الأبعاد الاجتماعية للإرهاب الإلكتروني

دراسة ميدانية

د/ محمد محمود أحمد الرمادي

المستخلص:

أدى التطور التكنولوجي والمعلوماتي الذي يشهده العالم إلى ظهور شكل جديد من أشكال الإرهاب يُطلَق عليه (الإرهاب الإلكتروني)، والذي أصبح يشكل تهديداً كبيراً على الأمن القومي للدول بل امتد تأثيره إلى تهديد الأمن والسلم الدوليين، ومما لا شك فيه أن التحول الرقمي والتوسع في استخدم التكنولوجيا الرقمية في معظم القطاعات والمؤسسات بل واعتماد الدول على تلك التكنولوجيا في إدارة البنية التحتية لها عن طريق الكمبيوتر وارتباطها بشبكة المعلومات الدولية والذي كان له الكثير من الإيجابيات إلا أن الاعتماد على تلك التكنولوجيا في كثير من القطاعات أدى إلى جعلها هدفاً للهجمات الإرهابية وأصبحت عُرضة لمخاطر أمنية وهجمات إلكترونية وأصبحت البنية التحتية والمنشآت العسكرية والاقتصادية وحتى الفعاليات السياسية مُهَددة للتعرض لهجمات إرهابية عن طايق تلك التكنولوجيا مما أدى إلى تعرض كثير من الأبرياء إلى القتل بالإضافة إلى الخسائر المادية والتأثير بالسلب على الروح المعنوية للمواطنين داخل مجتمعاتهم. وقد استشعرت مصر خطورة تلك الظاهرة خاصةً مع التوسع في استخدامات تكنولوجيا المعلومات وربطها بشبكة الإنترنت وذلك في كافة المؤسسات الاقتصادية والعسكرية والبنية التحتية، فأقدمت مصر إلى التوسع في التعاون الدولي لمنع استخدام واستغلال الإرهاب للتطور التكنولوجي ووضع إطار لمكافحة تفشي ظاهرة الإرهاب والفكر المتطرف.تكمن أهمية البحث على التركيز على الأبعاد الاجتماعية والتي لها دوراً مهماً في الحد من ظاهرة الإرهاب الإلكتروني ومحاولة التعرف على مظاهر تلك الظاهرة وأشكالها وأهم طرق مواجهتها، كذلك التعرف على أشكال التعاون الدولي والإقليمي في مواجهة ظاهرة الإرهاب الإلكتروني.

الكلمات الافتتاحية: الإرهاب الإلكتروني؛ الجريمة الإلكترونية؛ الأبعاد الاجتماعية.

تمهيد :

يشهد العالم اليوم تطوراً كبيراً في العديد من المجالات، خاصةً في مجال تكنولوجيا المعلومات، وذلك بسبب المتغيرات السريعة والمتلاحقة المترتبة على التقدم العلمي والتقني، وهكذا فقد مست الثورة المعلوماتية جميع مناحي الحياة وأصبحت أشبه ما يكون بأسلوب حياة لا غنى عنه بين معظم الناس ، وذلك لارتباطها بجميع القطاعات الحيوية. وتُعد الثورة المعلوماتية سلاح ذو حدين، حيث لايقتصر تأثيرها على الجانب الإيجابي فقط المرتبط بالثورة العلمية والتكنولوجية، وإنما أدت إلى انعكاسات سلبية خطيرة أوجدت أشكال متعددة من السلوكيات التي أُطلِقَ عليها (سلوكيات غير شرعية) ، ومنها ظهور ما يُسَمى بـ (الإرهاب الإلكتروني).

والإرهاب الإلكتروني Cyber Terrorism هو نوع من الإرهاب الذي يعتمد على التطور التكنولوجي والثورة المعلوماتية ، باستغلال شبكة الإنترنت . وذلك بغرض الهدم والتخريب ونشر الضرر الذي يستهدف التأثير السلبي على اقتصاديات الدول، والتخويف والتهديد المادي والمعنوي وإلحاق الضرر بالآخرين والذي نتيج عنه ضحايا ومصابين، وأيضاً القيام بمهاجمة نظم المعلومات على خلفية دوافع سياسية أو عرقية أو دينية.

إشكالية الدراسة:

إن إشكالية الدراسة تتحدد في محاولتها الإجابة عن تساؤلات تطرحها الظاهرة موضوع البحث والدراسة، فليست إزالة الحدود الجغرافية بين البشر هي الإنجاز الذي يجب أن ندين به لهذه الوسيلة الاتصالية الإلكترونية فقط، بل إن الإنجاز الأعظم لها هو ذاك الذي حققته على المستوي الثقافي والاجتماعي وهذا التطور التكنولوجي الذي شهده العالم ساهم بشكل كبير في التنمية الاقتصادية والاجتماعية والثقافية، وحتى أصبح من ضرورات الحياة اليومية للأفراد للتواصل والبحث وتبادل الأفكار وكافة أشكال المعلومات كذلك التسوق عبر مواقع الإنترنت.

حيث تُعد التغيرات التي يشهدها العصر الحالي هي التغيرات الأكثر سرعة وتمتد لنطاق واسع على مر التاريخ، وأصبحت وفرة المعلومات وانفجار تكنولوجيا المعلومات هو المحرك الذي يشكل جميع جوانب الحياة الاجتماعية والسياسية والثقافية و الاقتصادية، ولكن ومع هذه الميزات المتعددة كان هناك الوجه الأخر لتلك الاتكنولوجيا المتطورة والتي أدت بدورها لظهور العديد من المشكلات العابرة للحدود والتي لا يمكن لأي دولة منفردة القضاء عليها، ومن تلك المشكلات ظاهرة جديدة أثرت بشكل كبير على اقتصاديات دول كثيرة كذلك أثرت على سياساتها الداخلية والخارجة، ألا وهي ظاهرة (الإرهاب الإلكتروني) التي جعلت دول كثيرة تتعاون في طرق مواجهته وأساليب الحد منه.

كما تؤكد الدلائل أن المنظمات الإرهابية تستخدم شبكة الإنترنت بشكل متزايد كمنصة اتصال لتسهيل عملية الاتصال بين أعضائها، كذلك نشر المواد الدعائية ونقل المعلومات والمخططات الإرهابية.

كذلك تهدف الجماعات الإرهابية إلى جذب العناصر الإرهابية وتجنيدها والتأثير في الجمهور، عن طريق أسلوب الاستمالة العاطفية الذي تستعمله الجماعات الإرهابية في منصات المواقع والصحافة الإلكترونية، والأخطار التي تواجه المجتمعات نتيجة تواجد أفكار هذه الجماعات الأيديولوجية وانتشارها في هذه المواقع والتي تتسبب بانتشار ظاهرة الإرهاب والعنف وتثير الخوف والرعب في المجتمع[1].

تساؤلات الدراسة:

تحاول الدراسة الإجابة علي التساؤل الرئيس التالي: هل التركيز على الأبعاد الاجتماعية يُعطي دوراً إيجابياً في مواجهة الإرهاب الإلكتروني؟ بالإضافة إلي محاولة الإجابة على التساؤلات الفرعية التالية:

- ما مفهوم الإرهاب الإلكتروني وأهم أسبابه؟
- ما أهم مظاهر وأشكال الإرهاب الإلكتروني؟
- ما أهم طرق مواجهة ظاهرة الإرهاب الإلكتروني على المستوى الدولي كذلك على مستوى الهيئات والمنظمات؟
- ما رؤية أفراد عينة الدراسة لدور الأبعاد الاجتماعية في مواجة الإرهاب الإلكتروني؟

أهمية الدراسة:

تنبع أهمية دراسة الإرهاب الإلكتروني في أنه أصبح يشكل خطورة كبيرة على الأمن والسِلم الدوليين، فهناك قلق متزايد بشأن إساءة استخدام تقنية ا لمعلومات والاتصالات على أيدي الإرهابيين واستخدام القنيات الحديثة والإنترنت ووسائل التواصل الاجتماعي لارتكاب أعمال إرهابية أو التحريض عليها أو تجنيد أعضاء جُدُد أو التمويل والتخطيط.

وتهتم الدراسة بتوعية الأفراد في المجتمعات بالتعريف بالطرق ومناهج عمل التنظيمات الإرهابية على شبكات الإنترنت وكيفية استقطاب عناصر جديدة خاصةً من فئة الشباب، كذلك تهتم الدراسة بإلقاء الضوء على نماذج التعاون الدولي والإقليمي والوطني في مواجهة ظاهرة الإرهاب الإلكتروني والاتفاقيات الدولية الخاصة بمواجهة تلك الظاهرة التي أصبحت لها عواقب خطيرة على الأمن القومي واجتذبت اهتمام الكاديميين والمسؤوليين الحكوميين والاستخباراتيين في معظم البلدان للتوصل لحلول لتلك التهديدات المحتملة وبالتالي جعل الإنترنت أكثر أماناً كأداة اتصال من أجل التنمية الاقتصادية والتجارية والاجتماعية.

الإجراءات المنهجية للدراسة:

اعتمدت الدراسة على الأسلوب الوصفي التحليلي، والأسلوب المقارن لمحاولة التوصل لإجابات عن تساؤلات الدراسة .وفي هذا الإطار تم تطبيق استبيان الكتروني على شبكة الإنترنت للتعرف علي رؤية عينة الدراسة لمتغيرات البحث الرئيسية ، كما تم الاعتماد على البيانات الجاهزة لرصد مدي الزيادة في معدلات الإرهاب الإلكتروني.

الإطار النظري للدراسة:

تنطلق هذه الدراسة من نظرية الصراع الثقافي والاجتماعي " لثورتين سيلين Thorsten sellin ، وترى هذه النظرية أن الصراع الثقافي والاجتماعي يلعب دوراً هاماً في إحداث التفكك الاجتماعي الذي يؤدي إلى السلوك الإجرامي وارتفاع معدلة ، والصراع الاجتماعي يعني صراعاً بين جماعتين أو أكثر تتفاوت قيمهما من أجل تحقيق مصالحهما الخاصة(٢).

ويعني الصراع الثقافي صداماً بين عناصر ثقافتين ، وأهم هذه العناصر القيم والعادات والتقاليد ، ويأخذ الصراع الثقافي صوراً عديدة منها :

- الصراع بين قيم الجماعات المهاجرة والأقليات وبين قيم المجتمع العام.
- الصراع بين قيم الطبقات الاجتماعية على مستوي المجتمع.
- الصراع بين قيم الأجيال المتعاقبة(٣) .

وترى الأدبيات الحديثة في النظرية الاجتماعية أن الاتصال عبر الإنترنت نقلنا إلى العيش في زمن ثقافي من نوع خاص، قام أنطوني جيدنز بتلخيص خصائصه الاجتماعية وسماته الثقافية ببراعة فائقة، وإيجاز دقيق، بما يأتي[٤]:

- إن التحولات والتغيرات الاجتماعية والثقافية التي يتصف بها المجتمع المعاصر هي تحولات ذات قوة نابذة وطاردة (Centrifugal) للأفراد، وذات خصائص ثقافية مشوشة.
- إن الأفراد في المجتمعات التي ينتشر فيها هذا النوع من الاتصالات، هم أفراد مقطوعو الأوصال، بسبب استغراقهم وذوبانهم في خبرات يومية مجزأة ومبعثرة.
- يشعر الأفراد في هذا النوع من المجتمعات بالعجز وضعف المقاومة وقلة الحيلة (Powerless) في مواجهة العولمة وطغيانها وجبروتها.
- تخلو حياة الأفراد اليومية في هذه المجتمعات من أي معنى، بسبب سيادة أنظمة اجتماعية جافة تفتقر إلى الحياة والديناميكية (Abstract Systems) وتعمل على تفريغ حياة الأفراد اليومية من مغزاها ودلالاتها الاجتماعية الحميمية.

مفهومات الدراسة:

مفهوم الأبعاد الاجتماعية – مفهوم الإرهاب الإلكتروني:

١. مفهوم الأبعاد الاجتماعية:

أحدثت الثورة التكنولوجية والاتصالية تغييرات جذرية في حياة الأفراد والمجتمعات، وفرضت علينا أبعاد جديدة للعلاقات بين الأشخاص وبين الدول بعضهم ببعض، وتلك الأبعاد هي أبعاد مختلفة في أنساقها وبنيتها وخصائصها عن الأبعاد التقليدية.

فليست إزالة الحدود الجغرافية بين البشر هي الإنجاز الذي يجب أن ندين به لهذه الوسيلة الاتصالية الإلكترونية فقط، بل إن الإنجاز الأعظم لها هو ذاك الذي حققته على المستوي الثقافي والاجتماعي، فقد أنهت الإنترنت الفروق الثقافية والاجتماعية بين البشر ووحدهم في ثقافة ذات خصائص جديدة تختلف اختلافاً جوهرياً عما قبلها من خصائص، وهناك من يقيم تلك التغيرات في أنها تغييرات عملت على تفتيت العلاقات الاجتماعية بين الأفراد، وحولت ما كانت تتمتع به من دفء وحميمية إلى برود وفتور، وغيرت أنماط تفاعلهم الاجتماعي، وفتحت أمامهم مسارب سلوكية أضرت بقيمهم وأخلاقهم، فضلاً عما أوجدته بينهم من مشكلات جديدة غير مألوفة من قبل، كتبلد حسهم الاجتماعي والوجداني واغترابهم النفسي، وعزلتهم الاجتماعية، فضلاً عن العوالم الافتراضية المتخيلة (Virtual Realities) التي أوجدتها لهم ليعيشوا فيها كعوالم بديلة عن عوالمهم الحقيقية، علاوة على مساهمتها على انتشار نوع جديد من الإدمان بين مستخدمي هذه الوسائط الاتصالية والتي تسمي " إدمان الإنترنت Internet Addiction"[٥].

وفي الواقع فإن التطور التكنولوجي الإلكتروني الهائل بما له من ايجابيات واضحة على الفرد والمجتمع، إلا أنه ومن خلال الاتصال بشبكة الإنترنت نقلنا تغيرات اجتماعية وثقافية ذات خصائص مشوشة ومضطربة، خاصةً تلك المجتمعات التي يسهل فيها الاتصال بشبكة الإنترنت، حيث تجعل حياة الأفراد داخل تلك المجتمعات حياة جافة مُفرغه من معانيها الاجتماعية.

وعلي الرغم من تنامي التأثيرات الاجتماعية للإرهاب الإلكتروني، إلا أنه لابد من أهمية التركيز على الأبعاد الاجتماعية في عملية مكافحة الإرهاب، الأمر الذي يتطلب مقاربات مختلفة

وضرورة تحسين الأوضاع الاجتماعية وتجديد الخطاب الديني وفقاً لمستجدات الحياة وبناءً على واقعها المعاصر[٦].

ووفقاً لما سبق يمكن تعريف الأبعاد الاجتماعية للإرهاب الإلكتروني إجرائياً حيث نقصد به في هذه الدراسة التأثيرات الاجتماعية للإرهاب الإلكتروني سواءً علي المستوي الفردي أوعلي المستوي المجتمعي، فعلي المستوي الفردي يؤثر الإرهاب الإلكتروني علي حياة الفرد الشخصية وعلاقاته الاجتماعية، وعلي المستوي المجتمعي يؤثر الإرهاب الإلكتروني علي القيم الأخلاقية والدينية والعلاقات الاجتماعية السائدة في المجتمع، كذلك ما له من بعد اقتصادي يتضمن خسائر اقتصادية فادحة تضر باقتصاديات الدول وما يسببه من ذعر وضرر وقتلى وضحايا ومصابين بين أفراد المجتمع، وما يتضمنه من بعد قانوني يتطلب ضرورة استحداث قوانين قادرة على مواجهة تلك الظاهرة المستحدثة والتي لا تستطيع القوانين التقليدية مواجهتها والقضاء عليها.

٢. مفهوم الإرهاب الإلكتروني:

كانت بداية استخدام مصطلح **الإرهاب الالكتروني Cyberterrorism** في فترة الثمانيات علي يد **باري كولين Barry Collin** والتي خلص فيها إلى صعوبة تعريف شامل للإرهاب التكنولوجي. ولكنه تبنى تعريفاً للإرهاب الالكتروني مقتضاه؛ بأنه "هجمة الكترونية غرضها تهديد الحكومات أو العدوان عليها، سعياً لتحقيق أهداف سياسية أو دينية أو أيديولوجية، وأن الهجمة يجب أن تكون ذات أثر مدمر وتخريبي مكافئ للأفعال المادية للإرهاب"[٧].

الإرهاب بشكل عام يمكن القول بعدم وجود اتفاق على تحديد مفهومه، لأنه يُعَد عملية شائكة ومتداخلة لصدورها عن أسس نفسية تابعة لذات فاعلها وتشكيلاتها النفسية والثقافية والبيئية، فهناك صعوبة في صياغة تعريف قانوني للإرهاب وتمييزه عن الأنواع الأخرى من الجرائم، إلا أنه على الرغم من ذلك فهناك إجماع على أن الإرهاب ليس مجرد جريمة عادية، ولكنه يُشَكِل نوعاً خاصاً من أشكال الجريمة يتميز بكونه نسخة أكثر خطورة من الجريمة العادية ونوع من الجرائم الخارقة التي تشتمل في خصائصها بعض خصائص الحرب.

وعليه فالإرهاب بشكل عام يعرف بأنه (إستراتيجية عنف منظم ومتصل من خلال جملة من أعمال القتل والاغتيالات وخطف الطائرات واحتجاز الرهائن وزرع المتفجرات وخلافهمن أفعال التهديد التي تهدف إلى خلق حالة رعب عام بهدف تحقيق أهداف سياسية.

أما الإرهاب الإلكتروني فيمكن تعريفه على أنه (العدوان أو التخويف أو التهديد مادياً أو معنوياً باستخدام الوسائل الإلكترونية الصادرة من الدول أو الجماعات أو الأفراد على الإنسان ودينه أو نفسه أو عرضه أو عقله بغير حق بشتى صور الإفساد في الأرض[٨].

أما بالنسبة للأمم المتحدة فقد عرفت الهجمات السيبرانية على العموم، استغلال الشبكات الحاسوبية عن عمد باعتبارها وسيلة لشن هجوم، وتهدف هذه الهجمات عادةً إلى تعطيل النظم التي تستهدفها، وتتضمن تلك الأهداف بنظم الحاسوب والخواديم وبنيتها التحتية الأساسية. وذلك عبر استخدام الاختراق الحاسوبي، أو التقنيات المتقدمة للتهديد المستمر، أو فيروسات الحاسوب، أو البرمجيات الضارة، أو الإغراق أو غيرها من وسائل الدخول غير المصرح به، وقد تحمل الهجمات السيبرانية سمات عمل إرهابي بما في ذلك الرغبة في زرع الخوف دعماً لأهداف سياسية أو اجتماعية[٩]. ولكن مثلما لا يوجد إجماع على تعريف الجريمة الإلكترونية أيضاً لا يوجد تعريف مقبول عالمياً للإرهاب ولا في الإرهاب السيبراني حيث تراوحت التعريفات ما بين تعريفات فضفاضة بأنه النشاط الإرهابي عبر الإنترنت، إلى مفاهيم أضيق بأن "الإرهاب السيبراني جريمة تعتمد على الإنترنت ترتكب لأهداف سياسية لإثارة الخوف

والترهيب و/أو إكراه حكومة أو مجموعة مستهدفة، والتسبب أو التهديد بالتسبب في ضرر مثل التخريب أو ضد البنية التحتية"[١٠].

تعريف مكتب التحقيقات الفيدرالي (FBI) للإرهاب الإلكتروني، بأنه "هجوم مخطط، ذو دوافع سياسية، ويستهدف المعلومات والأنظمة الإلكترونية وبرامجها وبياناتها، ويترتب على ذلك استخدام العنف ضد أهداف غير قتالية، بواسطة مجموعات وطنية فرعية أو عملاء سريين"[١١].

أيضاً يعني بالإرهاب الإلكتروني استخدام الإنترنت لتجنيد أعضاء جدد، ووضع المعلومات التي تهدف إلى إثارة الكراهية القومية والتعصب القائم على العنصرية، ويتم دعم معظم المواقع المتطرفة والإرهابية من خارج الدول المُستهدفة، فمن السهل جداً إنشاء موقع إلكتروني على شبكة الإنترنت في أي بلد يستغرق الأمر فقط 50 دقيقة وبعض النقود، ومن السهل أيضاً أن يكون الموقع تحت اسم مستعار وأن يحوي أي معلومات، فعلي سبيل المثال من الممكن العثور على مواقع تُقدم خدمات قاتل مُحترف،كذلك من السهل العثور على مواقع تجارة المخدرات أو صناعة القنابل.(١٢)

ووفقاً لكليفورد أ.ويلك، فإن التهديد الحقيقي لأمن المعلومات يأتي من الداخل، فمن الحقائق المعروفة أن معظم الاختراقات الأمنية تحدث من داخل المنظمة، وبالتالي يمكن أن يحدث الإرهاب السيبراني أيضاً في شكل هجمات إلكترونية من قبل أشخاص مصرح لهم داخل المنظمة، ومن خلال ذلك الاختراق يستطيعوا الوصول إلى الشبكات والأنظمة الداخلية للمنظمة، وهذا النوع من الهجمات التي يتسبب فيها عناصر داخلية هي أخطر بكثير من الهجمات الخارجية بسبب صعوبة اكتشافها[١٣].

فالمتابع لشبكة الانترنت ومدى تنامي الخلايا الإرهابية من خلالها يستشعر الدور الكبير والخطير الذي تؤديه هذه الشبكة، فقد أصبحت مرتعاً لتكاثر هذه الخلايا وانتشارها فلم تعد الإنترنت تقتصر على مجرد مواقع فنية ورياضية، وإخبارية ... أو غرف دردشة يقضي الشاب فيها وقت فراغه بل أصبحت في كثيرٍ من الأحيان أكاديمية حربية تعلمه فنون الحرب، والقتال، ووسيلة سهلة لتجنيده وتأهيله ليصبح فيما بعد إرهابياً من الدرجة الأولى.

ويؤكد الدكتور " أحمد حسن موكلي " بأن التحول الكبير في مفهوم وغرض الانترنت جاء بعد دخول تنظيم القاعدة إلى هذا الفضاء الافتراضي لتحقيق أهدافه ومصالحه، فتنظيم القاعدة لم يكن يحلم لمجرد الحلم أن تكون له وسيلة إعلامية بهذا الحجم والسرعة في الانتشار تحقق له ما يسعى إليه من انتشار فكري يتحول في مراحل لاحقة إلى تنظيم حركي.(١٤)

كما عرفه (مركز حماية البنية التحتية القومية الأمريكية) بأنه كل عمل إجرامي يتم التحضير له عن طريق استخدام أجهزة الكمبيوتر والاتصالات السلكية واللاسلكية، ينتج عنه تدمير أو تعطيل الخدمات لبث الخوف بهدف إرباك وزرع الشك لدى السكان وذلك بهدف التأثير على الحكومة أو السكان لخدمة أجندة سياسية أو اجتماعية أيديولوجية[١٥].

وأشارت المادة الخامسة عشرة في الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في تعريفها عن ما هية الجرائم المتعلقة بالإرهاب والمرتكبة بواسطة تقنية المعلومات[١٦]:

- نشر أفكار ومبادئ جماعات إرهابية والدعوة لها.
- تمويل العمليات الإرهابية والتدريب عليها وتسهيل الاتصالات بين التنظيمات الإرهابية.
- نشر طرق صناعة المتفجرات والتي تستخدم خاصة في عمليات إرهابية.
- نشر النعرات والفتن والاعتداء على الأديان والمعتقدات.

وكما أن هناك اختلاف بين الجرائم التقليدية في مجملها وبين الجرائم الإرهابية فلا ينبغي الخلط بين مفهوم الجريمة الإلكترونية ومفهوم الإرهاب الإلكتروني فمثلما يكون الإرهاب التقليدي أكثر شدة وحدة من أشكال الإجرام الأخرى، فإن الإرهاب الإلكتروني دائماً ما يكون أكثر شدة من السلوكيات الأخرى التي يتم تنفيذها داخل أو خارج الفضاء الإلكتروني.

وحتى يتم إطلاق مصطلح (الإرهاب السيبراني) على بعض الجرائم يجب أن يكون لها مواصفات خاصة بهذا الفعل الإجرامي، حيث يجب ارتكاب السلوك الإرهابي في الفضاء الإلكتروني ومن الضروري أن يكون الاتجاه السلوكي لدى من ينفذ تلك الجرائم هيكل ومبدأ الضرر وعناصر مجتمعة تحت هدف واحد وهو الضرر وأن يتسم هذا الضرر بالعشوائية، وإلا فلا يمكن اعتبار هذا السلوك إرهاباً إلكترونياً، فلإرهاب الإلكتروني هو جريمة منظمة من جماعة منظمة تعمل بشكل منهجي لارتكاب عدد غير محدد من الجرائم على عكس الجرائم الفردية (الإلكترونية) والتي لا تمثل مثل هذا الخطر في حالة عمل فردي أو مجموعة خاصة بمفردهم حتى لو استخدموا أساليب مماثلة، فاختراق فرد لشبكة الكمبيوتر لأنظمة المراقبة في المطار وتعديل المعلومات التي يتم إصدارها في محطة مراقبة المطار والذي من الممكن أن يعرض حياة الناس للخطر فمن المؤكد انه سلوك إجرامي ولكنه ليس فعلاً إرهابياً إلكترونياً[١٧].

ووفقاص لما سبق، فيمكن تعريف الإرهاب الإلكتروني على أنه هجمات يتم تنفيذها من خلال إرهابيون (دول أو جماعات أو أفراد) ويتم من خلال استخدام تقنية المعلومات وشبكة الإنترنت والأقمار الصناعية، من أجل الوصول لأهدافهم الإرهابية وتحقيق أهدافهم السياسية، والتي من أهمها:

- **إثارة الذعر والتحريض على العنف الجسدي وتعريض حياة الناس وأمنهم للخطر.**
- **إلحاق الضرر بالممتلكات سواء كانت العامة والخاصة أو الإستيلاء عليها.**
- **الوصول إلى قواعد البيانات وتدميرها أو تخريبها.**
- **التدخل في الشئون الداخلية للدولة المستهدفة من خلال زعزعة الأمن والاستقرار في الدولة.**
- **تغيير الوعي وتزييف الواقع والتلاعب في الإدارك لدى الشعوب في دولة ما تجاه جوانب الدولة السياسية والاجتماعية والاقتصادية وهو ما يُسَمى بالتأثيرات النفسية للإرهاب الإلكتروني، ويُضاهي في خطورته خطورة الإرهاب التقليدي.**

٣. خصائص الإرهاب الإلكتروني:

- الإرهاب الإلكتروني لا يترك أي دليل مادي بعد ارتكاب جرائمه، وهذا مما يُصَعِب عملية التعقب واكتشاف الجريمة أساساً.
- سهولة إتلاف الأدلة في حال العثور على أي دليل يمكن به إدانة الجاني.
- إن مستخدمي هذا النوع من الإرهاب يمتازون بخلفيات وخبرات في استخدام الأجهزة والتقنيات الحديثة.
- إن الإرهاب الإلكتروني يحدث في بيئة هادئة لا تحتاج إلى القوة والعنف واستعمال الأسلحة، وإنما ما يحتاجه هو جهاز حاسب آلي وبعض البرامج وشبكة الإنترنت.
- عادةً ما تتم العمليات الإرهابية بتعاون عدة أشخاص أو (منظمات إرهابية)[١٨].
- لا يتطلبالإرهاب السيبراني أن يكون الإرهابيون السيبرانيون حاضرين فعلياً في موقع الجريمة، حيث يمكنهم من شن هجماتهم عن بُعد.
- يمكن للإرهابيين السيبرانيين إخفاء هويتهم بسهولة مما يؤدي لصعوب تعقبهم والقبض عليهم.

٤. الفاعل الرئيسي في ممارسة الإرهاب الإلكتروني[١٩]:

هناك ثلاثة أنواع من الفاعلين الرئيسيين في ممارسة الإرهاب الأكتروني، الذين يمتلكون القوة السيبرانية:

- الدولة: حيث لديها القادرة على تنفيذ هجمات إلكترونية وتطوير البنية التحتية وممارسة السلطات داخل حدودها.
- الفاعلون غير الدولة: يستخدم هؤلاء القوة الإلكترونية لأغراض هجومية بالأساس، إلا أن قدرتهم على تنفيذ الهجوم تتطلب مشاركة وكالات استخباراتية متطورة، وعادة لا تمتلك هذه الجماعات إمكانية الدولة في مجال القوة الإلكترونية، لكن يمكن لها تنفيذ هجمات إلكترونية تشمل اختراق المواقع واستهداف أنظمة الاتصالات وغيرها.. .
- الأفراد: وهو أولائك الذين يمتلكون المعرفة التكنولوجية والقدرة على توظيفها، وعادة ما تكون هناك صعوبة بالغة في الكشف عنهم، كما أنه من الصعب ملاحقتهم.

٥. الإرهابي الإلكتروني:

يعتقد الناس عادةً أن الإرهابيين مجانين أو مختل عقلياً، ويمكن تقسيم الأمراض النفسية إلى (المرض النفسي السريري والذي لا يستطيع التمييز بين الصواب والخطأ، لكن الشخص المصاب باضطراب الشخصية يمكنه التمييز بين الصواب والخطأ) فنادراً ما يكون الإرهابي مجنوناً أو ذهانياً.

فالإرهابيون السيبرانيون هم مجموعة فرعية من الإرهابيين، يرثون المظهر النفسي الأساسي للإرهابيين، فهم عقلاء وليسوا مجانين، والمجرم السيبراني له صورة مشابهة للإرهابيين التقليديين، بينما نجد أن الفرق بين الإرهابي الإلكتروني والإرهابي التقليدي هو أن الإرهابي الإلكتروني لديه مهارات قرصنة متطورة ولديهم إلمام واسع بالحاسوب -على عكس الإرهابيون التقليديون- كذلك أيضاً يتمتعون بدرجة عالية من التعليم، حيث أشارت الأبحاث أن ٧١% من الإرهابيين حصلوا على الأقل على تعليم جامعي[٢٠].

وإذا كان هناك اختلافات جوهرية بين الإرهابيون التقليديون والإرهابيون السيبرانيون، كذلك هناك عدة فروق بين المتسلل (المجرم) الإلكتروني والإرهابي الإلكتروني، حيث من الممكن أن يهاجموا نفس الهدف وعلى الرغم من ذلك فإن الإرهابي الإلكتروني بشكل عام لديه موارد أكثر من الهاكر لدعم الهجمات طويلة المدى والمستمرة.

ومن أهم الخصائص البارزة للإرهابيين الإلكترونيين ما يلي[٢١]:

- إذا افترضنا أن الإرهابيين الإلكترونيين قد يكون لديهم تمويل محدد، إلا أنهم قادرين على جمع ما بين مئات الآلاف إلى بضعة ملايين من الدولارات، ويكونون أيضاً على استعداد لإنفاق تلك الأموال التي جمعها لهجماته.
- الإرهابيون السيبرانيون قادرون على الوصول إلى الموارد التجارية عن طريق استشاريين وخبرات تجارية.
- الإرهابيون السيبرانيون قادرين على الحصول على جميع معلومات التصميم للجهات المستهدفة والتي في دائرة اهتمامهم.

٦. مخاطر وتهديدات الإرهاب الإلكتروني على أمن الدول:

يأخذ هذا النوع من الإرهاب شكل إرهاب الدول، ونظراً لخطورة هذه الظاهرة وما يترتب عليها من خسائر بشرية ومادية جسيمة، فقد تزايد الاهتمام بهذا النوع من الإرهاب من قِبَل الأجهزة الأمنية والاستخباراتية في العالم، حيث تتعدد الهجمات والصراعات في الفضاء الإلكتروني والحروب الإلكترونية مثل الصراع الصيني الأمريكي والذي هاجمت فيه الصين مواقع إلكترونية للولايات المتحدة عام ٢٠٠١، حيث تعرض أكثر من موقع أمريكي لهجمات من

قراصنة صينيين ضد مواقع البيت الأبيض والقوات الأمريكية ووزارة الطاقة، كذلك أيضاً الهجمات الروسية ضد الحملة الإنتخابية للولايات المتحدة في عام ٢٠١٦ والذي اتهم فيه ال إف بي أي ١٣ مواطناً روسياً بالتدخل في الانتخابات الرئاسية الأمريكية[٢٢].

ويُعَد أحد العوامل الرئيسية وراء انتشار تهديدات التنظيمات الإرهابية هو استخدام وسائل الإعلام الاجتماعي لنشر الدعاية والتحريض، ويشير أحد التحليلات إلى زيادة استخدام هذه المنصات الرقمية لتجنيد النشطاء الإرهابيين وتعليمهم وتشجيعهم وعلى سبيل المثال قد حولت تنظيم داعش من مجموعة متمردة تسيطر على أراضٍ حقيقية إلى (خلافة افتراضية)، وبدأ التنظيم الأن يستخدم الفضاءات الإلكترونية والمنصات الرقمية لنشر خطاب يوظف الدين في ارتكاب هذه الأعمال[٢٣].

إن من أخطر الهجمات الإرهابية للإرهاب الإلكتروني تلك التي تكون موجهة إلى البنية التحتية في الدول ومؤسسات الأعمال الوطنية، فالإرهاب الإلكتروني يؤدي إلى خسائر مادية فادحة حينما يوجهون هجماتهم إلى البنية التحتية والمؤسسات الوطنية خاصةً المؤسسات المالية مثل البنوك المركزية والتي تؤدي بدورها إلى تأثيرات سلبية على الاقتصادات الوطنية. بينما تعتبر إرسال رسائل بريد إلكترونية مصاب بالفيروسات هي من أسهل الجرائم الإرهابية التي يقوم بها الإرهابيون السيبرانيون خاصةً إذا كانت تلك الرسائل تحمل فيروسات جديدة لا تستطيع برامج الحماية ومكافحة الفيروسات التعرف عليها واكتشافها.

ومن أجل التوضيح، فإن المخاوف المتعلقة بالإرهاب الإلكتروني الفعلي واحتمالية حدوث خسائر مادية هي مخاوف حقيقية، وذلك عند الأخذ في الاعتبار أن البنيات التحتية الحساسة قد أصبحت عرضة للمزيد والمزيد من الهجمات الإلكترونية، ففي عام ٢٠١٧ أفادت التقارير أن ٤٠% من أنظمة البنية التحتية الحساسة قد تم استهدافها بواسطة هجمات إلكترونية، وذلك بزيادة تصل إلى الضعف بالمقارنةن مع السنة الماضية[٢٤].

وتُعد مخاطر هذه المواقع الإرهابية والإباحية على الدول والمجتمع مخاطر كارثية في ضوء الازدياد المضطرد في مستخدمي شبكة الإنترنت وتحول غالبية دول العالم للتحول الرقمي في كافة المجالات والأنشطة والذي أدى إلى زيادة التهديدات على الدول واستقرارها وإعاقة تحقيق التنمية المستدامة في تلك الدول، فضلاً عن تأثيراتها الكارثية على أفراد المجتمع وتحول دون تقدمه وتنميته وازدهاره، لما تخلفه من أثار مدمرة صحياً وبدنياً ونفسياً[٢٥].

وما تجدر الإشارة إليه أن خطورة الإرهاب الإلكتروني تزداد في الدول المتقدمة، التي تدار بنيتها التحتية بالحواسيب الآلية والشبكات المعلوماتية، ما يجعلها هدفاً سهل المنال، فبدلاً من استخدام المتفجرات تستطيع الجماعات والمنظمات الإرهابية من خلال الضغط على لوحة المفاتيح تدمير البنية المعلوماتية، وتحقيق آثار تدميرية تفوق مثيلتها المستخدمة فيها المتفجرات، حيث يمكن شن هجوم إرهابي مدمر لإغلاق المواقع الحيوية وإلحاق الشلل بأنظمة القيادة والسيطرة والاتصالات، أو قطع شبكات الاتصال بين الوحدات والقيادات المركزية، أو تعطيل أنظمة الدفاع الجوي، أو إخراج الصواريخ عن مسارها، أو التحكم في خطوط الملاحة الجوية والبرية والبحرية، أو شلّ محطات الطاقة والمياة، أو اختراق النظام المصرفي وإلحاق الضرر بأعمال البنوك وأسواق المال العالمية.

يُذكر أن تنظيم القاعدة قام باستغلال الإنترنت لتحقيق أهدافه سواء العسكرية أو الدعائية، فالكثير من العمليات الإرهابية التي تقوم بها (القاعدة) يلعب فيها (جوجل إيرث) (Google Earth) الدور الأكبر وفقاً لما أكده العديد من الخبراء، ورغم السيطرة المُحكَمة على الشبكة الدولية إلا أن ذلك لا يمنع ظهور (القاعدة) التي عادةً ما تستخدم الإنترنت وسيلة إعلامية لها[٢٦].

٧. الأبعاد الاجتماعية ومواجهة الإرهاب الإلكتروني:

٧.١. الأثار الاقتصادية للإرهاب الإلكتروني:

لقد أصبح من المألوف حالياً أن يتم تنفيذ كل المعاملات الاقتصادية عبر الإنترنت لكن تطور الإنترنت السريع كقناة لتنفيذ العمال الاقتصادية لم يوازيه بنفس القدر تطور في مستوى الأمن، فقد اشتهرت الإنترنت بكونها بيئة عدائية والدليل على ذلك زيادة الجرائم الاقتصادية الإلكترونية المنظمة خصوصاً تمويل الجماعات الإرهابية التي تؤكد على عدم اتخاذ الإجراءات اللازمة للحد من هذه الظاهرة[٢٧].

وقد قُدِرَ التأثير الاقتصادي العالمي للإرهاب بنحو ٢٦.٤ مليار دولار عام ٢٠١٩، وهذا يمثل انخفاضاً بواقع ٢٥% مقارنة بالعام ٢٠١٨، ومه هذا، لا يمكن لتقدير الأضرار المالية المرتبطة بالإرهاب أن تحدد الكمية الكاملة للأثار غير المباشرة التي تطال النشاط الاقتصادي والتأميني والتكاليف الأمنية المصاحبة لعمليات مكافحة الإرهاب[٢٨].

ولعل من أبز الآثار الاقتصادية خطورة والناجمة عن الفعل الإرهابي عبر منظومة وشبكات الحاسوب والإنترنت، هي[29]:

- البطالة: حيث تؤدي إلى توقع المزيد من الانخفاض في الإنفاق الاستهلاكي، وانخفاض في معدلات الإنفاق الاستثماري، اتجاه الاقتصاد صوب المزيد من التباطؤ في النمو، مع العديد من المشاكل السياسية والاجتماعية المتداخلة.
- حالة الركود والتضخم: إن الاستقرار السياسي والاقتصادي يزيد من فاعلي الطلب كنتيجة لزيادة الإنفاق الاستهلاكي، وهذا ينتج منه ارتفاع في المستوى العام للأسعار ويكون أحياناً في نظاق المقبول اقتصادياً، ولكن في حالات انعدام الأمن أو زيادة المخاوف فإن الطلب يتضاءل ويترتب على ذلك ركود في الأسواق وكساد في الطلب على المنتجات، وعلى العموم فإن التضخم تبعاً للوضع السياسي الدولي والمستوى الاقتصادي العام للدولة التي يمكن أن تواجه انتشار الإرهاب الرقمي، والذي قد يؤثر بوتيرة نسبية متفاوتة وبحسب درجة تركز حالة عدم الاستقرار الناجم عن هذا النوع من الإرهاب في حال بث الدعاية المغرضة وفي إمكانية الشروع بالتهديد للمواقع الاقتصادية المهمة في الدولة، فضلاً عن ترويج لبعض من مصادر العنف والعنف المضاد وفي مناطق مختلفة من العالم.
- الآثار على الاستثمار: العلمليات الإرهابية ومن خلال أجهزة الحاسوب وشبكات المعلوماتية، تهدف إلى تدمير المواقع والبيانات الإلكترونية والنظم المعلوماتية وتعطيلها عن العمل بعد أن تحدث ضرر كبير بالبناء المعلوماتي التحتي وذلك نتيجة التشاؤم وسيادة حالة عدم اليقين في أوساط المستثمرين الناتجة في المرحلة التي أعقبت أحداث الحادي عشر من سبتمبر وانعكاس ذلك على الكثير من قرارات الاستثمار سلباً.

من هنا، فإن الاستثمارات وتدفق الأموال في الأسواق تتعرض للتراجع في أسهمها نتيجة كونها جزء ممن يتعرض للتهديدات الإرهابية الإلكترونية عبر شبكة الإنترنت سواء كانت تلك الهجمات بدوافع اقتصادية أو سياسية.

٧.٢. الحكومة الإلكترونية وحماية الأمن المعلوماتي:

إن بروز مفهوم الحكومة الإلكترونية وانتشار تقنيات المعلومات في كل قطاع من قطاعات الأنشطة البشرية وتغلغلها المستمر فيها بات يؤكد أهمية موضوع الأمن المعلوماتي الوطني لها، بوصفه الأداة الفعَّالة لضمان حماية الحكومة الإلكترونية وضمان نجاح تطبيقاتها على أرض الواقع، ومن جهة أخرى فإن تطور المعرفة لدى مستخدمي الحاسوب وانتشار نظم الشبكات أضحى يشكل تهديداً إضافياً بسبب امتلاك زمرة منتخبة من هؤلاء المستخدمين خبرة رصينة

ورغبة في استكشاف الجوانب الخفية من المواقع الإلكترونية الأمر الذي يسوغ لهم محاولة اختراق نظم الشبكات المتخصصة أو ما يطلق عليه بالقرصنة الإلكترونية[30].

ونتيجة التحول الرقمي في حكومات العديد من البلدان والتوسع في استخدامات التكنولوجيا الرقمية في معظم المؤسسات كالتعليم والصحة والنقل والمواصلات والاقتصاد، كذلك في وظائف العمل الإلكتروني، فكان للحكومة الإلكترونية العديد من السمات الإيجابية في توفير المال والجهد وتقديم الخدمات العامة بتكلفة منخفضة ما يخفض من حجم الإنفاق الحكومي والتخلص من البيروقراطية، ولكن على الرغم من ذلك فهي عرضة لمخاطر أمنية عبر التهديدات والهجمات الإلكترونية لغرض التجسس أو التخريب [31].

ولا يزال منع أو تقييد استخدام الإنترنت لأغراض الإرهاب أو التطرف العنيف مصدر تركيز رئيسي للعديد من الدول الأعضاء التي تعمل في شراكة وثيقة مع القطاع الخاص.[32].

إن ظاهرة الإرهاب الإلكتروني تتفاقم يوماً بعد يوم نظراً لاستعماله للتكنولوجيا الحالية بالإضافة للثغرات الأمنية المتعددة في التعاملات التجارية الإلكترونية، سهل كثيراً عمل الإرهاب الإلكتروني باستخدام الفيروسات مثل إتلاف المعلومات والبيانات للمؤسسات الاستراتيجية الدولية، حيث يستهدف الإرهابيون عدة أهداف منها الاقتصادية أو التجارية على المستويين الإقليمي والدولي، وذلك عن طريق قرصنة أو تعطيل المعلومات، أو عن طريق استغلال الشبكات الاجتماعية المومصلة بالإنترنت، أو بالتجسس على مختلف تعاملات التجارة الإلكترونية[33].

وقد تضاعف اهتمام التنظيمات الجهادية باستخدام الوسائط الاجتماعية لدورها في نشر (أيديولوجيا الجهاد) إلى جيل الشباب في العشرينات أو حتى أصغر سناً، وكان التركيز على عدة مواقع فعَّالة مثل (يوتيوب) (إنستغرام) فيسبوك) (تويتر) بحسبان أن ذلك السن نشأ على مشاهدة مقاطع الفيديو على موقع يوتيوب وأصبح استخدام الوسائط المتعددة جزءاً لا يتجزأ من حياته الفعلية، وتساعد شبكة الإنترنت المنظمات الإرهابية المتفرقة في الاتصال بعضها ببعض والتنسق فيما بينها، نظراً لقة التكاليف بالنسبة لوسائل أخرى أيضاً لوفرة المعلومات التي يمكن تبادلها[34].

٧.٣ . الإرهاب الإلكتروني ومذبحة نيوزيلندا:

يُعد حادث الاعتداء على المسجدين في نيوزيلندا في مدينة كرايستشيرش في ١٥ مارس ٢٠١٩ وتضمنت بثاً حياً على موقع الفيس بوك قد صُنِفَت على أنها أسوأ جريمة قتل جماعي في تاريخ نيوزيلندا الحديث، وتُعَد دليلاً على أن شبكة الإنترنت ومواقع التواصل الاجتماعي حديثاً في عمق دائرة ترويج ثقافة التطرف والعنف والإرهاب لتُعَبِر عن أفكارهم الصاخبة المنحرفة[35].

حيث نتج عنها قتل ٥١ شخصاً وإصابة ٥٠ أخرون، حيث أصبح التفاعُل عبر مواقع التواصل الاجتماعي له أبعاد خاصة بعد المجزرة، حيث تنامت دعوات اليمين المُتطرّف للتمجيد والتعظيم ومواصلة طريق الإرهاب بجميع أشكاله وصوَره، ويحضرني هنا حديث الأكاديمي المُختصّ في شؤون الإرهاب جبريل ويمان، حينما قال إن ما يقرب من ٩٠% من الإرهاب المُنظَّم على شبكة الإنترنت يتمّ عبر منصّات وسائل الإعلام الاجتماعية مثل "تويتر" و"الفيسبوك" و"اليوتيوب" ومنتديات الإنترنت، [36].

الإرهاب الإلكتروني بعد حادث نيوزيلندا الإرهابي أثبت بالدليل القاطِع أن لهذه المنابر "الإرهابية" الافتراضية، نتائج عكسية كشفت عن الوجه "القبيح" للإرهاب الأسود، بقدرتها على تهديد الأمن والاستقرار الاجتماعيّين، والتأثير في الأوضاع السياسية والاقتصادية، وخلق حالة

من الذُعر والفوضى في المجتمعات المُستهدَفة، وقد شرعت بعض الدول الكبرى بالإشتراك مع نيوزيلندا بعقد قمة عالمية حول مكافحة التطرف على شبكة الإنترنت، وقد شارك فيها العديد من الشركات العالمية المتخصصة في تكنولوجيا المعلومات لدحر ظاهرة التطرف ومحاربة الكراهية وتجنب استخدام مواقع التواصل الاجتماعي في الأعمال الإرهابية.

وقد أوضحت القمة إلى كيفية تجنب بث الهجمات الإرهابية على مواقع التواصل الاجتماعي عبر تقنية البث المباشر كذلك وقف استخدام وسائل التواصل الاجتماعي كأداة للترويج للإرهاب وتجنب استخدامها في الأعمال الإرهابية، حيث قام المتهم بتصوير الحادث عبر كاميرا (جو بر) لنقل الأحداث على مواقع التواصل الاجتماعي (فيسبوك) وبمجرد تحميل المقطع المصور شاهده الملايين حول العالم خلال ١٧ دقيقة منذ بثه حتى تحرك مسؤولي الشبكات الاجتماعية لوقف بثه[37].

٨. الطرق والجهود المبذولة لمواجهة الإرهاب الإلكتروني:

٨.١ . الجهود الدولية في مواجهة الإرهاب الإلكتروني:

تُعَد إتفاقية الجرائم الإلكترونية (اتفاقية بودابست) هي أول معاهدة دولية تسعى للتصدي للجرائم الإلكترونية قادتها دول أوروبية وتم تأسيسها في عام ٢٠٠١، وتهدف إلى اتباع سياسة جنائية مشتركة تهدف إلى حماية المجتمع من الجرائم الإلكترونية، لا سيما من خلال اعتماد التشريعات المناسبة، وتنسيق القوانين الوطنية، وتحسين تقنيات التحقيق، وزيادة التعاون بين الدول، كما تضمن هذه الاتفاقية العابرة للحدود التعاون في القوانين والأنظمة الإلكترونية بين الدول الأعضاء، إلى جانب ذلك، تساعد الدول الأعضاء بعضها البعض من خلال التعاون في بناء القدرات والمساعدة المتبادلة وهذه الاتفاقية تعتبر مثال كتعاون دولي في القوانين السيبرانية[38].

وفي عام ٢٠٠٩ تم اعتماد اتفاقية بين حكومات الدول الأعضاء في منظمة شنغهاي للتعاون بشأن التعاون في مجال أمن المعلومات على الصعيد الدولي، وتعتبر المعاهدة الدولية الوحيدة ذات الطابع الإقليمي التي تتناول جزئياً قضايا مكافحة الإرهاب الإلكتروني هي الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الصادرة في ٢١ ديسمبر ٢٠١٠.

وفي عام ٢٠١٣ تم اعتماد اتفاقية تعاون الدول الأعضاء في الكومنولث في مجال أمن المعلومات، أما في عام ٢٠١٢ تم إبرام وثيقة الرياض الخاصة بالقانون الموحد لمكافحة جرائم تقنية المعلومات بدول مجلس التعاون الخليجي، وفي أبريل ٢٠١٨ في إطار الجمعية العامة تم اعتماد قرار (أنشطة منظومة الأمم المتحدة في مجال تنفيذ استراتيجية الأمم المتحدة العالية لمكافحة الإرهاب)[39].

<u>الأمم المتحدة:</u>

يعد استخدام أجهزة شبكات الكمبيوتر من قبل الجهات الإرهابية لتخريب البنى التحتية الوطنية الحيوية مثل الطاقة أو أنظمة النقل أو المياه أو المرافق الحكومية أو الرعاية الصحية أو الاتصالات مصدر قلق متزايد للدول الأعضاء في الأمم المتحدة. أعربت عدة منظمات إرهابية ، بما في ذلك تنظيم القاعدة وداعش / داعش ، عن نيتها بناء قدرات إلكترونية هجومية تسمح لها بتنفيذ هجمات مدمرة محتملة من بعيد. ومن الواضح أن هناك حاجة لبناء أمن الدول الأعضاء وقدرتها على الصمود ضد مثل هذه الهجمات ، فضلاً عن القدرة على التخفيف من تلك الهجمات والتعافي منها واستعادتها ، في حالة حدوثها ، فضلاً عن تقديم المسؤولين عنها إلى العدالة[40].

أعربت الدول الأعضاء، في الاستعراض السادس للاستراتيجية العالمية لمكافحة الإرهاب (A/RES/72/284)، عن قلقها إزاء تزايد استخدام الإرهابيين تكنولوجيات المعلومات والاتصالات، وبخاصة شبكة الإنترنت وغيرها من الوسائط، واستخدام هذه التكنولوجيات لارتكاب الأعمال الإرهابية أو التحريض عليها أو التجنيد لها أو تمويلها أو التخطيط لها. ولاحظت الدول الأعضاء كذلك أهمية التعاون بين أصحاب المصلحة في تنفيذ الاستراتيجية، بما في ذلك التعاون بين الدول الأعضاء والمنظمات الدولية والإقليمية ودون الإقليمية والقطاع الخاص والمجتمع المدني[41].

لقد اتخذ مكتب الأمم المتحدة لمكافحة الإرهاب عدة مبادرات لتعزيز قدرات الدول الأعضاء على منع إساءة استخدام الإرهابيين التطورات التكنولوجية والتخفيف من حِدة أثاره، ويشمل ذلك مواجهة الجرائم الإلكترونية على البُنَى التحتية الحيوية، علاوة على تطوير استخدام وسائل التواصل الاجتماعي كمصادر وادلة رقمية لمكافحة الإرهاب الإلكتروني عبر شبكة الإنترنت.

وأكدت الأمم المتحدة أهمية التعاون بين أصحاب المصلحة في تنفيذ الاستراتيجية، بما في ذلك التعاون بين الدول الأعضاء والمنظمات الدولية الإقليمية ودون الإقليمية والقطاع الخاص والمجتمع المدني[42].

مجلس الأمن:

صدر عن مجلس الأمن عدة قرارات حول مكافحة الإرهاب وأشهر قرار اتخذه مجلس الأمن قرار رقم ١٣٧٣ والذي نص على جملة من التدابير الملزمة للدول أهمها[43]:

- إلتزام جميع الدول بتحريم تقديم المساعدة للأنشطة الإرهابية.
- رفض توفير الدعم المالي للإرهابيين والجماعات الإرهابية.
- عدم توفير ملاذ أمن للإرهابيين والجماعات والتنظيمات الإرهابية.
- ضرورة تبادل المعلومات بشأن الجماعات التي تخطط لشن هجمات إرهابية.

وفي القرار ٢٣٤١ (٢٠١٧)، يهيب مجلس الأمن بالدول الأعضاء إلى "إنشاء أو تعزيز الشراكات الوطنية والإقليمية والدولية مع الجهات صاحبة المصلحة من القطاعين العام والخاص، حسب الاقتضاء، لتبادل المعلومات والخبرات من أجل منع الهجمات الإرهابية على الهياكل الأساسية الحيوية والحماية منها والتخفيف من آثارها والتحقيق فيها ومواجهتها والتعافي من أضرارها، وذلك بوسائل منها التدريب المشترك واستخدام أو إنشاء شبكات ملائمة للاتصال والإنذار في حالات الطوارئ".

وقرار مجلس الأمن ٢٣٧٠ (٢٠١٧) "يحث الدول الأعضاء على العمل بصورة تعاونية لمنع الإرهابيين من حيازة الأسلحة، بما في ذلك من خلال تكنولوجيات المعلومات والاتصالات، مع احترام حقوق الإنسان والحريات الأساسية والامتثال للالتزامات بموجب القانون الدولي، ويشدد على أهمية التعاون مع المجتمع المدني والقطاع الخاص في هذا المسعى، بما في ذلك من خلال إقامة شراكات بين القطاعين العام والخاص"[44].

وفي قراره ٢٣٩٦ (٢٠١٧) لاحظ مجلس الأمن أن الإرهابيين يصوغون روايات مغلوطة ومكذوبة بغرض تحسين صورتها في المجتمع ومن أجل تجنيد المؤيدين والمقاتلين من شتى البقاع، كذلك حشد التأييد المجتمعي، خاصةً من خلال استغلال الموارد التكنولوجية والتقنية عبر شبكة الإنترنت ووسائل التواصل الاجتماعي.

وتُعَد السويد أول دولة تسن تشريعات خاصة بجرائم الحاسب الآلي، إذ صدر قانون البيانات السويدي عام ١٩٧٣ الذي عالج قضايا الاحتيال عن طريق الحاسب الآلي، ثم تبعتها الولايات المتحدة الأمريكية إذ شرَّعت قانوناً خاصاً بحماية أنظمة الحاسب الآلي عام ١٩٧٦، وقد استحدثت الولايات المتحدة الأمريكي قسم محاربة جرائم الكمبيوتر والإرهاب الإلكتروني في مكتب التحقيق الفدرالي عام ١٩٩٨، أما بريطانيا فتأتي ثالثةً من حيث الدول التي تسن قوانين خاصة بجرائم الحاسب الآلي، إذ أقرت قانون مكافحة التزوير والتزييف عام ١٩٨١، وسنت عام ٢٠٠٦ قانون الإرهاب الذي يجرم في الجزء الأول منه قيام شخص بنشر أقوال يقصد بها التشجيع المباشر وغير المباشر لأفراد الجمهور على أن يقوموا بالتحضير لأعمال إرهابية أو التحريض عليها[45].

سياسة مكافحة الإرهاب[46]:

والتي تهدف بالأساس إلى العمل على إيقاف الإرهاب بصورة عامة وليس بشكل محدد من أشكاله، ويعد الاتحاد الدولي للاتصالات (ITU) هو الهيئة الوحيدة المسئولة عن مكافحة الإرهاب الإلكتروني من بين هيئات الأمم المتحدة، كما أن الأمم المتحدة كانت قد أنشأت الشبكة الدولية الإعلامية للعدالة الجنائية (UNCIDIN) وهي متخصصة في المجال الإلكتروني.

- الانتربول: يهتم الإنتربول بمواجهة الجرائم الإلكترونية وعلى رأسها الإرهاب الإلكتروني، كما أن منظمة الإنتربول تعمل على تحليل وسائل التواصل الإجتماعي للوصول إلى البيانات والأدلة التي تدين الإرهابيين وتدل على أماكن تواجدهم لتسهيل الوصول إليهم ومنع هذه العمليات الإرهابية سواء التي تتم على أرض الواقع أو تلك الإلكترونية.
- اللجنة الأوروبية المعنية بالجرائم الإلكترونية: والتي بدأت عملها منذ ١٩٩٧ وهي في تعريفها للجرائم الإلكترونية تضم الإرهاب الإلكتروني، وذلك من خلال المطالبة بتطوير القانون الجنائي ليواكب تطور الإرهاب من خلال استخدام الإنترنت.
- مجموعة الثمانية (G8): في عام ١٩٩٧ تم إنشاء اللجنة الفرعية رقم ٩٨ للاهتمام بالجرائم المتعلقة بالتكنولوجيا المتقدمة والمسئولة عن مكافحة الجرائم الإلكترونية، وبدأت الاهتمام بجرائم الإرهاب الإلكتروني منذ عام ٢٠٠٧ وتم الاتفاق على تجريم استخدام الجماعات الإرهابية للإنترنت كأداة لتنفيذ عملياتهم الإرهابية دون تحديد ماهية هذه العمليات الإرهابية.

٨.٢ . الجهود المصرية في مكافحة جرائم الإرهاب الإلكتروني:

استشعرت مصر متمثلة في القيادة السياسية منذ فترة أهمية التعاون الدولي لمنع استخدام واستغلال الإرهاب للتطور التكنولوجي والمعلوماتي، حيث يُضفي التقدم التكنولوجي أبعاد خطيرة على الظاهرة، من خلال التحريض على التطرف وتجنيد الأفراد وانتشار خطر العناصر الإرهابية من المقاتلين الأجانب، فكان ولابد من توحيد الجهود الدولية في إطار فعال لمكافحة تفشي ظاهرة الإرهاب والفكر المتطرف، حيث تعاملت مصر مع تلك الظاهرة من كافة جوانبها بما في ذلك الأمنية والسياسية والاقتصادية والاجتماعية والفكرية والدينية، فضلاً عن التصدي لآليات التمويل والدعم السياسي والإعلامي للجماعات الإرهابية[47].

والحقيقة أن القانون الجنائي لا يتطور بنفس السرعة التي تتطور بها التكنولوجيا أو مهارة الذهن البشري وفي تسخير هذه المبتكرات للاستخدام السئ، فإذا سلمنا بأن قانون العقوبات الحالي لا يكفي لمواجهة هذا الإجرام الجديد فلا ينبغي أن نقف مكتوفي الأيدي أنا هذا الفراغ التشريعي أو النقص التشريعي بل يجب على المشرع أن يتدخل لمراجعة النصوص القائمة حتي تصبح كفيلة بحماية الحاسب الآلي ومكافحة الإجرام الذي يتولد عن استخدامة واستخدام الشبكة الدولية[48].

غير أن المشرع استطاع أن يضيف بعض القوانين التي تواجه الإجرام المعلوماتي في داخل القانون التقليدي، وذلك في محاوله لسد العجز التشريعي في القانون التقليدي، وهذه القوانين هي كالتالي[49]:

أولاً: قانون العقوبات والنصوص رقم 58 لسنة 1937.
ثانياً: قانون حماية حقوق الملكية الفكرية (رقم 82 لسنة 2002).
ثالثاً: قانون تنظيم الاتصالات (قانون 10 لسنة 2003).
رابعاً: قانون تنظيم التوقيع الإلكتروني (قانون 15 لسنة 2004).
خامساً: قانون الطفل (قانون 126 لسنة 2008).

وقد صدَّقت مصر في العام ٢٠١٨ على القانون رقم ١٧٥ في شأن جرائم تقنية المعلومات، والذي أكد على أهمية تعاون السلطات المختصة مع نظيراتها الأجنبية في إطار الاتفاقيات الدولية والإقليمية والثنائية المصدق عليها، أو تطبيقاً لمبدأ المعاملة بالمثل، بتبادل المعلومات بما من شأنه أن يكفل تفادي ارتكاب جرائم تقنية المعلومات، والمساعدة على التحقيق فيها، وتتبع مرتكبيها- على أن يكون المركز الوطني للاستعداد لطوارئ الحاسب والشبكات هو النقطة الفنية المعتمدة في هذا الشأن.

وقد اهتم القانون بمواجهة العديد من جرائم تقنية المعلومات وأهمها[50]:

- (مادة ١٣) الإعتداء على سلامة شبكات وأنظمة وتقنيات المعلوماتجريمة الانتفاع بدون وجه حق بخدمات الاتصالات والمعلومات.
- مادة (١٤) جريمة الدخول غير المشروع.
- مادة (١٥) جريمة تجاوز حدود الحق في الدخول.
- مادة (١٦) جريمة الاعتراض غير المشروع.
- مادة (١٧) جريمة الاعتداء على سلامة البيانات والمعلمات والنظم المعلوماتية.
- مادة (١٨) جريمة الاعتداء على البريد الإلكتروني أو المواقع أو الحسابات الخاصة.
- مادة (١٩) جريمة الاعتداء على تصميم موقع.
- مادة (٢٠) جريمة الاعتداء على الأنظمة المعلوماتية الخاصة بالدولة.
- مادة (٢١) جريمة الاعتداء على سلامة الشبكة المعلوماتية.
- مادة (٢٢) البرامج والأجهزة والمعدات المستخدمة في اتركاب جرائم تقنية المعلومات.
- مادة (٢٣) جرائم الاحتيال والاعتداء على بطاقات البنوك والخدمات وأدوات الدفع الإلكتروني.
- مادة (٢٤) الجرائم المتعلقة باصطناع المواقع والحسابات الخاصة والبريد الإلكتروني.
- مادة (٢٥) الجرائم المتعلقة بالاعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتي غير المشروع.

ومما سبق نجد الأن أًصبح من الإجباري أن تستثمر معظم البلدان وخاصةً البلدان المتقدمة والنامية المزيد من الأموال لتعزيز نظام الأمن السيبراني الخاص بها، حيث أدى التوسع في الاستخدام الواسع النطاق للفضاء الإلكتروني في معظم الأعمال والاتصالات والإدارة بالتوازي مع نقص الوعي بالأمن السيبراني، والذي أدى إلى النمو المقلق للإرهاب الإلكتروني، هذا إلى جانب عدم وجود قواعد وأنظمة دولية موحدة وقوية وعدم تعديل القوانين والقواعد المنظمة الحالية، هذه العوامل تساعد بشكل خطير الإرهاب الإلكتروني في التطور والنمو وأن يشكل تهديداً للأمن والسلم العالميين.

كذلك يجب أن يتم تفعيل وتعظيم الدور الذي تقوم به مؤسسات المجتمع المدني في التصدي لظاهرة الإرهاب بشكل عام والإرهاب السيبراني بشكل خاص ووأد بذور الفتنة والتطرف

والإرهاب مهما كانت مصادرها محلية أو خارجية، فإن دور المجتمع المدني مهم وأساي في وقاية المجتمع من تلك الظواهر والعمل معاً جنباً إلى جنب في تعزيز دور الدولة في القضاء على تلك الظواهرة الإرهابية "الإرهاب الإلكتروني".

٩. الإجراءات المنهجية:

٩.١. تحليل البيانات الميدانية (الاستبانة):

قام الباحث بتصميم استمارة استبيان إلكتروني على عينة عشوائية من خلال وضعها على منصات شبكة الإنترنت، وجاءات الردود الخاصة باستجابات المبحوثين (٦٨) مُفردة، وقد قام الباحث بالتحقق من صدق وثبات أسئلة استمارة الاستبيان عن طريق تطبيق الاستمارة على عدد 5 أفراد من العينة، ثم بعد مضي أسبوع تم إعادة تطبيقها على نفس العدد مرة أخرى، وتم حساب معامل الارتباط باستخدام معامل ألفا كرونباخ Cronbach Alpha من خلال برنامج SPSS وقد بلغ معامل الارتباط لمعظم الأسئلة في الاستمارة أكبر أو يساوي (٠.٨٠) ويُعّد هذا مقبولاً جداً استناداً إلى دراسات سابقة.

كذلك أيضاً، تم عرض الاستبيان على عدد من المحكمين من أساتذة علم الاجتماع وتم تنقيح الاستبانة من الأسئلة التي تبتعد عن الموضوع.

وقد اعتمد دليل المقابلة على عدة محار رئيسة:

- أولاً: خصائص عينة الدراسة.
- ثانياً: مفهوم الإرهاب الإلكتروني ومظاهره وأهم أشكاله.
- ثالثاً: الأبعاد الاجتماعية ومواجهة ظاهرة الإرهاب الإلكتروني.

فيما يلي رؤية تحليلية لنتائج الاستبانة:

أولاً: خصائص عينة الدراسة:

١) النوع:

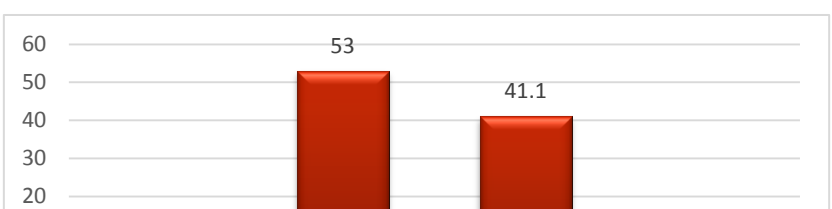
المتغير	العدد	النسبة %
ذكر	٥٦	%٨٢.٣
أنثى	١٢	%١٧.٧
المجموع	٦٨	%١٠٠

جدول رقم (١)

من خلال الجدول رقم (١) يلاحظ أن فئة ال عينة، ثم تأتي فئة الإناث بنسبة (١٧.٦%) أقل من ثلث العينة مما يدل على استجابة افراد العينة من الذكور أكثر إقداماً على الإجابة في مواضيع تحمل عنوان الإرهاب الإلكتروني، حيث من الممكن أن يتغاضى كثير من الإناث عن الإجابة نظراً لما يعنيه عنوان الموضوع من خطورة لفظية.

٢) الفئة العمرية:

جدول رقم (٢)



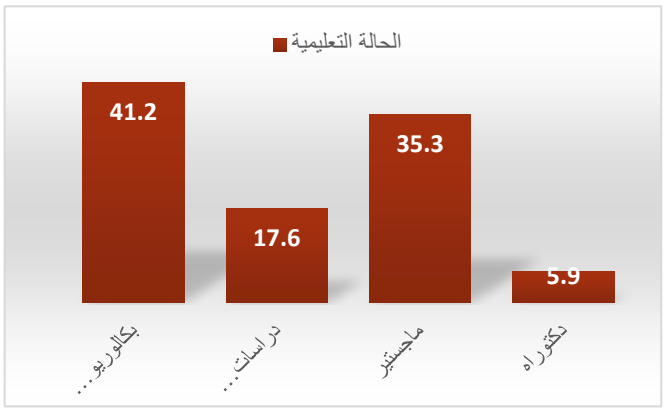
المتغير	العدد	النسبة %
١٨-٢٤	٤	%٥.٩
٢٥-٣٤	٣٦	%٥٣
٣٥-٥٤	٢٨	%٤١.١
٥٥+	٠	%٠
المجموع	٦٨	%١٠٠

يتضح من الجدول رقم (٢) أن الفئة العمرية من (٢٥-٣٤) قد احتلت المرتبة الأولى بنسبة (٥٣%)، ثم جاءت الفئة العمرية (٣٥-٥٤) بنسبة (٤١.١%)، ثم الفئة العمرية من (١٨-٢٤) بنسبة (٥.٩%)- وبيانات الجدول تعكس أن أغلبية عينة الدراسة من المرحلة العمرية التي تتسم بالشباب والرجولة، حيث لديها القدرة على التعامل مع كل ماهو جديد من مصطلحات، وهذه الفئة تُعَد من أكثر الفئات استخداماً لشبكة الإنترنت.

٣) الحالة الوظيفية وعدد سنوات الخبرة:

جدول رقم (٣)

المتغير	العدد	النسبة %
بكالوريوس/ليسانس	٢٨	%٤١.٢
دراسات عليا	١٢	%١٧.٦
ماجستير	٢٤	%٣٥.٣
دكتوراه	٤	%٥.٩
المجموع	٦٨	%١٠٠



يتضح من الجدول (٣) أن (الحالة التعليمية) لكل أفراد العينة مع اختلاف درجاتهم الوظيفية وتنوعها لا يوجد بينهم تعليم أقل من التعليم العالي، حيث جاءت فئة (بكالوريوس/ليسانس) في المرتبة الأولى بنسبة (٤١.٢%)، ثم فئة (ماجستير) بنسبة (٣٥.٣%)، ثم جاءت فئة (دراسات عليا) في المرتبة الثالثة بنسبة (١٧.٦%)، وأخيراً جاءت فئة (دكتوراه) في المرتبة الرابعة.

ولا شك أن هذا يعكس مدى تأثير الحالة التعليمية على تشكيل الوعي الثقافي لأفراد العينة، ومدى تأثرهم بكل المواضيع الهامة والمعاصرة التي تخص استخدامعم لشبكة الإنترنت، والتوسع في استخداماتهم لنظ المعلومات.

٤) الحالة الوظيفية وعدد سنوات الخبرة:

قَدَم الباحث هذا السؤال على شكل سؤال مفتوح حتى يتم الحصول على إجابات متنوعة، فجاءت إجابات المبحوثين على هذا السؤال بنسبة ٥٣% من أفراد العينة، وتنوعت الوظائف ما بين (مطور تطبيقات للأندرويد مع خبرة ٤ سنوات – ومخرج تليفزيوني مع خبرة ٢٠ سنة – محامي مع خبرة ٢٠ سنة – مدير تسويق مع خبرة ٢١ سمة – مدرس مع خبرة ١٠ سنوات في مجال التعليم – طبيب عظام مع خبرة ٧ سنوات – موظف مع خبرة ٧ سنوات

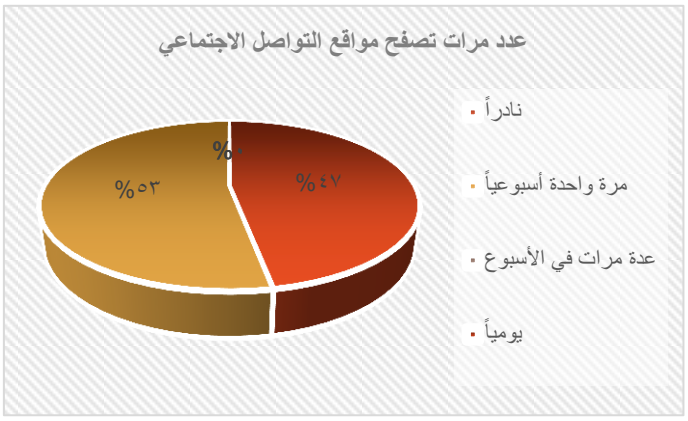
– أستاذ جامعي مع خبرة ١٢ سنة)، وتوضح لنا هذه البيانات مدى الخبرة العلمية والعملية لدى أفراد العينة والتي تؤثر على تشكيل الوعي الثقافي لديهم وتشكيل اهتماماتهم في أثناء التعامل مع شبكة الإنترنت ومدى معرفتهم لمصطلح الإرهاب الإلكتروني.

ثانياً: مفهوم الإرهاب الإلكتروني ومظاهره وأهم أشكاله:

٥) كم عدد المرات التي تتصفح فيها مواقع التواصل الاجتماعي؟

جدول رقم (٤)

المتغير	العدد	النسبة %
نادراً	٠	٠%
مرة واحدة أسبوعياً	٠	٠%
عدة مرات في الأسبوع	٠	٠%
يومياً	٣٢	٤٧.١%
عدة مرات في اليوم الواحد	٣٦	٥٢.٩%
المجموع	٦٨	١٠٠%



يتضح من الجدول السابق جدول رقم (٤) أن الوقت الذي يقضيه أفراد العينة على مواقع التواصل الاجتماعي يعكس مدى اهتمام أفراد العينة بأهمية التواصل عبر مواقع التواصل الاجتماعي لفترات كبيرة، حيث جاءت في المرتبة الأولى فئة (عدة مرات في اليوم الواحد) بنسبة (٥٣%) ثم فئة (يومياً) بنسبة (٤٧%) في المرتبة الثانية، أما باقي الفئات فجات كلها بنسبة (٠%)، أي أن عينة البحث كلها تقريباً يتواجدون على شبكة الإنترنت ومواقع التواصل الاجتماعي بصورة دائمة سواء يومياً أو عدة مرات في اليوم، والذي يعكس الأهمية التي أصبحت عليها مواقع التواصل الاجتماعي في اختراق الحياة الاجتماعية وتأثيرها على حياة الأفراد في كافة المجالات.

٦) هل لديك مِعرفة مُسبَقة بمصطلح الإرهاب الإلكتروني؟

جدول رقم (٥)

المتغير	العدد	النسبة %
لا، لم أسمع بهذا المصطلح من قبل	٢٨	٥.٩%
نعم، ولكني غير متأكد من ماهيته	٢٤	٣٥.٣%

نعم، لدي القليل من المعرفة الخاصة بالمقصود بالإرهاب الإلكتروني	١٢	%٤١.٢
نعم، أفهم تماماً مفهوم الإرهاب الإلكتروني	٤	%١٧.٦
المجموع	٦٨	%١٠٠

يتضح من الجدول رقم (٥) أن فئة (نعم، لدي القليل من المعرفة الخاصة بالمقصود بالإرهاب الإلكتروني) بنسبة (٤١.٢%) في المرتبة الأولى، ثم تلتها فئة (نعم، ولكني غير متأكد من ماهيته) بنسبة (٣٥.٣%)، ثم جاءت فئة (لم أسمع بهذا المصطلح من قبل) وفئة (نعم، أفهم تماماً مفهوم الإرهاب الإلكتروني) بنسب (٥.٩%) و (٤.٥%) على التوالي، مما يعكس ظهور

المتغير	العدد	النسبة %
أن يحدث في الفضاء السيبراني	٣٢	%٢١.٦
استخدام شكل من أشكال نظام الكمبيوتر من أجل تنفيذ هجمات على نظام الكمبيوتر المستهدف أو المعلومات التي يحتوية	٣٦	%٢٤.٤
يسبب الخوف من خلال العنف أو إيذاء الأشخاص أو الممتلكات	٤٠	%٢٧
أن يكون ذات دوافع سياسية أو دينية أو أيديولوجية	٤٠	%٢٧
المجموع	١٤٨	%١٠٠

المصطلح لدى أفراد العينة كمصطلح حديث نسبياً جاء نتيجة التوسع في الاعتماد على نظم المعلومات وشبكة الإنترنت في كافة المجالات، حيث بدأ المصطلح يطرح نفسه أمام مستخدمي شبكة الإنترنت كتهديد لا بد من فهم ماهيته.

٧) <u>حتى نستطيع تصنيف عمل ما على أنه إرهاب إلكتروني، يجب أن يتسم الفعل بكونه... (اختيار متعدد)؟</u>

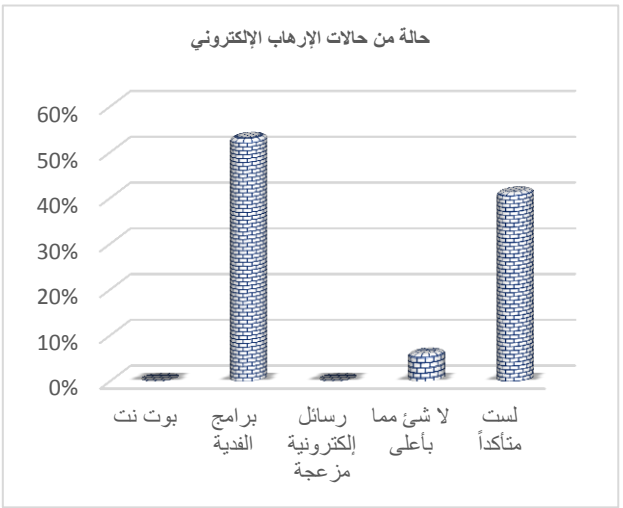
جدول رقم (٦)

يتضح من الجدول (٦)، تعدد وتقارب الفئات في الاختيارات أفراد العينة من حيث تداخل جميع الفئات في عملية تكوين أهداف عمليات الإرهاب الإلكتروني، حيث اشتراك تلك العوامل واجتماعها معاً يوضح طبيعة العمليات الإرهابية السيبرانية في كونها مرتبطة بنظم المعلومات وشبكة الإنترنت وأن من أهم ما يميز الإرهاب الإلكتروني هو حدوثه في الفضاء السيبراني مستخدماً نظم المعلومات وشبكة الإنترنت ويعمل على بث الرعب والقتل والتخريب ويحمل دوافع سياسية أو دينية، وأن مايميزها عن الإرهاب التقليدي هي أن الأنظمة الإلكترونية والبنية التحتية المعلوماتية نفسها أصبحت هي هدف للإرهابيين، وهذا ما أكده أيضاً دراسة (جانيت بريتشارد ولوري إي ماكدونالد) حيث أكدوا على وصف الإرهاب الإلكتروني بأنه هجمات تحدث في الفضاء السيبراني ذات دوافع سياسية وتهدف إلى إحداث أضرار جسيمة مثل الخسائر في الأرواح أو الأضرار الاقتصادية الجسيمة[51].

٨) يصل المجرمون إلى جهاز الكمبيوتر الخاص بشخص ما ويقومون بتشفير الملفات والبيانات الشخصية له ولا يتستطيع الوصول إلى هذه ا لبيانات ما لم يدفع للمجرمين لفك التشفير الخاص بتلك الملفات، هذه الممارسة تسمى ....:

المتغير	العدد	النسبة %
بوت نت	-	-
برامج الفدية	٣٦	%٥٣
رسائل إلكترونية مزعجة	-	-
لا شئ مما بأعلى	٤	%٥.٩
لست متأكداً	٢٨	%٤١.١
المجموع	١٤٨	%١٠٠

جدول رقم (٧)



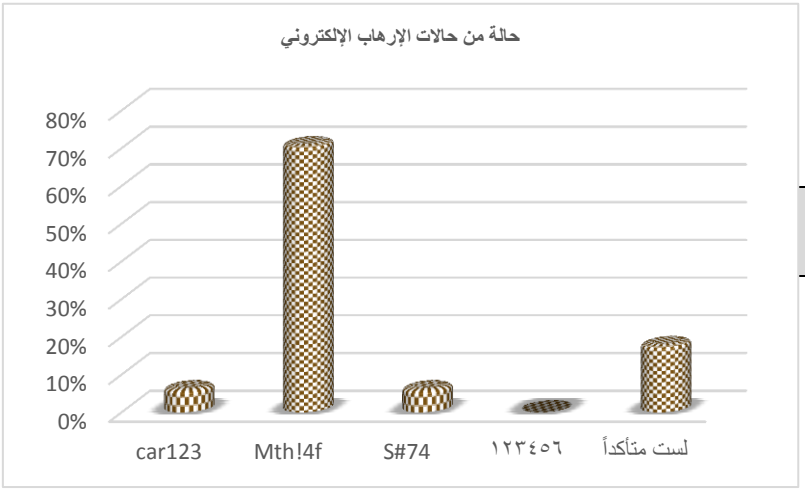
يتضح من الجدول رقم (٧)، الاختلاف بين أفراد العينة من حيث معرفتهم بأنواع الجرائم السيبرانية، حيث اتضح من هذا السؤال أن نسبة (٥٣%) كانت على علم بهذه الحالة وأنها

تُسمى بـ (حرائم الفدية) في الجرائم الإلكترونية وهذا يُعد نوع من أنواع الإرهاب الواقع على الشخص، حيث يتعرض الفرد لابتزاز من أحد المجرمين بعد السيطرة على بياناته على الجهاز الخاص به وطلب فديه لإرجاع تلك البيانات، بينما جاءت فئة (لست متأكداً) بنسبة (٤١.١%) وهي نسبة عالية نوعاً ما في عدم معرفتها بهذا النوع من الجرائم رغم انتشارها مثل الدخول غير المشروع والاستيلاء على البيانات وانتهاك السرية والخصوصية للبيانات الشخصية والإضرار بصاحبها،

المتغير	العدد	النسبة %
Car123	4	%٥.٩
Mth!4f	48	%٧٠.٦
S#74	4	%٥.٩
0123456	-	-
لست متأكداً	١٢	%١٧.٦
المجموع	68	%١٠٠

٩) أي من كلمات المرور الأربعة التالية هي الأكثر أماناً؟

جدول رقم (٨)

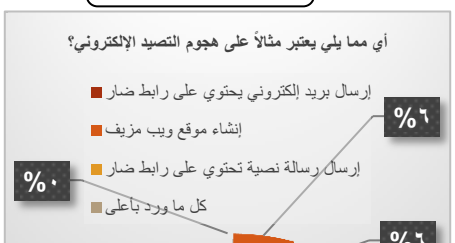


المتغير

توضح بيانات الجدول رقم (٨) مدى اهتمام أفراد العينة بكلمات المرور الخاصة بهم كنوع من أنواع الحماية لبياناتهم سواء على الكمبيوتر أو على الموبايل، حيث أظهرت اختيارات أفراد العينة لفئة (Mth!4f) بنسبة (٧٠.٦%) على أنها كلمة المرور الأكثر أماناً مدى وعي المبحوثين بالمستوى الأول من مستويات الأمان عند اتصال أجهزتهم بشبكة الإنترنت.

١٠) أي مما يلي يعتبر مثالاً على هجوم (التصيد الإلكتروني)؟

جدول رقم (٩)



إرسال بريد إلكتروني إلى شخص ما يحتوي على رابط ضار يتنكر في شكل رسالة بريد إلكتروني من شخص أعرفه.	-	-
إنشاء موقع ويب مزيف يشبه إلى حد كبير موقع الويب الحقيقي لخداع المستخدمين لإدخال معلومات تسجيل الدخول الخاصة بهم.	٤	%٥.٩
إرسال رسالة نصية إلى شخص ما تحتوي على رابط ضار يتنكر في شكل إشعار يفيد بأن ا لشخص قد فاز في مسابقة ما.	٤	%٥.٩
كل ما ورد بأعلى.	٦٠	%٨٨.٢
لست متأكداً.	-	-
المجموع	٦٨	%١٠٠

في هذا السؤال تحديداً (جدول رقم ٩) اختار الباحث توجيه عينة البحث ناحية أحد الجرائم الإلكترونية الواسعة الانتشار وهي (التصيد الإلكتروني Phishing) لمعرفة مدى اطلاعهم ومعرفتهم بالجرائم الإلكترونية والتي هي باب للإرهاب الإلكتروني، واختار الباحث (التصيد الإلكتروني) تحديداً لانتشاره الواسع وتعرض معظم مستخدمي الإنترنت له من خلال الاحتيال في شكل رسائل بريد إلكتروني أو نصوص مزيفة تبدو وكأنها من شركة مشروعة يتم من خلالها تثبيت برامج الفدية التي تسمح للمحتالين الوصول إلى جهاز الكمبيوتر الخاص بالضحية ثم سرقة بياناته ومعلوماته الشخصية وأرقام بطاقات الائتمان حيث يمكن أن تظهر مواقع التصيد الاحتيالي متطابقة مع مواقع الويب الرسمية مما يدفع المستخدمين إلى إدخال بياناتهم الحقيقية على الويب الضار.

وتُعَد عمليات التصيد الاحتيالي من أكثر الهجمات شيوعاً على المستهلكين، وفقاً لمكتب التحقيق الفيدرالي، وقع أكثر من ١١٤.٧٠٠ شخص ضحية لعمليات التصيد الاحتيالي في عام ٢٠١٩، وخسروا ما يقارب من ٥٧.٨ مليون دولار أي بمتوسط خسائر ٥٠٠ دولار لكل واحد منهم[52].

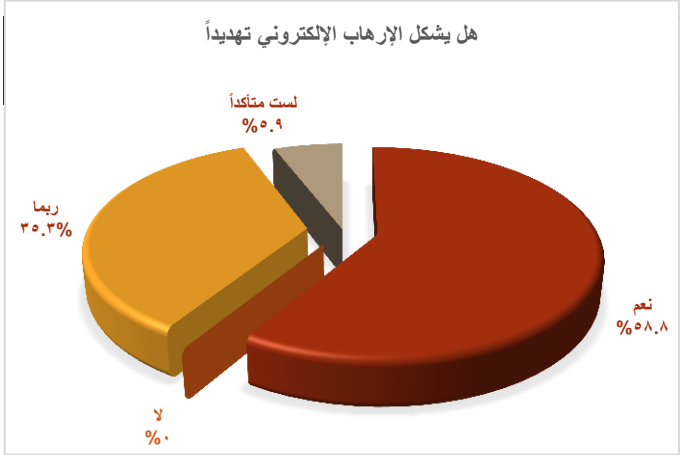
وهذا ما أكدته بيانات الجدول السابق، حيث جائت في المرتبة الأولي فئة (كل ما ورد بأعلى) بنسبة (٨٨.٢%) والتي تعني بأن معظم أفراد عينة البحث على دراية بمفهوم التصيد

الإلكتروني وخطورته في كونه باب لكل المشكلات التي قد تنتج عن اختراق للجهاز وسرقة بيانات الضحية ومساومته وتجنيده في بعض الأحيان.

١١) من وجهة نظرك، هل يشكل الإرهاب الإلكتروني تهديداً كبيراً؟

المتغير

جدول رقم (١٠)



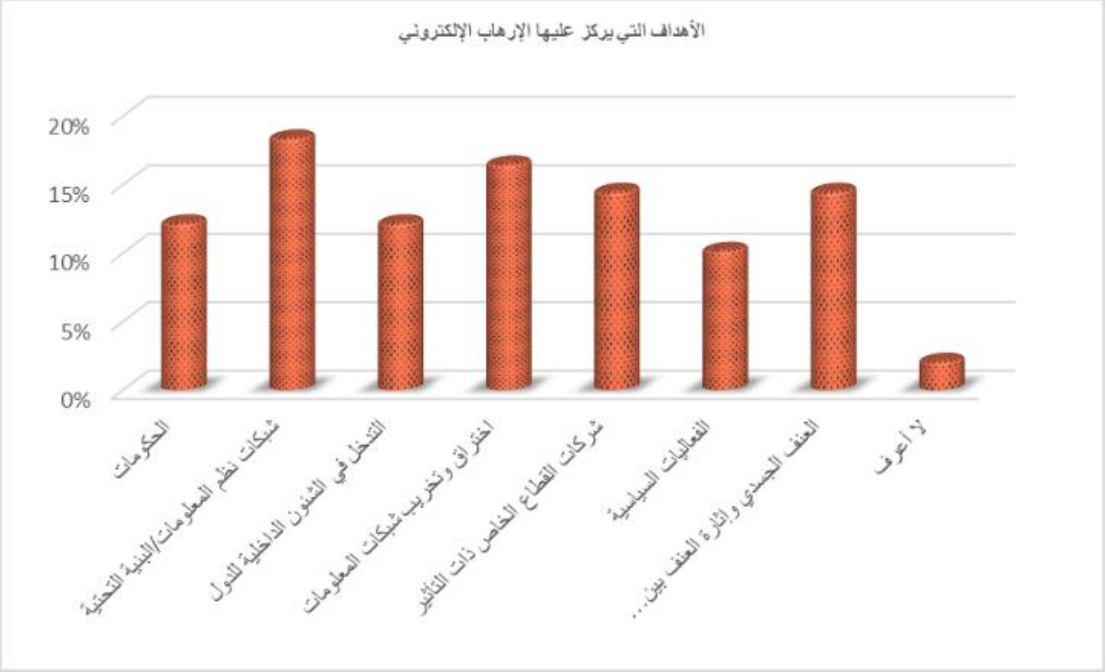
المتغير	العدد	النسبة %
نعم	٤٠	%٥٨.٨
لا	-	-
ربما	٢٤	%٣٥.٣
لست متأكداً	٤	%٥.٩
المجموع	٦٨	%١٠٠

من خلال هذا الجدول رقم (١٠) يتضح أن أكثر من نصف العينة كانوا يعتبرون أن الإرهاب الإلكتروني يسبب تهديداً كبيراً، حيث جائت في المرتبة الأولي فئة (نعم) بنسبة (٥٨.٨%)، بينما جائت بعدها في الترتيب فئة (ربما) بنسبة (٣٥.٣%)، أي أن ما يُقارب من (٩٥%) من أفراد العينة يعتبرون أن الإرهاب الإلكتروني يمثل تهديداً أو من المحتمل أن يمثل تهديداً كبيراً، وهذا الإحساس بخطر الإرهاب الإلكتروني نابع من التحول الإلكتروني في كافة القطاعات والتوسع في الاعتماد على شبكة الإنترنت في كافة المجالات مما يسبب زيادة في احتمالية استخدامها في القيام بأعمال إرهابية، بينما جائت في المرتبة الأخيرة فئة (لست متأكداً) بنسبة (٥.٩%).

١٢) إذا كانت وجهة نظرك أن الإرهاب الإلكتروني يشكل تهديداً كبيراً، فما هو التهديد أو الأهداف التي يكز عليها؟ (اختيار متعدد).

الدول/ الحكومات	٢٤	%١٢.٢
البنية التحتية الحساسة/ شبكات الكمبيوتر	٣٦	%١٨.٤
المؤسسات/القطاع الخاص/ الاقتصاد	٢٨	%١٤.٣
التدخل في الشئون الداخلية للدولة المستهدفة من خلال زعزعة الأمن والاستقرار في الدولة	٢٤	%١٢.٢
إختراق قواعد البيانات وتدميرها أو تخريبها	٣٢	%١٦.٣
الفعاليات السياسية (مثل الانتخابات بكافة أشكالها السياسية)	٢٠	%١٠.٢
إثارة الذعر والتحريض على العنف الجسدي وتعريض حياة الناس وأمنهم للخطر إثارة الذعر والتحريض على العنف الجسدي وتعريض حياة الناس وأمنهم للخطر	٢٨	%١٤.٣
لا أعرف	٤	٢.١ %
المجموع	١٩٦	%١٠٠

جدول رقم (١١)



في الجدول رقم (١١)، جاء استطلاع رأي عينة البحث من خلال فئات متعددة الاختيار، حيث استجاب أفراد العينة في اختيار الفئات بعدد (١٩٦) اختيار، وتنوعت الاختيارات وتقاربت حول الأهداف المحتملة لعمليات الإرهاب الإلكتروني، حيث جاءت الفئة الأكثر اختياراً من عينة البحث وهي فئة (شبكات نظم المعلومات والبنية التحتية) بنسبة (١٨.٤%) حيث تم اختيارها (٣٦) اختيار من عينة البحث، وتلتها فئة (اختراق وتدمير قواعد البيانات وتخريبها) بنسبة

(١٧%) وقد تم اختيارها عدد (٣٢) اختيار، ثم فئة (شركات القطاع الخاص الكبرى) بالتساوي مع فئة (إثارة الذعر والعنف الجسدي) بنسبة (١٥%)، ثم فئة (التدخل في شئون الدولة) بنسبة (١٢%)، تلتها فئة (الفعاليات السياسية) بنسبة (١٠%)، وأخيراً فئة (لا أعرف) بنسبة (٢%).

ويدل هذا التعدد في الاختيارات على تنوع أهداف الإرهاب الإلكتروني ومقدار الخسائر التي من الممكن أن يسببها، حيث التوسع في استخدام نظم المعلومات وشبكات الكمبيوتر في معظم المجالات الحساسة بالدول وربطها بشبكة الإنترنت أدى إلى التوسع في أهداف الإرهابيين السيبرانيين والتوسع في عملياتهم والقدرة على إحداث خسائر اقتصادية وبشرية فادحة..

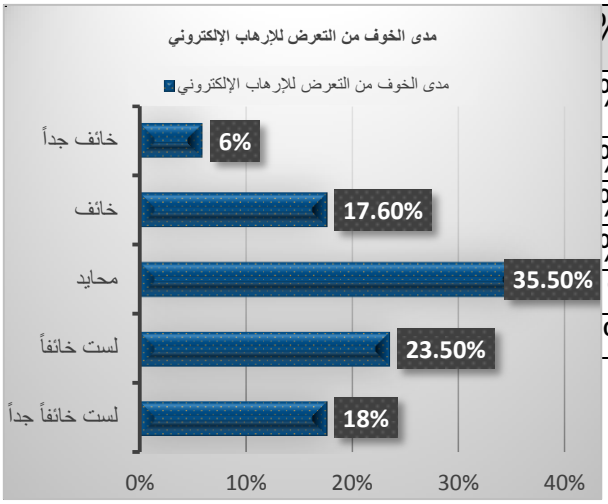
وهذه النتائج أكدتها دراسة (فريدة بن عمروش) حيث أكدت على أن الإرهاب الإلكتروني يهدف إلى تحقيق جملة من الأهداف غير المشروعة يمكن إبرازها في ضوء الآتي[53]:

(نشر الخوف والرعب بين الأشخاص والدول – الإخلال بالأمن المعلوماتي – تدمير البنية التحتية المعلوماتية – إثارة الرأي العام – الاستيلاء على الأموال).

١٣) يستخدم الإرهابي الإلكتروني جهاز الكمبيوتر لشن هجماته، إلى أي مدى يصل خوفك الحالي من هجوم إرهابي إلكتروني ضدك أو ضد عائلتك؟

جدول رقم (١١)

المتغير	العدد	النسبة %
لست خائفاً جداً	١٢	%١٧.٦
لست خائفاً	١٦	%٢٣.٥
محايد	٢٤	%٣٥.٣
خائف	١٢	%١٧.٦
خائف جداً	٤	%٥.٩
المجموع	٦٨	%١٠٠



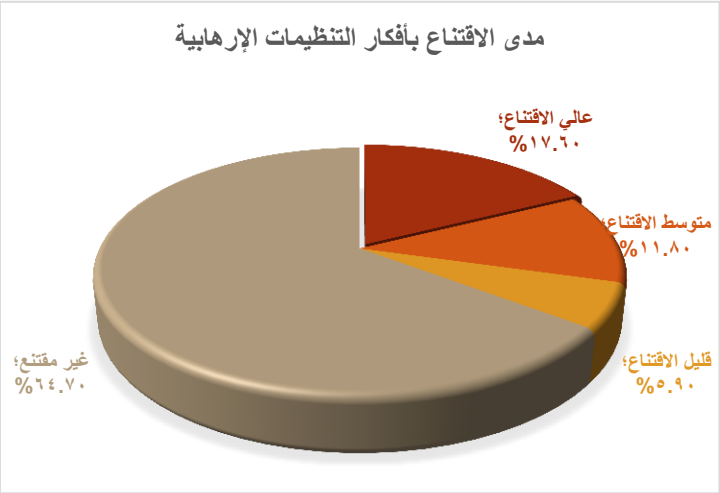
تم ترميز هذا السؤال الخاص بمدى خوف عينة البحث من التعرض للإرهاب الإلكتروني في شكل مقياس خماسي (مقياس ليكرت) وقياس مدى خوف عينة البحث من التعرض للإرهاب الإلكتروني، حيث جاءت النتائج لتؤكد أن نسبة (٣٥.٥%) من المبحوثين أجابت بأنها على الحياد من مدى احتمالية تعرضها لهجمات إرهاب إلكتروني وربما يرجع ذلك للنظر إلى الإرهاب الإلكتروني على أنه ليس بالظاهرة المهمة في الوقت الحاضر وعدم توليها أي اهتمام،

ويُعَزِز ذلك ما تلتها من فئة حيث جاءت فئة (لست خائفاً) وفئة (لست خائفاً جداً) بنسب (٢٣.٥%) و (١٧.٦%) على التوالي وهو ما أكد على أن معظم أفراد العينة يستبعدون أي عمل إرهابي عن طريق الإنترنت تجاههم أو أفراد عائلاتهم، وهذا يُعد مثيراً للاهتمام حيث يُعد الإرهاب الإلكتروني مصدر تهديد كبير حالياً واحتمالية وقوعه هي احتمالية كبيرة حيث أصبح يمثل تهديداً كبيراً.

المتغير	العدد	النسبة %
عالي الاقتناع	١٢	%١٧.٦
متوسط الاقتناع	٨	%١١.٨
قليل الاقتناع	٤	%٥.٩
غير مقتنع	٤٤	%٦٤.٧
المجموع	٦٨	%١٠٠

جدول رقم (١٣)

١٤) ما مدى اقتناعك بأفكار التنظيمات الإرهابية؟



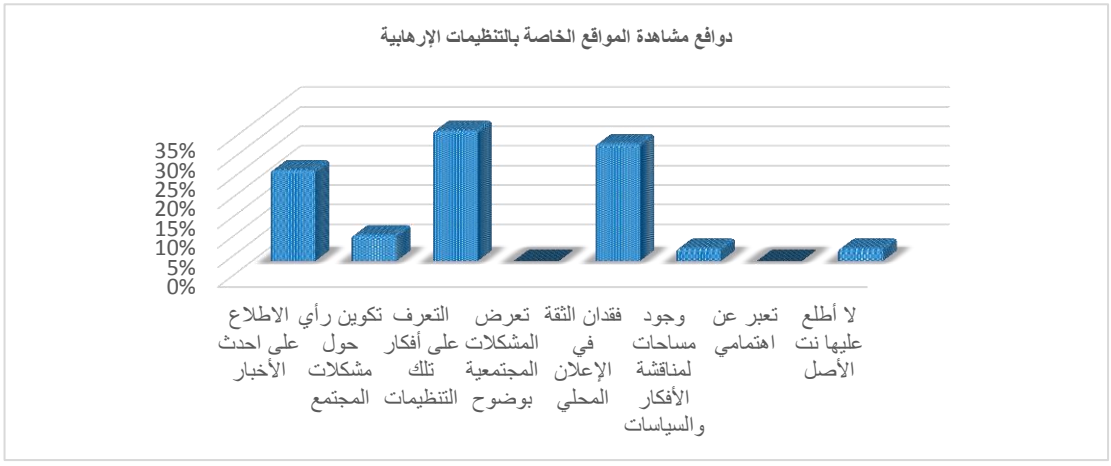
المتغير	العدد	النسبة %

يوضح الجدول رقم (١٣) من خلال مقياس رباعي مدى اقتناع المبحوثين بأفكار مواقع التنظيمات الإرهابية على شبكة الإرنت، حيث جاءت في مقدمة الترتيب فئة (غير مقتنع) بنسبة (٦٤.٧%) ليعكس مدى وعي المبحوثين بسلبية تلك المواقع وما تبُثَّه من أفكار هدامة، ثم جاءت فئة (عالي الاقتناع) بنسبة (١٧.٦%) ثم فئة (متوسط الاقتناع) بنسبة (١١.٨%) وأخيراً فئة (قليل الاقتناع) بنسبة (٥.٩%).

١٥) من وجهة نظرك، ما هي الدوافع الأساسية لمشاهدة المواقع الخاصة بالتنظيمات الإرهابية؟ (اختيار متعدد)

جدول رقم (١٤)

الاطلاع على أحدث الأخبار	٢٨	%٢٣.٣
تكوين رأي حول مشكلات المجتمع	٨	%٦.٧
التعرف على أفكار تلك التنظيمات والجماعات	٤٠	%٣٣.٤
تلك المواقع تعرض المشكلات المجتمعية بصورة واضحة وحقيقية دون تزييف	٠	%٠
فقدان الثقة في الإعلام المحلي	٣٦	%٣٠
وجود مساحات لمناقشة الأفكار والملفات الخاصة بالسياسات العامة للدولة	٤	%٣.٣
تعبر عن اهتمامي	-	%٠
لا أطلع عليها من الأصل	٤	%٣.٣
المجموع	١٢٠	%١٠٠



من خلال الجدول السابق رقم (١٤) نجد أن ما يُقارب من (٨٥%) من عينة البحث لديهم دوافع في زيارة المواقع الخاصة بالتنظيمات الإرهابية حتى لو كانت هذه الزيارة نتيجة إعلانات في صفحات الويب أو عبر رسائل البريد الإلكتروني، ولابد هنا من ربط تواجد أفراد العينة الدائم على منصات التواصل الاجتماعي (انظر الجدول رقم٤) وبين أسبابهم في تصفح تلك المواقع الخاصة بالتنظيمات والجماعات الإرهابية حيث هناك علاقة كبيرة بين تواجد المبحوثين على منصات التواصل الاجتماعي بصورة يومية متكررة وبين تعرضهم وتصفحهم لتلك المواقع وهذا ما أكدته دراسة (أسماء الجيوشي) أن هناك فروق ذات دلالة إحصائية تبعاً لكثافة تعرض المبحوثين لمواقع التواصل الاجتماعي ومدى اقتناعهم بأفكار تلك التنظيمات، فالمبحوثين متوسطي التعرض لمواقع التواصل الاجتماعي التي تستخدمها التنظيمات الإرهابية اكثر تأثراً واقتناعاً بأفكار التنظيم من المبحوثين في المعدلات الأخرى من التعرض للمواقع، ربما يرجع ذلك في أنهم لا يتعرضون لصفحات محددة في مواقع التواصل الاجتماعي وإنما يستخدمون

بشكل عارض مواقع إلكترونية كثيرة ومتنوعة تعكس موضوغات مختلفة مكنتهم من التأثر بالتجنيد الفكري الإلكتروني بأبعاده الفرعية بمستوى أعلى من المبحوثين منخفضي وكثيفي التعرض لمواقع التواصل الاجتماعي[54].

ومن أهم الدوافع لدى أفراد العينة فئة (فقدان الثقة في الإعلام المحلي بنسبة ٣٠%) والذي يؤكد على وضع علامات استفهام حول الإعلام المحلي في معالجة تلك الأحداث وافتقاده للمهنية في التعامل مع الأحداث الإرهابية، حيث يلعب الإعلام دوراً هاماً ومؤثراً في توجهات الرأي العام واتجاهاته وصياغة مواقفه وسلوكياته من خلال الأخبار والمعلومات التي تزوده بها وسائل الإعلام المختلفة، وهذا ما أكده د/ مجيد حمزة في نتائج بحثه بعنوان (الإعلام الإلكتروني للإرهاب وسبل المواجهة إعلامياً) حيث أكد أنه "لابد من وضع استراتيجية إعلامية موحدة وخطاب ديني عقلاني على مستوى العالم الإسلامي والعربي تلتزم به جميع وسائل الإعلام لمواجهة إعلام التنظيمات الإرهابية المختلفة ومنها تنظيم (داعش)[55].

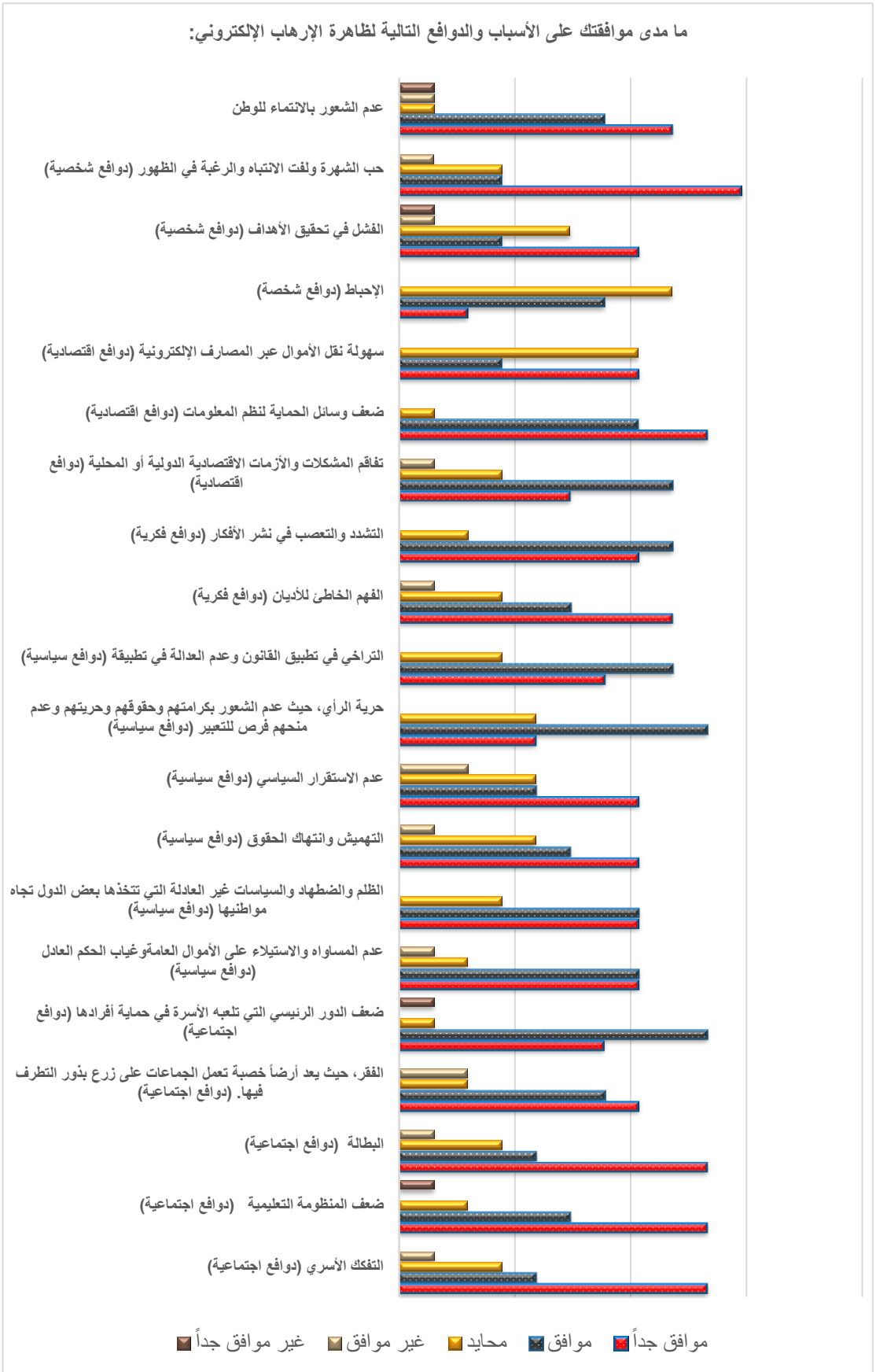
١٦) ما مدى موافقتك على الأسباب والدوافع التالية لظاهرة الإرهاب الإلكتروني:
هناك العديد من الدوافع والغايات التي تدفع الشخص إلى ارتكاب الأفعال الإرهابية عبر شبكة الإنترنت، وقد وضع الباحث مجموعة من الدوافع والأسباب (اجتماعية- شخصية- نفسية- اقتصادية...) وعرضها على أفراد العينة من خلال مقياس خماسي (موافق جداً – موافق – محايد – غير موافق – غير موافق جداً)، وجائت استجابات المبحوثين كالآتي:

- **الدوافع الاجتماعية:** هناك شبه اتفاق بين أفراد العينة على أهمية الدوافع الاجتماعية في تشكيل وعي الأفراد وأفكارهم، حيث الاهتمام بالتربية الاجتماعية والنفسية للفرد داخل الأسرة والرقابة على اتجاهاته الفكرية والسلوكية التي تعكس غالباً نشأته داخل الأسرة، وهذا ما اكدته استجابات المبحوثين في اختياراتهم للدوافع الاجتماعية حيث جاءت (ضعف الدور التي تلعبه الأسرة في حماية أفرادها) كأحد أهم الدوافع المؤدية إلى اتجاه السلوكيات الإجرامية، كذلك وافق معظم أفراد العينة على كل الدوافع الاجتماعية كأحد الأسباب المؤدية للإرهاب الإلكتروني والطريق الإجرامي بشكل عام (كما هو موضح بالشكل رقم ١٥).
- **الدوافع السياسية:** أيضاً، كانت لدى أفراد عينة البحث شبه اتفاق على أهمية الدوافع السياسية كأحد الأسباب المؤدية للعنف بصورة عامة والإرهاب الإلكتروني بصورة خاصة، وجاءت في مقدمة الدوافع السياسية (عدم المساواة وغياب الحكم العادل، التراخي في تطبيق القانون، والظلم والضطهاد التي تنتهجها بعض الدول، التهميش، عدم الاستقرار السياسي، حرية الرأي) لذلك هناك ضرورة للوصول لحول سياسية للأزمات الداخلية، وإدماج كافة

التيارات في الحياة الاجتماعية والسياسية وعدم تهميشهم، تجنباً للعنف والانتقام، ووصولاً للاستقرار المجتمعي.

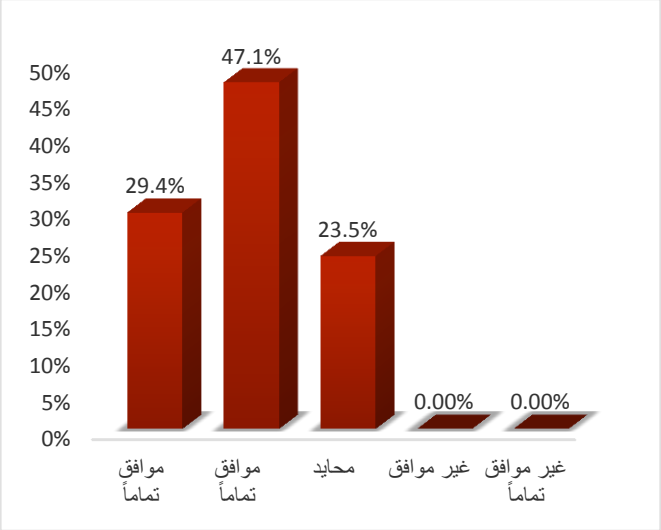
- **الدوافع الفكرية:** تحولت شبكة الإنترنت ومواقع التواصل الاجتماعي من مجرد فضاء سيبراني للتعارف والدردشة إلى مساحة لتبادل الأفكار والنقاشات في الآراء السياسية والاقتصادية والدينية، من هنا كان للدوافع الفكرية دوراً هاماً في تحديد اتجاهات الأفراد وممارساتهم على شبكة الإنترنت، حيث جاءت موافقة العينة على فئة (التشدد والتعصب في نشر الأفكار) في مقدمة الدوافع الفكرية بنسبة (٢٣.٣% موافق جداً، و نسبة ٤٧% موافق جداً) ثم فئة (الفهم الخاطئ للأديان) بنسبة (٤٧% موافق جداً ونسبة ٢٩.٥%)، وبالتأكيد لابد من مواجهة تلك الدوافع الفكرية من خلال زيادة الدور التوعوي الذي يلعبه الأزهر في فهم الدين والعمل على تطوير أساليبهم الدعوية ومواكبة التطور، فللأزهر الشريف والمجتمع المدني أيضاً دوراً مهماً في تعديل تلك الأفكار والسيطرة عليها دعوياً.
- **الدوافع الاقتصادية:** كان التوسع في الاعتماد على وسائل تقنية المعلومات الدور الأكبر في تغيير شكل الحياة، خاصةً الاقتصادية منها حيث أصبح الحاسب الآلي أحد مقومات المؤسسات المالية، لذلك كانت الدوافع الاقتصادية من الدوافع الهامة في اتجاه السلوك الإرهابي في الفضاء السيبراني، حيث جاءت فئة (ضعف وسائل الحماية لنظم المعلومات) في المرتبة الأولى باتفاق كل أفراد العينة بنسبة ٤٧% موافق جداً، ونسبة ٤٧% موافق أي بنسبة تأكيد تصل ل ٩٥% على أن الإرهابيين يعملون على استغلال الثغرات في جدران الحماية لاختراق أهدافهم والسيطرة عليها.
- **الدوافع الشخصية:** طبقاً لاختيارات أفراد العينة، جاءت فئة (حب الشهرة ولفت الانتباه والرغبة في الظهور) في المرتبة الأولى من الدوافع الشخصة التي تدفع صاحبها لسلك طريق الإجرام وذلك بنسبة (٥٩%) موافق جداً و (١٨%) موافق، بينما جاءت في الاختيار الثاني فئة (عدم الشعور بالانتماء للوطن) بنسبة (٤٧%) موافق جداً ونسبة (٣٥%) موافق، وتنوعت إجابات أفراد العينة في فئة (الفشل في تحقيق الأهداف) بنسبة (٣٥% موافق جداً، ١٨% موافق، ٢٩.٥% محايد، ٥.٩% غير موافق، ٥.٩% غير موافق جداً، أما فئة (الإحباط) كأحد الدوافع الشخصية التي تؤدي بصاحبها إلى الإرهاب فجاءت بنسبة (١١.٨% موافق جداً، ٣٥% موافق، ٤١% محايد، ٠% غير موافق، ٥.٩% غير موافق جداً).

جدول رقم (١٥)


ما مدى موافقتك على الأسباب والدوافع التالية لظاهرة الإرهاب الإلكتروني:
عدم الشعور بالانتماء للوطن
حب الشهرة ولفت الانتباه والرغبة في الظهور (دوافع شخصية)
الفشل في تحقيق الأهداف (دوافع شخصية)
الإحباط (دوافع شخصة)
سهولة نقل الأموال عبر المصارف الإلكترونية (دوافع اقتصادية)
ضعف وسائل الحماية لنظم المعلومات (دوافع اقتصادية)
تفاقم المشكلات والأزمات الاقتصادية الدولية أو المحلية (دوافع اقتصادية)
التشدد والتعصب في نشر الأفكار (دوافع فكرية)
الفهم الخاطئ للأديان (دوافع فكرية)
التراخي في تطبيق القانون وعدم العدالة في تطبيقة (دوافع سياسية)
حرية الرأي، حيث عدم الشعور بكرامتهم وحقوقهم وحريتهم وعدم منحهم فرص للتعبير (دوافع سياسية)
عدم الاستقرار السياسي (دوافع سياسية)
التهميش وانتهاك الحقوق (دوافع سياسية)
الظلم والضطهاد والسياسات غير العادلة التي تتخذها بعض الدول تجاه مواطنيها (دوافع سياسية)
عدم المساواه والاستيلاء على الأموال العامةوغياب الحكم العادل (دوافع سياسية)
ضعف الدور الرئيسي التي تلعبه الأسرة في حماية أفرادها (دوافع اجتماعية)
الفقر، حيث يعد أرضاً خصبة تعمل الجماعات على زرع بذور التطرف فيها. (دوافع اجتماعية)
البطالة (دوافع اجتماعية)
ضعف المنظومة التعليمية (دوافع اجتماعية)
التفكك الأسري (دوافع اجتماعية)
موافق جداً
موافق
محايد
غير موافق
غير موافق جداً

١٧) هل تعتقد أن قانون الجريمة الإلكترونية الصادر في عام ٢٠١٨، أثر على حرية الرأي والتعبير عبر الإنترنت وأدى لتدخل الدولة كإجراء نوعي للضبط الاجتماعي وبين إقامة الإنترنت كخدمة؟

جدول رقم (١٦)



المتغير	العدد	النسبة %
موافق تماماً	٢٠	%٢٩.٤
موافق	٣٢	%٤٧.١
محايد	١٦	%٢٣.٥
غير موافق	٠	%٠
غير موافق تماماً	٠	%٠
المجموع	٦٨	%١٠٠

أظهر الجدول رقم (١٦) تخوف أفراد العينة من القانون الجديد للجريمة الإلكترونية في كبح الحريات على شبكة الإنترنت وتقييد حركة الأفراد في ممارسة حرياتهم على شبكة الإرنت وخاصةً في مواقع التواصل الاجتماعي، حيث جاءت فئة (موافق) في المرتبة الأولى بنسبة (٤٧.١%) ثم فئة (موافق جداً) بنسبة (٢٩.٤%) وهاتين النسبتين يمثلان (٧٦.٥%) من حجم العينة، بينما جائت فئة (محايد) بنسبة (٢٣.٥%) وباقي الفئتان (غير موافق) و (غير موافق تماماً) بنسبة (٠%) أي أنه لا أحد في العينة رفض وعارض أن القانون لن يكون عائقاً أمام حرية التعبير وهو ما يؤكد التخوف الكبير من استخدام الدولة للقانون في قمع حرية التعبير على شبكة ا لإنترنت.

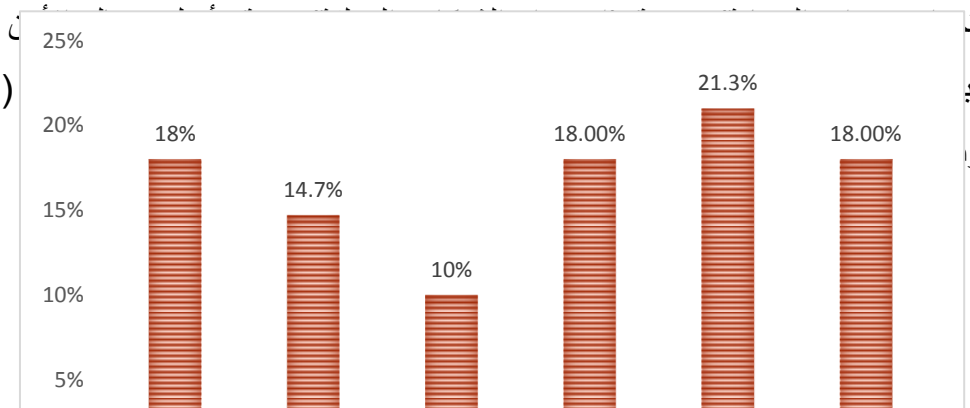
وهذا ما أكده التقرير الصادر من المم المتحدة (كما أن احترام حقوق الإنسان وسيادة القانون جزء لا يتجزأ من مكافحة الإرهاب. ويشار بالأخص إلى أن الدول الأعضاء قد أكدت هذه الالتزامات في استراتيجية الأمم المتحدة العالمية لمكافحة الإرهاب وأقرت فيها بأن "اتخاذ تدابير فعَّالة لمكافحة الإرهاب وحماية حقوق الإنسان هدفان لا يتعارضان بل متكاملان ويعزز كل منهما ا لآخر"[56].

المتغير	العدد	النسبة %
استخدام جدران الحماية	٤٤	%١٨
معالجة مشكلات الفقر والبطالة	٣٦	%١٤.٧
الاهتمام بالتربية الأسرية	٢٤	%١٠
استخدام الشبكات المغلقة حيث أكثر أماناً	٤٤	%١٨
وضع تشريعات جديدة توائم التقدم التقني وتستطيع مواجهة جرائم تقنية المعلومات	٥٢	%٢١.٣
العمل على تأهيل رجال الأمن ورجال الضبط القضائي من خلال دورات متخصصة بجرائم الإرهاب المعلوماتي	٤٤	%١٨
المجموع	٢٤٤	%١٠٠

١٨) <u>في رأيك، ما هي أكثر الإجراءات فعالية في مواجهة الإرهاب الإلكتروني؟</u>

جدول رقم (١٧)

يتضح من الجدول رقم (١٧) أن فئة (وضع تشريعات جديدة توائم التقدم التقني) جاءت كأول اختيار لعينة البحث في إجراءات التصدي للإرهاب الإلكتروني بنسبة (٢١.٣%)، ثم جاءت فئة (استـ ورجال الضبـ (الاهتمام بالتر



خاتمة:

حللت الدراسة كيف يؤثر الإرهاب الإلكتروني على الأمن القومي سواء المصري أو الإقليمي والعالمي، حيث وجدت هذه الدراسة أن الهجمات الإلكترونية في مصر أصبحت في زيادة وأصبحت أكثر خطورة من ذي قبل على الأمن القومي، والتي ارتبطت هذه الزيادة في الهجمات بالتوسع في استخدام الكمبيوتر ونظم المعلومات في كافة القطاعات ومختلف قطاعات الاقتصاد، وخاصة انتشار التهديدات التي يشكلها الإرهاب الإلكتروني على المجتمع ككل مع انتشار استخدام الإنترنت في كافة القطاعات والتي شجعت المنظمات الإرهابية على لاستغلال الفرص المتاحة واختراقها ونشر أفكارها من خلال مواقع خاصة بها على شبكة الإنترنت تبث من خلالها أفكار وثقافات خبيثة وتقوم بتجنيد ضعاف النفوس واصحاب الأهداف والدوافع الشيطانية، واستخدامها كمنصة اتصال لتسهيل الاتصالات بين الأعضاء ونشر مواد الدعاية الخاصة بها وإرسال المعلومات واستقبالها، كذلك الدعم المادي للأعمال الإرهابية المخطط القيام بها.

من هنا، فإن هذه الظاهرة التي تواجه المجتمعات تُعَد واحدة من أهم التحديات التي تواجه الدول والحكومات والسلطات الجنائية، ليس فقط بسبب المعرفة الفنية والتقنية المحدودة المطلوبة لممارسة التحقيق في مثل هذه الجرائم ولكن أيضاً للإطار القانوني غير المتجانس الذي يربط الدول بعضها ببعض في موضوع تبادل الأدلة الإلكترونية، فعلى الرغم من الاتفاقيات المتعددة وعلى رأسها اتفاقية بودابست الخاصة بالجرائم الإلكترونية والتي وفرت أدوات المساعدة القانونية والإجرائية الدولية في كافة الأمور المتعلقة بالتحقيقات والمقاضاة في الجرائم المتعلقة بالإرهاب الإلكتروني.

النتائج:

إجابة السؤال الأول: ما مفهوم الإرهاب الإلكتروني:

- اتضح من الدراسة الميدانية أن معظم أفراد العينة أكدوا على أن الإرهاب الإلكتروني هو الاستخدام السيئ لشبكة الإنترنت لإحداث ضرر كبيرفي المجتمع ونشر الخوف والرعب والإخلال بالأمن العام وتدمير البنية التحيتية للبلد المستهدف.
- أكدت الدراسة على وجوب العمل على وضع تعريف شامل للإرهاب يتم التفريق من خلاله بين المقاومة المشروعة والدفاع عن النفس والمال وبين العمل الإرهابي.

إجابة السؤال الثاني: ما أهم مظاهر وأشكال الإرهاب الإلكتروني؟

- أكدت عينة الدراسة على تنوع الأهداف التي يرصدها الإرهاب الإلكتروني وأشكاله، والتي من الممكن أن تحقق أكبر الخسائر، حيث تنوعت تلك الأهداف بين (تدمير البنية التحتية بنسبة ١٨.٤%، واختراق قواعد البيانات وتدميرها أو تخريبها بنسبة ١٦.٣%، وإثارة الذعر وتعريض حياة الناس للخطر بنسبة ١٤.٣%، والتأثير السلبي على القطاع الخاص والاقتصاد بنسبة ١٤.٣%، والتدخل في الشئون الداخلية للدول بنسبة ١٢.٢%.
- اتضح من الدراسة أن معظم أفراد العينة لا يعتبرون الإرهاب الإلكتروني ظاهرة خطيرة في الوقت الحالي ولا تُشكل مصدراً للقلق تجاههم، حيث من خلال الجدول رقم (١٢) نجد أن إجابات المبحوثين جاءت (لست خائفاً جداً ولست خائفاً بنسبة ٤١.١%) بينما فئة (محايد بنسبة ٣٥.٣%) أي أن أكثر من ثُلُثَي العينة لا يخافون من أضرار الإرهاب الإلكتروني وهذا يدل على كونه ظاهرة تُركز على توجيه الضرر للمجتمع ككل والتأثير بالضرر على

المجتمع بصورة عشوائية بخلاف الجرائم الإلكترونية التي يُضَار فيها الشخص الواحد أو مجموعة من الأشخاص بصورة فردية.

إجابة السؤال الثالث: ما أهم طرق مواجهة ظاهرة الإرهاب الإلكتروني على المستوى الدولي كذلك على مستوى الهيئات والمنظمات؟

- أكدت الدراسة ضرروة أن تقوم الحكومات بدعم شركات تكنولوجيا المعلومات الكبيرة حتى تكون قادرةعلى مواجهة الإرهابيين على التجنيد والعمل عبر الإنترنت، والذي يعطي الشركات المتوسطة والناشئة أيضاً القدرة على الانضمام للمعركة ضد الإرهاب في المستقبل.
- يجب على الحكومات القيام بحماية أنظمتها الإلكترونية من تلك التهديدات من خلال (استخدام جدران الحماية – وبرامج مكافحة الفيروسات – وسن التشريعات) كما جاء في استجابات المبحوثين في الجدول رقم (١٧) من ضرورة تأمين البنية التحتية المعلوماتية.
- سن التشريعات والقوانين التي تسد الثغرات المستغلة في ارتكاب الإرهاب الإلكتروني بصفة خاصة والجرائم الإلكترونية بصفة عامة، ولكن مع ضمان حرية التعبير على شبكة الإنترنت وألا تؤثر التدابير والقوانين المنظمة لخدمة الإنترنت على حقوق الإنسان وهذا ما أكدته عينة البحث في السؤال رقم ١٧، حيث أكد ما يقارب من ٧٧% من العينة على التداخل بين سن القوانين الخاصة بالجرائم الإلكترونية وبين حقوق الإنسان وحريته أثناء التواجد على شبكة الإنترنت وخاصة مواقع التواصل الاجتماعي.
- أكدت الدراسة على أهمية التعاون الدولي بين الدول ومراقبة كافة التحركات الإرهابية ومراقبة الأفعال الإرهابية التي تقع على أراضيها وتسهيل تبادل الأدلة الإلكترونية.

إجابة السؤال الرابع: ما رؤية أفراد عينة الدراسة لدور الأبعاد الاجتماعية في مواجهة الإرهاب الإلكتروني؟

- تفعيل دور المؤسسات (الجامعة – المسجد- وسائل الإعلام...) والتحذير من خطورة تلك الأفكار الإرهابية على الأسرة والمجتمع.
- أظهرت النتائج الحاجة إلى الاهتمام بدور التعليم والمدرسة على وجه الخصوص، من خلال وضع مادة الأمن المعلوماتي أو أمن الكمبيوتر كمادة تدريس في الصفوف الدراسية الأساسية والتي من شأنها وضع مفاهيم واضحة لتلك الأفعال الإرهابية وتعريف مفهوماتها للطلاب من أجل التوعية والفهم، وهذا ما أكدته أيضاً دراسة (زينة ياوز، التجنيد الإلكتروني للأطفال) في ضرورة استحداث مادة جديدة في المدارس للتعريف بمخاطر الإرهاب وأساليبه في التوغل عبر شبكة الإنترنت ونشر روح التسامح والمودة[57].
-

-

يجب مراعاة الأبعاد الاجتماعية والتي لها أثر كبير في اتخاذ العديد من الشباب قرارا بالانضمام إلى تلك الجماعات الإرهابية، حيث يجب معالجة تلك المشكلات مثل التفكك الأسري وتحسين منظومة التعليم والحد من البطالة، والاهتمام بدور الأسرة المهم في غرس القيم والأخلاقيات الإيجابية داخل أفرادها.

التوصيات:

- تعزيز التعاون بين الدولة بمؤسساتها (الأمنية – الرسمية) وبين منظمات المجتمع المدني للتصدي لظاهرة الإرهاب بشكل عام والإرهاب الإلكتروني بشكل خاص.
- تشجيع البحث العلمي في مواجهة الظواهر الإرهابية والكشف عن عواملها وأسبابها ودوافعها وكيفية مواجهتها.
- ضرورة تطوير المناهج التعليمية في المدارس والجامعات وإدخال مواد جديدة تختص بتغطية واسعة لمفهوم أمن الكمبيوتر والأمن السيبراني، وأن تكون السياسات التعليمية متماشية مع سياسة الدولة في مواجهة الإرهاب والتطرف خاصة عبر شبكة الإنترنت، ومساعدة الطلاب في فهم التهديدات والتقنيات والأهداف المحتملة لأي تهديد إرهابي إلكتروني.

المراجع:

(١) هشام التميمي، كفاح حيدر فليح، الاستمالة العاطفية في الصحف الإلكترونية، مجلة الباحث الإعلامي، مجلد ١١، العدد ٤٤،، ٢٠١٩ ص ٢١٧: https://abaa.uobaghdad.edu.iq/index.php/abaa/article/view/281

(٢) عماد الدين سلطان ، مختصر الدراسات الأمنية ، الجزء الأول ، المركز العربي للدراسات المنية والتدريب ، الرياض ، 1986 ، ص 113 .

(٣) صلاح الدين محمد منسي ، دراسات في السلوك الإجرامي ، مكتبة كلية الآداب ، جامعة الزقازيق ، 1987 ، ص ص 67 – 68 .

(٤) حلمي خضر ساري، تأثير الاتصال عبر الإنترنت في العلاقات الاجتماعية (دراسة ميدانية في المجتمع القطري)، مجلة جامعة دمشق، المجلد ٢٤، العدد الأول+الثاني، ٢٠٠٨، ص ٣٠٩.

(٥) ساري، حلمي خضر، تأثير الاتصال عبر الإنترنت في العلاقات الاجتماعية "دراسة ميدانية في المجتمع القطري"، مجلة دمشق، مج ٢٤، ع ١،٢، ٢٠٠٨، ص ص ٣٠٦-٣٠٧.

(٦) الكويتية، وكالة الأنباء الكويتية، الجامعة العربية تؤكد الأبعاد الاجتماعية في مكافحة الإرهاب، ٢٤ أكتوبر، ٢٠١٧: https://www.kuna.net.kw/ArticleDetails.aspx?id=2652241&language=ar

(٧) أحمد ناصر أبو السعود، الإرهاب الإلكتروني، الموسوعة السياسية: https://political-encyclopedia.org/dictionary

(٨) مركز البيانات للدراسات والتخطيط، الإرهاب الإلكتروني أسبابه وطرق العالج، ٣٠ سبتمبر، ٢٠١٩: https://www.bayancenter.org/2019/09/5458/

(٩) استخدام الإنترنت في أغراض إرهابية، مكتب الأمم المتحدة المعني بالمخدرات والجريمة UNODC، الأمم المتحدة، نيويورك، ٢٠١٣، ص ص ١١-١٢:

https://www.unodc.org/documents/terrorism/Publications/The_Use_of_Internet_for_Terrorist_Purposes/Use_of_the_Internet_for_Terrorist_Purposes_Arabic.pdf

(10) Cyberterrorism, The Doha declaration: PROMOTING A CULTURE OF LAWFULNESS, UNODC, 29 MAY, 2021:

https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberterrorism.html

(١١) بيتر سنجر، الإرهاب الإلكتروني: خرافات، وحقائق، وفيروس ستوكسنت، وتنظيم داعش، ووسائل الإعلام الاجتماعي، ومسرح المواجهة، مركز الإمارات للدراسات والبحوث الاستراتيجية، الطبعة الأولى، ٢٠١٨، ص٣.

(١٢) Vladimir Golubev, Cyber-crimes - Analytical data compiled, Source: Computer Crime Research Center, January 03, 2008:

http://www.crime-research.org/analytics/cyber_crimes0108.

(13) Shamsuddin Abdul Jalil, Countering Cyber Terrorism Effectively :Are We Ready To Rumble؟, GIAC Security Essentials Certification (GSEC), Practical Assignment, Version 1.4b, Option 1, June 2003, p.4.

(١٤) أحمد حسن موكلي، دور الإنترنت في تجنيد الخلايا الإرهابية، ورقة بحث مقدمة في مؤتمر تقنية المعلومات والأمن الوطني ١-٤/ديسمبر/٢٠٠٧م.

(١٥) توفيق مجاهد، طاهر عباسة، جريمة الإرهاب الإلكتروني في ضوء أحكتم الاتفاقات العربية لمكافحة تقنية المعلومات لعام ٢٠١٠، مجلة العلوم القانونية والسياسية، المجلد ٠٩، العدد ٠٣، ديسمبر ٢٠١٨، ص ٨٢.

(١٦) الاتفاقية العربية لمكافحة جرائم تقنية المعلومات/ الأمانة العامة لجامعة الدول العربية، إدارة الشئون القانونية، الشبكة القانونية العربية، ص ٤: http://www.moj.gov.jo/EchoBusV3.0/SystemAssets/

(١٧)Laura Mayer Lux, Defining cyberterrorism, Rev. chil. derecho tecnol. vol.7 no.2 Santiago dic., 2018: https://scielo.conicyt.cl/scielo.

(١٨) يوسف بن أحمد الرميح، الإرهاب والإعلام الجديد..(الإرهاب الرقمي)، موقع جريدة الجزيرة الإلكتروني، العدد ١٥٥٠٠، السبت ٧ مارس، ٢٠١٥:

https://www.al-jazirah.com/2015/20150307/ar1.htm

(١٩) توفيق شريخي، فاطمة حشاني، الإرهاب الإلكتروني وتأثيره على أمن الدولة، رسالة ماجستير، قسم العلوم السياسية، كلية الحقوق والعلوم السياسية، جامعة محمد بوضياف، الجزائر، ٢٠١٨، ص ٣٥.

(٢٠)Jian Hua, Sanjay Bapna, The economic impact of cyber terrorism, Journal of Strategic Information Systems, (٢٠١٢)، http //:dx.doi.org/10.1016/j.jsis.2012.10.004.

(٢١)Jian Hua, Sanjay Bapna, The economic impact of cyber terrorism. The Journal of Strategic Information Systems, Volume 22, Issue 2 ،June 2013, Pages 175-186

(٢٢) ياسمين أحمد صالح، الإرهاب الإلكتروني في ظل أزمة فيروس كورونا.. الأنماط والتداعيات، مجلة كلية السياسة والاقتصاد، العدد التاسع، يناير، ٢٠٢١، ص ٦٨.

[٢٣] ستيفن بالكويل، كريستيان ألكسندر، اتجاهات الإرهاب العالمي: نزوع المتطرفين إلى التكيف والتطور، ترينذز للبحوث والاستشارات. https://trendsresearch.org/ar/insight/

[٢٤] بيتر سنجر، مرجع سابق، ص ٦.

[٢٥] محمود الرشيدي، المواقع الإلكترونية الإرهابية والإباحية، مركز المعلومات ودعم اتخاذ القرار، ٢٠ أبريل، ٢٠٢٠: https://www.idsc.gov.eg/IDSC/DocumentLibrary/View.aspx?id=4119

[٢٦] هشام بشير، الإرهاب الإلكتروني في ظل ثورة المعلومات، مركز الخليج للأبحاث، العدد ٩٢، الثلاثاء، ٠١ مايو، ٢٠١٢: https://araa.sa/index.php?option=com_content&view=article&id=244:2014-06-13-16-21-31&catid=132:articles&Itemid=294

[٢٧] أحمدي بوجلطية بوعلي، الإرهاب الالكتروني وطرق مواجهته على المستوى العربي دراسة للتجربتين السعودية والقطرية، قسم العلوم الاقتصادية والقانونية، الأكاديمية للدراسات الاجتماعية والإنسانية، العدد ٨، رقم ٢، ٢٠١٦، ص ١٨٠.

[٢٨] ستيفن بالكويل، كريستيان ألكسندر، مرجع سابق.

(٢٩)Hetram yaday, shashant gour, "Cyber Attacks: An impact on Economy to an organization, International Journal of Information & Computation Technology., ISSN 0974-2239 Volume 4, Number 9 (2014), pp. 939.

[30] ليتم فتيحة، ليتم نادية، الأمن المعلوماتي للحكومة الإلكترونية وإرهاب القرصنة، مجلة الفكر، العدد الثاني عشر، ٢٠١٥، ص ٢٣٨: https://platform.almanhal.com/details/article/79779#

[31] الأمن السيبراني. الحكومة الإلكترونية. الخدمات الحكومية الرقمية، المركز الأوروبي لدراسات مكافحة الإرهاب والإستخبارات ECCI، إعداد وحدة الدراسات والتقارير، ٢٣ أكتوبر، ٢٠٢٠: https://www.europarabct.com/?p=72350

[32] ميشيل كونينكس، دور الأمم المتحدة في الرد على التهديد الإرهابي العالمي، معهد واشنطن لدراسات الشرق الأوسط، ١٧ يوليو، ٢٠٢٠: https://www.washingtoninstitute.org/ar/policy-analysis/dwr-alamm-almthdt-fy-alrd-ly-althdyd-alarhaby-alalmy

[33] نجاري بن حاج، الآليات القانونية لمكافحة الإرهاب الإلكتروني، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة مولود معمري، الجزائر، ٢٠١٦، ص ٤٢: https://dl.ummto.dz/handle/ummto/1126

[34] محمد عبد القادر، ظاهرة الجهاد الإلكتروني، جريدة المجلة الإلكترونية، الثلاثاء، ١٩ يناير، ٢٠٢١: (https://arb.majalla.com/

[35] فادي الدحدوح، الإرهاب الإلكتروني في سياق مجزرة نيوزيلندا، موقع الجزيرة الإلكتروني، ٢٣ سبتمبر، ٢٠١٩: https://www.aljazeera.net

[36] محمد الدحدوح، الإرهاب الإلكتروني في سياق مجزرة نيوزيلندا، جريدة الميادين الإلكترونية، ٢٧ سبتمبر، ٢٠١٩: https://www.almayadeen.net

(37) هايدي صبري، فرنسا تستضيف قمة عالمية لمكافحة الإرهاب الإلكتروني، جريدة العين الإلكترونية، أبو ظبي، الثلاثاء، ١٤ مايو، ٢٠١٩: https://al-ain.com/article/macron-newsland-terrorism

(38) Jobin Sebastian, P.Sakthivel, Cyber terrorism: A potential threat to global security, peareon journal of social sciences&humanities, volume 6, issue 6, 2020, p339: http://www.pearsonjournal.com/

(39) ناصر العلي، الجهود المبذولة في مكافحة الإرهاب الإلكتروني، مجلة الباحث للدراسات الأكاديمية، المجلد ٨، العدد ١، ٢٠٢١، ص ٣٥.

(40) United Nations, Cybersecurity Challenge: https://ideas.unite.un.org/counterdigiterrorism/Page/Home

(41) أمن الفضاء، مكتب مكافحة الإرهاب، الأمم المتحدة (UN Counter-Terrorism Centre (UNCCT)): https://www.un.org/counterterrorism/ar/cct/programme-projects/cybersecurity

(42) https://www.un.org/counterterrorism/ar/cct/programme-projects/cybersecurity.

(43) ناصر العلي، الجهود المبذولة في مكافحة الإرهاب الإلكتروني، مجلة الباحث للدراسات الأكاديمية، المجلد ٨، العدد ١، يونيو، يناير ٢٠٢١، ص ٣٨.

(44) قرار مجلس الأمن رقم ٢٣٧٠، الأمم المتحدة، مجلس الأمن، ٢ أغسطس، ٢٠١٧: https://undocs.org/ar/S/RES/2370(٢٠١٧)

(45) جبار حسين، زينب كاطع، الإرهاب الإلكتروني أسبابه وطرق العلاج، سلسلة إصدارات مركز البيان للدراسات والتخطيط، ٣٠ سبتمبر، ٢٠١٩: https://www.bayancenter.org/2019/09/5458/

(46) رانيا سليمان وأخرون، سياسات مكافحة الإرهاب الإلكتروني .. مصر والسعودية نموذجاً، المركز العربي للبحوث والدراسات، الأحد، ٢ فبراير، ٢٠٢٠: http://www.acrseg.org/41483

(47) السيسي وغوتيريس يتفقان على مكافحة الإرهاب الإلكتروني، موقع جريدة العربية الإلكتروني، ٣ أبريل، ٢٠١٩: https://www.alarabiya.net/arab-and-world/egypt/2019/

(48) مني فتحي أحمد عبد الكريم، الجريمة عبر الشبكة الدولية للمعلومات، مرجع سابق، ص 309.

(49) الإدارة العامة للمعلومات والتوثيق، إدارة مكافحة جرائم الحاسبات وشبكة المعلومات، وزارة الداخلية، الموقع الإلكتروني: http://citizen-service.moiegypt.gov.eg/crimes_web/main.htm

(50) قانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية، العدد ٣٢ مكرر (ج)، ١٤ أغسطس، ٢٠١٨.

(51) Prichard, J.J & .MacDonald, L.E. (2004). Cyber Terrorism: A Study of the Extent of Coverage in Computer Science Textbooks .*Journal of Information Technology Education: Research, 3* .٢٨٩-٢٧٩ ،(١)Informing Science Institute .Retrieved May 25, 2021 from https://www.learntechlib.org/p/111454/.

(52) Adam Hayes, phishing, Investopedia, 18 may, 2021: https://www.investopedia.com/terms/p/phishing.asp

(53) فريدة بن عمروش، الإرهاب الإلكتروني: دراسة في إشكالات المفهوم والأبعاد، المجلة الجزائرية للعلوم الاجتماعية والإنسانية، المجلد ٠٨ـ العدد ٠٢، ٢٠٢٠، ص ص ٢٢٢-٢٢٣.

(54) أسماء الجيوشي مختار، دور استخدام التنظيمات الإرهابية لمواقع التواصل الاجتماعي في اقتناع الأفراد بأفكارها، ندوة دور مؤسسات المجتمع المدني في التصدي للإرهاب، المجلة العربية للدراسات الأمنية والتدريب، المجلد ٣٠، العدد ٦٠، الرياض، ٢٠١٤، ص ١١٣.

(55) مجيد كامل حمزة، الإعلام الرقمي الإلكتروني للإرهاب وسبل المواجهة إعلامياً، المجلة السياسية والدولية، كلية الفنون الجميلة، جامعة بغداد، العدد ٣٥-٣٦، ٢٠١٧، ص ٨٨.

(56) مكتب الأمم المتحدة المعني بالمخدرات والجريمة، استخدام الإنترنت في أغراض إرهابية، الأمم المتحدة، نيويورك، ٢٠١٣، ص ١٣٣:

https://www.unodc.org/documents/terrorism/Publications/The_Use_of_Internet_for_Terrorist_Purposes/Use_of_the_Internet_for_Terrorist_Purposes_Arabic.pdf

(57) زينة ياوز آوجي، غالب خزعل محمد، التجنيد الإلكتروني للأطفال في الأعمال الإرهابية، مجلة كلية التربية الأساسية، الجامعة المستنصرية، المجلد ٢٤، العدد ١٠٢، ٢٠١٨.

The social dimensions of cyber terrorism

A field study

Dr. Mohamed Mahmoud Ahmed Al ramady

Abstract:

The technological and information development that the world is witnessing has led to the emergence of a new form of terrorism called (electronic terrorism), which has become a major threat to the national security of countries, but its impact has extended to threatening international peace and security. There is no doubt that digital transformation and the expansion in the use of technology Digital in most sectors and institutions, and even the reliance of countries on this technology in managing their infrastructure through the computer and its connection to the international information network, which had many positives However, the reliance on this technology in many sectors has made it a target for terrorist attacks and has become vulnerable to security risks and cyber attacks. Infrastructure, military and economic facilities and even political actors are threatened by terrorist attacks through this technology, which has led to the exposure of many innocent people to death. In addition to material losses and negatively affecting the morale of citizens within their communities. Egypt has sensed the seriousness of this phenomenon, especially with the expansion of the use of information technology and linking it to the Internet in all economic and military institutions and infrastructure, so Egypt proceeded to

expand international cooperation to prevent the use and exploitation of terrorism for technological development and to set a framework to combat the spread of the phenomenon of terrorism and extremist thought. Focusing on the social dimensions, which have an important role in limiting the phenomenon of electronic terrorism and trying to identify the manifestations of this phenomenon and its forms and the most important ways to confront it, as well as identifying forms of international and regional cooperation in confronting the phenomenon of electronic terrorism.

Key words: cyber terrorism; cyber crime; social dimensions.