن البرمجيات الخبيثة فقط، بلغ 17.5 بليون دولار في العام 2004م، وانخفض إلى 13.3 بليون دولار في العام 2006م (Bradley, 2013, 6).

ج- تداعيات الإرهاب الإلكتروني على المستوى السياسي:

يسبب الإرهاب الإلكتروني إشكالات كبيرة في العلاقات بين الدول والمؤسسات، فهو يسهم في تفشي مبدأ عدم الثقة بين الدول، خاصة وأنه يتخذ أشكالاً متعددة، ويتلون بألوان كثيرة. ومن أبرز الأمثلة في هذا المجال، فضيحة التصنت على المكالمات الهاتفية، وهي القضية التي أدت إلى توتر العلاقات الدبلوماسية بين الولايات المتحدة الأمريكية وحليفتها ألمانيا بعدما ثبت تورط الأولى في التجسس على المستشارة الألمانية "أنجيلا ميركل" طيلة 8 سنوات (منذ عام 2002م إلى غاية 2010م). ولولا تسريب عميل وكالة الأمن القومي الأمريكية السابق إدوارد سنودن لوثائق تثبت تورط أمريكا في جرائم من هذا النوع، لبقيت الأمور كذلك إلى أجل غير مسمى. كما كان لهذه الفضيحة المدوية تداعيات كبيرة على العلاقات الدبلوماسية بين الولايات المتحدة وحلفائها من الدول الأوربية على وجه الخصوص، وأبرز أثر لذلك هو فقدان هذه الدول الثقة في أمريكا لأنها لم تستسغ إقدامها على هذا العمل مع العلم أنها حليفة لها (العلالمة، 2016، 203).

المحور الثاني : الاتجاهات الحديثة في مواجهة الإرهاب الإلكتروني

في ضوء ما سبق عرضه من مفهوم الإرهاب الإلكتروني وتنوع صوره وأشكاله وتداعياته الأمنية والاقتصادية والسياسية أصبح من الضروري البحث عن الاتجاهات والخطط والآليات الحديثة لمواجهته.

يتناول هذا المحور الاتجاهات الحديثة فى مواجهة الإرهاب الإلكتروني، والمتمثلة في المواجهة الأمنية، والمواجهة الإعلامية للحد من مخاطر الإرهاب الإلكتروني، والقضاء عليه، وكذلك تجارب واتجاهات بعض الدول، التي كانت لها تجارب رائدة في هذا المجال، وتتمثل هذه الاتجاهات في ما يلي:

الاتجاه الأول: التعاون الدولي للسيطرة على الارهاب الإلكتروني:

- الوصول إلى تحديد مفهوم دولي موحد للإرهاب بصفة عامة والإرهاب الإلكتروني بصفة خاصة.
- عقد الاتفاقات بين الدول بخصوص تنظيم كافة الإجراءات المتعلقة بالوقاية من هذه الجريمة وعلاجها وتبادل المعلومات والأدلة في شأنها، بما في ذلك تفعل اتفاقيات تسليم الجناة في جرائم الإرهاب الإلكتروني تعزيز التعاون الدولي من خلال مراقبة كل دولة للأعمال الإجرامية التخريبية الإلكترونية الواقعة في أراضيها ضد دول أو جهات أخرى خارج هذه الأراضي. (عنترة، 2018، 173)
- عقد شراكات بين الدول وبعضها البعض مع مراعاة إزالة الفجوات المتباينة وتقديم الدعم الفني والمادي وتعزيز التعاون الاستخباراتي لتبادل المعلومات الحساسة اللازمة لمواجهة التهديدات الإرهابية حيث يصبح التعاون الدولي حجر الزاوية في سلامة الانترنت والأمن المعلوماتي. (الدهشان، 2018، 107)
- وضع آليات على أساس اقليمي ودولي تضمن مكافحة الإرهاب الإلكتروني ، والمواقع المتطرفة بشكل لا يؤدي إلى انتهاك حقوق الإنسان والخصوصية، ويساعد في نفس الوقت على الحفاظ على الأمن القومي ، وسلامة المواطنين (مكتب الأمم المتحدة المعني بالجريمة، 2012، 23).
- مبادرة الأمم المتحدة التي قام بها مكتب الأمم المتحدة المعني بمكافحة الجريمة، وبدعم من حكومة ايرلندا الشمالية، والحكومة البريطانية في دعم وبناء إطار معرفي، وقانوني يتم استخدامه دولياً، ووضع أطر قانونية وتشريعية لملاحقة الجرائم الإلكترونية، والحد من الإرهاب الإلكتروني، والتصدي الفعال لاستخدام الانترنت في الأغراض الإرهابية، وذلك باتخاذ تدابير فاعلة في مجال العدالة الحياتية، للتصدي لهذا التحدي العابر للحدود الوطنية. (مكتب الأمم المتحدة المعني بالجريمة، 2012، 25).

الاتجاه الثاني: سن القوانين والتشريعات الخاصة التي تجرم الارهاب الإلكتروني:

- سن القوانين والتشريعات الخاصة التي تسد كافة الثغرات التي تكتنف جريمة الإرهاب المعلوماتي وسبل التحقيق فيها كالقوانين المتعلقة بحفظ الأدلة وإثباتها وتعقب القائمين بها دولياً وجنائياً.
- تقنين مفهوم الإرهاب الإلكتروني ، أي وضع تشريعات قانونية تنص على عقوبات محددة لمن يمارس الجريمة الإلكترونية (مكتب الأمم المتحدة المعني بالجريمة، 2012، 23).
- ومن الدول التي أخذت زمام المبادرة في سن تشريعات تتعقب جرائم الإرهاب الإلكتروني مصر فقد تم إصدار العديد من القوانين في هذا المجال من بينها (قانون التوقيع الإلكتروني رقم 15/2004، وقانون تنظيم الاتصالات رقم 2003/10 وقانون حماية حقوق الملكية الفكرية رقم 2002/82) وقانون مكافحة الإرهاب بتاريخ 16 أغسطس 2015 والذي سلط الضوء على الدور الغير مشروع الذي يمكن استغلال شبكة الانترنت فيه بالقيام بجرائم تتعلق بأمن وسلامة المواطن أو ما أطلق عليه الإرهاب الرقمي، بالإضافة إلى التنسيق الدائم مع الانتربول الدولي في مجال تبادل المعلومات ورصد ومتابعة الأنشطة الإجرامية وخاصة فيما يتعلق بالنشاط الإرهابي التكنولوجي وذلك لتزايده المستمر في الفترة الأخيرة. (عنترة، 2018، 174)
- كما أصدرت دول مثل المملكة العربية السعودية جملة من الأنظمة والتعليمات واللوائح لاستخدام شبكة الانترنت والاشتراك فيها بهدف مواجهة الإرهاب الإلكتروني بالإضافة إلى تدريب أو تنظيم هذه الجهات دورات قانونية عن موضوع مكافحة جرائم الحاسب الآلي لتنمية معارف العاملين في مجال مكافحة الجرائم بأخر الإصدارات القانونية في هذا الشأن، وقد تم إنشاء محكمة خاصة للنظر في قضايا الإرهاب الإلكتروني تحت مسمى المحكمة الجزئية المتخصصة، واستحداث دائرة مختصة في هيئة التحقيق والادعاء العام تحت مسمى "دائرة قضايا أمن الدولة ومكافحة الإرهاب". (داغر، 2016، 163)

الاتجاه الثالث: تشكيل هيئة وطنية تعمل على وضع استراتيجية للأمن المعلوماتي ومكافحة الإرهاب الإلكتروني:

- تشكيل هيئة وطنية من الخبراء والمختصين تعمل على وضع وتطوير استراتيجية وطنية للأمن تركز على حماية البنية التحتية لشبكات المعلومات والنظم وتنسيق وتوحيد الجهود بين الجهات المختلفة في الدولة (الأمنية، التشريعية، والقضائية، والإعلامية)

- تفعيل دور المجلس الأعلى للأمن السيبراني، حيث أصدر رئيس الحكومة المصرية الأسبق "إبراهيم محلب" قراراً في ديسمبر 2014 بإنشاء مجلس أعلى لأمن البنية التحتية، يتبع رئاسة مجلس الوزراء تحت مسمى "المجلس الأعلى للأمن السيبراني"، ويتشكل المجلس من ممثلين من قطاعات الدولة المختلفة لمتابعة أي مخاطر أمنية متعلقة بشبكة الانترنت والمعلوماتية (حسونة،2015).
- وفي الولايات المتحدة تم تشكيل لجنة تحت رعاية الرئيس الأمريكي وذلك لحماية منشآت البنية التحتية الحساسة للولايات المتحدة الأمريكية وعلى رأسها البنية المعلوماتية وشبكات الحواسب الآلية التي تسطير عليها وزارة الدفاع الأمريكية، وكان أول تقرير لهذه اللجنة هو تحديد ما يمكن أن نطلق عليه عناصر البنية التحتية الحساسة وقد حددتها اللجنة في مصادر الطاقة الكهربية، الاتصالات بالإضافة إلى شبكات الكمبيوتر والمعلومات الرقمية والمنشآت الحيوية التي ممكن أن تكون الهدف الأول لأية هجمات إرهابية تستهدف أمن الولايات المتحدة الأمريكية، وفي اعقاب ذلك قامت كافة الوكالات الحكومية في الولايات المتحدة الأمريكية، بإنشاء هيئاتها ومراكزها الخاصة لإدارة الأزمات وللتعامل مع هجمات الإرهاب الإلكتروني المحتملة، فقامت وكالة الاستخبارات الأمريكي بإنشاء مركز حرب المعلوماتية ووظفت ألفا من خبراء أمن المعلومات، وقوة ضاربة على مدى 24 ساعة لمواجهة الإرهاب الإلكتروني وقامت القوات الجوية باتخاذ خطوات مماثلة ومثلها المباحث الفيدرالية.
- وعلى الصعيد الأوربي فقد قامت قوات الأمن في أوربا وخاصة التابعة لدول حلف الأطلسي باتخاذ إجراءات مماثلة ووضعت نصب أعينها أن الهجمات الإلكترونية قد تستهدف العناصر العسكرية والاقتصادية والسياسية أي مراكز القيادة والتحكم والبنوك والمؤسسات المالية ومؤسسات المنافع العامة كمؤسسات المياه والكهرباء وذلك لأن الهدف الأعلى لهذه الهجمات الإلكترونية يكون إخضاع إرادة الشعوب.

(الألفي، 2013، 24)

الاتجاه الرابع: تبني استراتيجية إعلامية ومجتمعية شاملة في مواجهة الإرهاب الإلكتروني:

- عقد حوارات مجتمعية ومؤتمرات تهدف إلى تسليط الضوء على حجم وخطورة ظاهرة الإرهاب الإلكتروني، والأبعاد السياسية والتقنية لها، وكذلك أحدث الوسائل، وأكثرها فاعلية في مواجهة الإرهاب الإلكتروني (حسونة،2015).

- تفعيل دور وسائل الإعلام في مواجهة الفكر الإجرامي للتنظيمات الإرهابية على شبكة الانترنت والتحذير من مختلف المواقع المحرضة على العنف والداعية للتعبئة والتجنيد للفكر المتطرف مع ضرورة التعاون مع الجهات الأمنية في الحصول على المعلومات اللازمة للمساعدة على مواجهة هذه النوع من الإرهاب أو ما يطلق عليه بالإعلام الأمني.
- بث مادة إعلامية حول ضحايا الإرهاب والنتائج المدمرة المترتبة على استخدام الانترنت في تشجيعه والترويج له والتعامل بحرص ويقظة مع ما تنشره التنظيمات الإرهابية على المواقع الإلكترونية المختلفة. (عنترة، 2018، 173)
- نشر قيم المواطنة والتسامح والفكر الوسطي وتعزيز مكانة المؤسسات الأمنية في نفوس المواطنين من خلال تعظيم إنجازاتها وتقدير جهودها في مجال مكافحة جرائم الإرهاب الإلكتروني. (داغر، 2016، 163)

وقد كان للمملكة العربية السعودية تجربة رائدة في مكافحة الإرهاب الإلكتروني الذي نشأ في بعض مواقع التواصل الاجتماعي (فيس بوك- تويتر- منصات الدردشة- المجموعات البريدية المغلقة)، حيث لجأت المملكة العربية السعودية إلى وضع استراتيجية موحدة ومحكمة، لها رافدين أحدهما أمني، والآخر فكري وأيدولوجي ، وذلك لمواجهة الجماعات المتطرفة التي تقوم بتجنيد الشباب من خلال اقناعهم بالفكر الإرهابي عبر مواقع التواصل الاجتماعي، وذلك من خلال مواقع ومنصات إلكترونية مضادة تشرح صحيح الدين الوسطي المعتدل، وتبين خطأ الأفكار المتطرفة، وبعدها عن سماحة الدين، بالإضافة للدور الأمني في هذا الإطار من تتبع المواقع التي تروج للإرهاب، ورصد ما يدور فيها، والتنسيق مع الدول الصديقة لضبط العناصر الإرهابية التي تروج للعنف، وتقوم بنشر ثقافة التطرف (السبيعي، 2013، 55).

ويوجد اتجاه آخر تبنته الحكومة البريطانية بعد استشعارها الخطر المحدق من تزايد عدد الشباب البريطاني الذي ينضم إلى تنظيم الدولة الإسلامية (داعش) يومياً، وذلك عبر تجنيدهم من خلال منصات التواصل الاجتماعي (فيس بوك- تويتر)، وقد أنفقت المملكة المتحدة نحو 173 مليون جنيه استرليني في تمويل لمشروع متكامل يعتمد على تنشيط منصات إعلامية وإلكترونية على مواقع التواصل الاجتماعي لردع الشباب المقيمين في بريطانيا عن الانضمام للإرهابيين في سوريا والعراق، والقتال في صفوفهم. كما أنشأ مسلمون بريطانيون موقع الجهاد، الذي يرصد الفاعليات الإرهابية في شبكة الانترنت، رافعاً شعار الجهاد ضد الإرهاب (الشهري، 2010، 43) ، (Weimann, 2006, 37).

ومن الاتجاهات الحديثة التي تتبناها الولايات المتحدة الأمريكية في مواجهة الإرهاب الإلكتروني سياسة الشبكة، أو استراتيجية الحرب والحرب المضادة، حيث ترتكز على ثلاثة محاور أساسية هي: أ- الرصد والمراقبة ، ب – سحب المحتوى الرقمي، ج- الدعاية المضادة. حيث تقوم المباحث الفيدرالية الأمريكية بمتابعة آلاف الحسابات المنتشرة عبر وسائل التواصل الاجتماعي، ومحاولة حصر أعداد الحسابات التي تروج للعنف، وتحض على الكراهية ، وتروج للإرهاب، ومتابعة أعداد الشباب المتابعين لها، ورصد تحركات الإرهابيين، ومصادر التمويل، والمواقع التي توفر محتوى يسهل لهم صناعة الأسلحة، أو الوصول إليها (Gertstenfeld, 2013, 33).

كما تم رصد عدة حسابات رقمية، تقوم الجماعات الإرهابية من خلالها ببث نشاطاتها، والترويج لأفكارها، في محاولة منها للتعويض عن افتقادها إلى المنابر الاعلامية الأخرى من صحافة وإذاعة وتليفزيون، مما اضطر الحكومة الفيدرالية إلى اجبار أدوات ومواقع تويتر وفيس بوك ويوتيوب على التخلي عن سياساتها الداعمة للخصوصية، والحفاظ على حرية الرأي واخضاع المتابعين والناشطين الرقميين لشروط مشاركة قاسية، وذلك استجابة للضغوط والنداءات التي أطلقتها أجهزة الاستخبارات، والتي ألزمت هذه المواقع على التعاون لمكافحة الإرهاب الإلكتروني، مما اضطرها في يناير 2012م إلى الإعلان عن سياسة الرقابة، عبر مراقبة التغريدات أو التعليقات التي يتعارض مضمونها مع القوانين، أو المؤيدة لخطاب العنف والإرهاب، وحظر هذه الحسابات، وتصنيفها تحت فئة "محتوى عنيف أو مشجع للكراهية والإرهاب"، مما يستدعي اغلاقها فوراً وملاحقة أصحابها جنائياً (Gertstenfeld, 2013, 35).

والواقع أنه رغم الوعي المتزايد بالتداعيات السياسية والاقتصادية والاجتماعية للجرائم السيبرانية، وأهمية وضرورة وجود قواعد مشتركة تسهل الوصول إلى تفاهم بين الدول، فإنه لا يزال هناك الكثير مما ينبغي القيام به لوضع معايير دولية محددة وقانون دولي قابل للتطبيق حول العالم السيبراني (Sirohi, 2015, 4).

وفي ضوء ما سبق، وما تم عرضه من سمات الإرهاب الإلكتروني ، وأشكاله، ومخاطره، وكذلك الاتجاهات الحديثة التي تبنتها العديد من الدول للسيطرة عليه، والحد من انتشاره، وكذلك الجهود الحثيثة التي يقوم بها المجتمع الدولي ممثلاً في الأمم المتحدة لاتخاذ الإجراءات العاجلة الفعالة لمكافحة الجريمة والإرهاب في العصر الرقمي، يمكن تلخيص أوجه الاستفادة من التجارب السابقة فيما يلي:

1- وضع مفهوم دولي وموحد للإرهاب بصفة عامة، والإرهاب الإلكتروني بصفة خاصة، وتأكيد أهمية دور وسائل الإعلام ووسائل التواصل الاجتماعي في بلورة اتجاهات لمواجهة الأفكار المتطرفة، والجرائم التي تتعلق بالإرهاب الإلكتروني(الدهشان، 2018، 107).

2- دعم التعاون الدولي من خلال مذكرات التفاهم المشتركة، واتفاقيات تبادل المعلومات الضرورية اللازمة لمواجهة الجرائم الإلكترونية، ورصد ومتابعة الأنشطة الإرهابية، خاصة في ما يتعلق بالنشاط الإرهابي الإلكتروني المتزايد (Seib and Janbek,2011,44).

3- تبني استراتيجية موحدة ومحكمة لمواجهة الإرهاب الإلكتروني والسيطرة على المحتوى الذي يحض على الكراهية والتطرف، ومواجهة الجماعات الإرهابية التي تقوم بتجنيد الشباب عبر شبكات التواصل الاجتماعي، وذلك عن طريق الاقناع الفكري، وإنشاء منصات إلكترونية مضادة للتصدي لهذا الفكر المتطرف، يقودها لجان إلكترونية وشباب قادر على مجاراة العناصر المتطرفة والدخول في مناظرات فكرية تفند مزاعمهم الضالة، وفهمهم القاصر للدين (الشرقاوي، 2014، 16).

4- تصميم منظومة فاعلة لتوعية المواطنين والشباب بالجرائم الإلكترونية ، والإرهاب الفكري الذي يمارس عبر شبكات الانترنت ووسائل التواصل الاجتماعي، والتي تحول دون وقوع الشباب في براثن الإرهاب الإلكتروني (عقيقي، 2014).

5- مراجعة الخطط والاتفاقيات المعتمدة بين الدول والهيئات الدولية وأجهزة الاستخبارات المعنية بمكافحة الجريمة السيبرانية والإرهاب الإلكتروني، وذلك عن طريق إجراء البحوث والدراسات، وعقد ورش عمل بهدف تحديث وتطوير البنى التشريعية والفكرية لمكافحة الجريمة الإلكترونية على المستويات الوطنية والإقليمية والدولية (صادق، 2005، 45).

6- ونتيجة لما أظهرته التجارب السابقة من صعوبة تعقب مرتكبي الحرائم الإلكترونية، وتميزها بالتقنية والتعقيد، فلابد من مواجهة هذا الخطر الفكري والاجتماعي على أكثر من مستوى، مما يتطلب تضافر الجهود بين الحكومات والشركات الكبرى العاملة في مجال المعلومات، والمسئولة عن مواقع التواصل الاجتماعي، مثل (جوجل- فيس بوك- يوتيوب- تويتر)، وذلك لمصادرة وحجب الحسابات الشخصية، والمواقع التي تحمل الفكر الإرهابي، وتروج لترويع المدنيين، وتهدد الأمن والسلم الدوليين (الدهشان، 2018، 110).

المحور الثالث: كيفية الاستفادة من الاتجاهات الحديثة فى تفعيل دور التربية في التصدي للإرهاب الإلكتروني فى مصر:

يمكن القول إن التربية بصفة عامة، والمدرسة بصفة خاصة يجب أن تتحمل الدور المناط بها في تقليل الإرادة الإجرامية لدى أفراد المجتمع حيث إن الأمن الفكري يرتبط ارتباطاً

وثيقاً وجوهرياً بالتربية والتعليم، إذ بقدر ما تنغرس القيم الأخلاقية النبيلة في نفوس أفراد المجتمع بقدر ما يسود ذلك المجتمع الأمن والاطمئنان والاستقرار، ويمثل النسق التربوي أحد الأنساق الاجتماعية المهمة التي تؤدي عملاً حيوياً ومهماً في المحافظة على بناء المجتمع واستقراره.

كما أن المجتمع يستطيع البقاء فقط إذا وجد بين أعضائه درجة من التجانس والتكامل، ويعد النظام التربوي في المجتمع أحد الركائز المهمة في دعم واستقرار مثل هذا التجانس، وذلك بغرس قيم ومعايير المجتمع الضرورية لإحداث عملية التكامل الاجتماعي داخل البناء الاجتماعي، فمن خلال العملية التربوية يتشرب الأفراد القيم الاجتماعية الإيجابية التي تغرس في نفوسهم قيم الانتماء الوطني ومشاعر الوحدة الوطنية التي تخلق التماثل الاجتماعي الضروري للمحافظة على بقاء الأمن والاستقرار في المجتمع، والتي تمثل صمام الأمان، ودرع الحماية من مخاطر الإرهاب الإلكتروني (السلطاني، 2015، 574).

ومن هذا المنطلق سيتم توضيح الدور الذي يمكن أن تقوم به المؤسسات التربوية في مكافحة سلوك العنف والإرهاب الإلكتروني والتطرف، ويلاحظ أن التغيرات الاجتماعية والثقافية والتي نتجت عن الثورة الرقمية والتقنية الهائلة وشيوع الجرائم الإلكترونية والإرهاب الفكري الذي يمارس عبر شبكات الانترنت والمواقع الإلكترونية أصبحت تفرض على النسق التربوي مسؤوليات مضاعفة تتجاوز حدود التعليم في نمطيته التقليدية وتفرض عليه الاضطلاع بدور أكثر أهمية في إكساب الشباب المعايير والقيم التي تحافظ على أمن واستقرار المجتمع، إذ أن النسق التربوي في الوقت الحاضر أصبح يعاني من الكثير من الضغوط بسبب قصوره عن أداء بعض الأدوار المناطة به مما يتطلب إعادة النظر فيه بعقلية انفتاحية لا ترفض القديم كله ولا تقبل الجديد كله دون دراسة وتمحيص (السلمي، 2014، 187).

ويمكن الاستفادة من الاتجاهات السابقة في تعزيز دور التربية لمواجهة الإرهاب الإلكتروني والتطرف انطلاقاً من الجوانب الآتية (دريب ، 2016، 332)، (الجعفري، 2013، 21):

1- في ظل تعقد الحياة والتقدم الهائل في مجال الاتصالات، وتعدد أشكال الجريمة، وظهور الإرهاب والجرائم الإلكترونية، مما يحتم على التربية التركيز على التنشئة الأمنية التي تعزز وتدعم ضرورة التعاون مع رجال الأمن من خلال تعميق الحوار والانفتاح الفعال بين المؤسسات التربوية والمؤسسات الأمنية من خلال مناقشة المشكلات التي تواجه أفراد المجتمع ووضع تصورات وخطط واستراتيجيات مشتركة بين المؤسسات التربوية والأمنية لمواجهتها والحد منها.

2- إضافة مناهج جديدة حول الوقاية من الجريمة الإلكترونية والانحراف، توضح للشباب سبل الوقاية من الوقوع فريسة لجرائم النصب والغواية الإلكترونية، وذلك من خلال الاستفادة من التجارب الدولية حول دور مؤسسات التربية في الوقاية من الجريمة الإلكترونية، ولعل من المستغرب انعدام أية برامج حول الوقاية من الجريمة المعلوماتية والإرهاب الإلكتروني حتى في برامج التعليم الجامعي رغم وجود كم هائل من برامج الوقاية المطبقة في الكثير من الدول.

3- ربط المدرسة بالمجتمع المحلي وتفعيل دورها في حماية أمن المجتمع المحلي بصفة عامة، وأمن المعلومات بصفة خاصة، وعدم قصر نشاطها داخل أروقة المدرسة فقط ويمكن تفعيل ذلك عن طريق إنشاء مجلس يسمى المجلس الأمني للوقاية من الإرهاب الإلكتروني ودعم الأمن الفكري ويتكون هذا المجلس من عدد من أفراد المجتمع المحلي بالإضافة إلى مجموعة من أعضاء الجهاز الفني والإداري في المدرسة مع مجموعة من رجال الأمن وتكون مهمة هذا المجلس توعية أفراد المجتمع المحلي بمخاطر الجرائم بمختلف أشكالها، التقليدية والإلكترونية، وعقد اللقاءات والندوات لمناقشة المشكلات المحلية ومحاولة التعاون الفاعل للقضاء عليها وطرح الحلول التي يمكن أن تساهم في تقليصها ورفع التوصيات لصانعي القرار لتفعليها.

دعم المواطنة الرقمية والتأكيد على اكساب التربية مهارات التعايش في العالم الرقمي للشباب، والوصول بهم إلى مرحلة من النضج الفكري والتفكير الناقد الذي يمكنهم من تحدي الإرهاب الإلكتروني، والوقاية من آثاره المدمرة .

ويمكن للتربية أن تواجه مخاطر الإرهاب الإلكتروني من خلال عناصرها المختلفة، كما يلي (السلمي، 2014، 188)، (السلطاني، 2015، 578)، (عبدالكافي، 2007، 88)، (داغر، 2016، 173):

أولا: دور المقررات الدراسية في مواجهة تحديات الإرهاب:

1- تعميق المقررات الدراسية بالدرجة الأولى لمفهوم الولاء للوطن والمواطنة لبناء مواطن صالح عن طريق تعريف المواطن ماهية حقوقه وواجباته، وبالتالي لا ينجرف بسهولة خلف الأفكار الهدامة التي تنتشر على مواقع التواصل الاجتماعي.

2- إدخال مادة "أخلاقيات استخدام الانترنت" ضمن المناهج الدراسية في التعليم الجامعي ما قبل الجامعي.

3- يجب أن تأكد المقررات الدراسية على احترام جميع الأعراف للمسلمين وغير المسلمين، وهذا من شأنه أن يحمي الطلاب من الأفكار المتشددة ، والمواقع الإلكترونية التي تروج لهذه الأفكار.

4- التأكيد دائماً على أن الوحدة الوطنية هي الطريق الصحيح لبناء وطن قوي وتعزيزها في نفوس الطلاب.

5- التأكيد على مفهوم التسامح والمحبة والسلام في المقررات الدراسية لترسيخ العقيدة الصحيحة في نفوس الطلاب كعرض القصص أو النماذج التاريخية والتركيز في المقررات على الشواهد التاريخية والدينية والاجتماعية التي تركز على وحدة أبناء الوطن، ويمكن تعزيز ذلك من خلال المعلومات الموجودة على شبكة الانترنت.

6- صياغة المناهج بعقلية انفتاحيه متناسبة مع تكنولوجيا العصر ومتغيراتها ومفاهيم العولمة التي سادت العالم بكافة اتجاهاته.

7- التركيز على المفاهيم الأمنية لضمان أمن الوطن بطريقة تناسب المستوى العمري للطلاب والتأكيد على أن مسؤولية حماية الوطن هي مسؤولية جميع أفراده.

8- تحديث المناهج الدراسية بصورة دائمة وبحسب مقتضيات العصر لتحصين الطلاب من بعض ظواهر الإرهاب الإلكتروني، والعنف، والتطرف الفكري.

9- وضع المناهج الدراسية ضمن خطة التنمية الشاملة للدولة واستراتيجياتها بحث تتوافق مع حاجات المجتمع ومتغيراته.

ثانياً: دور المعلم في مواجهة تحديات الإرهاب الإلكتروني :

1- يجب أن يتميز المعلم بالانفتاح العقلي والقدرة على التعامل مع التكنولوجيا الحديثة.

2- أن يكون المعلم مثالاً لعدم التعصب الديني والطائفي والتصدي لمثل هذه الأفكار المنتشرة على مواقع الانترنت.

3- يساعد المعلم على غرس المفاهيم والقيم الأخلاقية النابعة من الإسلام في نفوس طلابه كالتسامح والمحبة واحترام الأديان.

4- يساعد المعلم على تنمية الاتجاهات الفكرية والسلوكية الصحيحة والولاء للوطن لدى طلابه ، ويستعين في ذلك بأدوات ووسائل تكنولوجيا التعليم المتاحة.

5- يستخدم الأساليب التدريسية التي تساعد على مشاركة الطلاب وتعاونهم في الدرس دون تميز طائفي كاستخدام أسلوب التعليم التعاوني.

6- يستغل المعلم ما يعرض على الفضائيات ويوضح من خلاله مخاطر الإرهاب الإلكتروني أثناء إلقائه الدروس.

7- يحث المعلم طلابه على إجراء البحوث التي تشجع فكرة الحوار بين الأديان ونبذ الإرهاب ودور الطلاب بكافة طوائفهم في بناء وطنهم والولاء له.

ثالثاً: دور المرشد التربوي في مواجهة تحديات الإرهاب الإلكتروني:

1- أن يكتشف المرشد التربوي السلوكيات غير الاعتيادية وتوثيقها بدقة في البطاقة المدرسية لغرض متابعتها ومعالجتها والاستفادة منها مستقبلا.
2- يسعى المرشد التربوي من خلال عقد جلساته الحوارية مع الطلاب إلى نبذ الفكر الإرهابي وتوضيح أخطاره على المجتمع بكافة طوائفه، ويحذر الطلاب من الطرق التي تتبعها الجماعات المتشددة في نشر أفكارها عبر الانترنت.
3- نشر الوعي بين صفوف الطلاب بمخاطر التعامل مع المواقع السيئة على شبكة الانترنت؛ والمخاطر النفسية والاجتماعية الناجمة عن الاستخدامات غير الآمنة للإنترنت.
4- يحث المرشد التربوي طلبته على الانتماء لمؤسسات (اجتماعية، دينية، تربوية) تنمي الوعي ضد الإرهاب.
5- يحاول المرشد التربوي إرشاد طلابه إلى ضرورة التعاون مع الأسر المتضررة من الإرهاب.

رابعاً: دور الإدارة المدرسية في مواجهة تحديات الإرهاب الإلكتروني

1- تقوم الإدارة المدرسية بتوعية الطالب بسبل مواجهة الإرهاب الإلكتروني والوقاية منه، من خلال عقد الندوات الثقافية .
2- التعاون مع منظمات المجتمع المدني ولاسيما الجمعيات الأهلية، للقيام بدورها في وقاية الشباب من الوقوع في الممارسات الخاطئة والسلوكيات الضارة أخلاقياً عبر شبكة الانترنت.
3- تشكيل لجان طلابية تعمل على تنسيق العمل الطلابي بين مختلف الطوائف داخل المدرسة.
4- ابتعاد إدارة المدارس عن التميز في التعامل مع الطلاب واستخدام الطرق البديلة كإثارة روح المنافسة والتعاون مع الطلاب.

خامساً: دور الأنشطة الطلابية في مواجهة تحديات الإرهاب الإلكتروني

1- التأكيد على الأنشطة الطلابية التي تعزز مفهوم المحبة بين الطلاب بمختلف طوائفهم.
2- نشر الصور والملصقات التي تنبذ فكرة الإرهاب وتعزز التماسك والوعي الأمني بين أفراد المجتمع بكافة طوائفهم من خلال الأنشطة الطلابية التي تُقيم دور القيادات الوطنية والدينية التي تحارب الإرهاب الإلكتروني.
3- الابتعاد عن الأنشطة الطلابية التي تسبب الخلافات بين طوائف المجتمع.

4- إقامة المهرجانات الشعرية والأدبية والفنية التي تنبذ الفكر الإرهابي.

5- تكوين منتديات ومجموعات حوارية على الانترنت لكل المواد الدراسية ، وحث الطلاب على المشاركة بها.

6- تأكد الأنشطة الطلابية على نبذ التميز الطائفي ورفع العلم المصري وقراءة النشيد الوطني الذي يظهر وحدة أبناء المجتمع في مواجهة فكرة الإرهاب بكل أشكاله وعلى رأسها الإرهاب الجديد الرقمي أو الإلكتروني.

خاتمة:

أصبح المجتمع المصري والعالم العربي في حاجة عاجلة إلى مبادرات وأنساق وبرامج تربوية متميزة لمواجهة تحديات الإرهاب الإلكتروني ، ففي ظل الزخم الهائل الذي ولدته الثورة الرقمية والانفجار المعرفي، أصبحت التربية منوطة بأن توفر برامج لحماية أطفالنا وشبابنا وتعزيز سلامتهم ضد الاستخدامات السلبية للمواقع الإلكترونية وشبكات الانترنت، ويأتي في مقدمتها الإرهاب الإلكتروني والجرائم المعلوماتية، فأصبح من الضروري العمل على تكوين عقلية قادرة على تفعيل واستخدام مهارات التفكير الناقد؛ حتى يتمكن الشباب المتصفح من تفنيد محتوى المواقع الإلكترونية التي تقدم محتوى يحث على العنف، وخطاب الكراهية ورفض الآخر، التي تستخدم بغية تجنيد عناصر من الشباب والناشئة، ودفعهم لاعتناق أفكار متطرفة ضد السياق المجتمعي والانساني. فلابد من إعادة النظر في المنظومة التربوية، ولابد للتربية أن تحاول أن تنبي المواطن الرقمي وتؤسس لفكر الأمن الرقمي حتى يمكن السيطرة على الإرهاب الإلكتروني.

المراجع

آل علي، ميثاء محمد (2019). الإرهاب الإلكتروني: دراسة مقارنة. رسالة ماجستير، كلية الإمام مالك للشريعة والقانون، الإمارات العربية المتحدة.

الألفي، محمد محمد (2013). تشريعات مكافحة جرائم الإرهاب الإلكتروني : الأحكام القانونية والأنماط. ورقة عمل مقدمة للندوة العلمية حول " القوانين العربية والدولية في مكافحة الإرهاب" في الفترة من 15– 17 أبريل، 2013، الرياض.

الثقفي، محمد (2005). الدور الأمني للمسجد، ورقة عمل مقدمة لندوة المجتمع والأمن، كلية الملك فهد الأمنية بالرياض من 2/21 حتى 1425/2/24هـ.

جريدة الشرق الأوسط (2005). تداعيات الإرهاب في الوطن العربي.(لندن، عدد 8 أغسطس)،ص 3.

جريدة الشرق الأوسط (2009) . الإرهاب الإلكتروني. 19 يونيو 2009، العدد 9700.

الجعفري، عصام (2013) الإرهاب: الأسباب والعلاج، مؤتمر موقف الإسلام من الإرهاب، جامعة الإمام محمد بن سعود الإسلامية بالرياض، الفترة من 1–3 ربيع الأول.

حسونة ، هاجر . الإرهاب الإلكتروني: هل يتحول لمصدر التهديد الأول للعالم؟. متاح على: https://alkhaleejonline.net/%D8%B9%D9%84%D9%88%D9%85-%D9%88%D8%AA%D9%83%D9%86%D9%88%D9%84%D9%88%D8%AC%D9%8A%D8%A7/%

خليل، سحر عيسى محمد (2019). آليات تربوية مقترحة لمواجهة الإرهاب الإلكتروني لدى طلاب المرحلة الجامعية من وجهة نظر أعضاء هيئة التدريس بجامعة أسوان. المجلة التربوية، كلية التربية، جامعة سوهاج، ع58، 79– 127.

دريب، محمد جبر (2016). دور المدرسة في مواجهة تحديات الإرهاب من وجهة نظر الهيئات التدريسية. كلية التربية للبنات/جامعة الكوفة، العدد.

الدهشان، جمال علي (2018). الإرهاب في العصر الرقمي (الإرهاب الإلكتروني): صوره، مخاطره، آليات مواجهته، المجلة الدولية للبحوث في العلوم التربوية، 3(1)، 83– 121.

الدهشان، جمال علي (2017). جمال الدهشان يكتب: الإرهاب الإلكتروني أخطر أشكال الإرهاب فى عصر المعلوماتية. متاح في http://www.shbabalnil.com/%d8%a7%d9%84%d8%af%d9%83-%d8%aa%d9%88%d8%b1-%d8%ac%d9%85%d8%a7%d9%84

الداغر، مجدي محمد عبدالجواد (2016)، دور الإعلام الجديد في تشكيل معارف واتجاهات الشباب الجامعي نحو ظاهرة الإرهاب على شبكة الانترنت: دراسة ميدانية، مجلة حوليات الآداب والعلوم الاجتماعية، العدد (36)، الرسالة 453، 9-289.

السبيعي، سعد بن عبيد (2013). الاعلام الجديد ودورة في تعزيز الامن في المملكة العربية السعودية : دراسة تطبيقية على بعض النخب السعودية في الرياض . رسالة دكتوراه – جامعة نايف العربية للعلوم الامنية ، الرياض .

السبيعي، مذكر بن سحمي مثيب الملحي(2020). نحو رؤية استراتيجية لمكافحة الإرهاب السيبراني : دراسة ميدانية على مراكز المعلومات والتقنية في الجامعات السعودية بمدينة الرياض. رسالة ماجستير. – جامعة نايف العربية للعلوم الأمنية–كلية العلوم الاستراتيجية.

السلطاني ، نسرين حمزة (2015). دور التربية والتعليم في تحصين عقول الناشئة من التطرف والإرهاب. مجلة كلية التربية الأساسية للعلوم التربوية والإنسانية/جامعة بابل، العدد 23.

السلمي، فاطمة بنت عايض (2014). دور المدرسة الثانوية في مواجهة الإرهاب وتعزيز الانتماء الوطني لدى الطالبات بمحافظة حفر الباطن: الواقع والمأمول. مجلة البحوث الأمنية، العدد (57) ، 185- 241.

سليمان، فاديا (2015). الجرائم المعلوماتية وأثرها على العمليات المالية والمصرفية، الدراسات المالية والمصرفية ،(1)، 112- 156.

سليمان، محمد رضا أحمد (2016). دور وسائل الإعلام الجديد في مواجهة التأثيرات السلبية للشائعات المرتبطة بالإرهاب على المجتمع السعودي باستخدام

استراتيجية المنصات المتعددة: دراسة تحليلية وميدانية مع تصور مقترح. مجلة دراسات الطفولة، كلية الدراسات العليا للطفولة، جامعة عين شمس، 19(70)، 45– 57.

الشرقاوي، ايمان عبد الرحيم السيد (2014). جدلية العلاقة بين الاعلام الجديد والممارسات الإرهابية: "دراسة تطبيقية على شبكات التواصل الاجتماعي" . ورقة بحث مقدمة لمؤتمر "دور الاعلام العربي فيي التصدي لظاهرة الإرهاب " في الفترة من 16 – 18 ديسمبر 2014م ، جامعة نايف للعلوم الامنية، الرياض ، السعودية"ص ص 15–18

الشهري، فايز عبد الله (2010). الخطاب الفكري على شبكة الانترنت . رؤية تحليلية لخصائص وسمات التطرف الإلكتروني. ". الرياض – جامعة الملك سعود .

شومان، محمد (2012)، الإرهاب وتقنيات الاتصال، متاح على الرابط التالي: http://penclub.virtualave.net/494.htm

صادق، عبدالرحيم (2005). الإرهاب السياسي والقانون الجنائي. القاهرة : دار النهضة العربية.

العباسي، ريهام عبدالرحمن رشاد (2016). أثر الإرهاب الإلكتروني على تغير مفهوم القوة فى العلاقات الدولية، دراسة حالة: تنظيم "الدولة الاسلامية"، المركز الديمقراطي العربي للدراسات الإستراتيجية والاقتصادية والسياسية، متاح على https://democraticac.de/?p=34528https://democraticac.de/?p=34528https://democraticac.de/?p=34528https://democraticac.de/?p=34528https://democraticac.de/?p=34528

عبدالكافي، اسماعيل عبدالفتاح (2007). الإرهاب ومحاربته في العالم المعاصر، القاهرة: الهيئة العامة لقصور الثقافة.

عقيقي، فيفيان (2014). الإرهاب على مواقع التواصل الاجتماعي: كل ما يجب أن تعرفه. متاح على: http://www.annahar.com/

الغافري، حسين (2008). الإرهاب الإلكتروني. مقال على الرابط التالي: Hussian.alhafri@ita.gov.om

لعلالمة، رشيد(2016). نظرة شرعية في الإرهاب الإلكتروني: أسبابه وتداعياته ووجوب مواجهته. مجلة البحثية للعلوم الإنسانية والاجتماعية (5)، 198-207.

المحلاب، عبدالله بن عبدالعزيز بن فهد (2008). الإرهاب الإلكتروني في عصر المعلومات. بحث مقدم إلى المؤتمر الدولي الأول حول "حماية أمن المعلومات والخصوصية في قانون الانترنت" والمنعقد بالقاهرة في المدة من 2-4 يونيو 2008م.

الرومي، محمد أمين (2008). **غسل الأموال في التشريع المصري والعربي**، المحلة الكبرى: دار الكتب القانونية.

محمد، سماح زكريا (2016). دور المؤسسات التربوية في مواجهة الإرهاب الإلكتروني. مجلة كلية التربية، جامعة كفر الشيخ، (16)1، 281- 343.

مكتب الأمم المتحدة المعني بالجريمة (2012). استخدام الانترنت في أغراض ارهابية. فيينا: مطبوعات هيئة المم المتحدة.

اليوسف، عبدالله (2010). التقنية والجرائم المستحدثة. ورقة عمل مقدمة في ندوة "الظواهر الإجرامية المستحدثة وسبل مواجهتها"، تونس خلال الفترة 14-2010/3/16.

Arquilla, J. & Ronfeldt, D. (2011).Networks and Netwars: The Future of Terror, Crime, and Militancy. USA; Rand publication, P281.

Bologna S., Bernhard, H. Gritzalis, D. (2013). Critical Information Infrastructure Security. Berlin ; Springer, 2013.

Bradley, K. (2013) .Anatomy of Cyberterrorism: Is America vulnerable.A Research Paper Submitted to the Faculty in Partial Fulfillment of the Graduation Requirements, February.

DeFranco, J. (2014). What Every Engineer Should Know About Digital Cyber Security .Boka Raton : CRC press, 2014.

Ekpe, U. H. (2013). The Impact of Terrorism(Including Cyber Terrorism)and Threats of Terrorism on International Business (or Nation Sate .)Journal of the International Relations and Affairs Group, 3(1), P38.

Gertstenfeld, P. & others , (2013). " A Content Analysis of Extremist Internet Sites " Analysis of Social Issues & Public Policy .3(1),9-44.

Haseski, Halil Ibrahim (2020). Cyber Security Skills of Pre-Service Teachers as a Factor in Computer-Assisted Education. **International Journal of Research in Education and Science**, 6(3), 484-500.

Lee, N. (2015). Counterterrorism and Cybersecurity: Total Information Awareness. 2ndEd, Switzerland ; Springer Internatio-nal Publishing.

Lester, Teresa M (2018). An Investigation on Cyber Safety Awareness among Teachers and Parents. ProQuest LLC, Ed.D. Dissertation, Gardner-Webb University.

Lucas, Kweilin T. (2018). Cyber-Bullying among College Students: A Test of Social Learning Theory. Ph.D. Dissertation, Indiana University of Pennsylvania, ERIC Number: ED588025.

Seib, P. and Janbek, D. M. (2011) . **Global Terrorism and New Media: The Post-Al Qaeda Generation**, (New York: Routledge, 2011).

Sirohi , M. (2015). **Cyber Terrorism and Information Warfare**. Delhy . Alpha Editions.

Touloupis, Thanos; Athanasiades, Christina (2020). Information and Communication Technologies Teachers' Perspective Regarding Online Risk Behaviors in School Age. **International Online Journal of Primary Education**, 9(1), 1-17 .

Weimann, G. (2006). Terror on the Internet: The New Arena, the New Challenges (Washington, D.C., United States Institute)4(. of Peace Press, 2006), pp. 37-38

Wortham, J. (2012). A political coming of age for the tech industry, The New York Times, 17 January .