معهد فلسطين لأبحاث الأمن القومي

دراسات أمنية

الإرهاب الرقمي

إعداد: د.أسامة خالد

باحث في الدراسات الإستراتيجية والأمنية

وحدة التطرف والأمن الفكري

يناير/2024

معهد فلسطين لأبحاث الأمن القومي

المحتويات

الملخص:

في هذه الدراسة يشير الباحث إلى خطورة استثمار الجماعات الإرهابية للتطور التكنولوجي والإعلام الرقمي بما يخدم مصالحها واستراتيجياتها وهو ما قد يشكل تهديدا مباشرا على مستوى الدولة أو المجتمع أو الفرد. وتحدث الباحث حول ماهية الإرهاب الرقمي كمصطلح حديث في الدراسات الأمنية لكونه مرتبط بالتقدم التكنولوجي الحديث " تكنولوجيا الإرهاب" ومقدرة الجماعات الإرهابية على التكيف مع هذا التطور بواقع استراتيجيات مختلفة تساهم في استمرار نشاطها وديمومة تحريضها الذي يعتبر تهديدا عابرا للحدود والزمان. وكشف الباحث عن الأساليب والخصائص المتعلقة بالإرهاب الرقمي من عدة جوانب وصولا إلى استخدام التطبيقات المشفرة والتي تشكل ملاذاً آمناً لها من ملاحقات الأجهزة الأمنية وتتبعها والحد من خطورتها.

توصل الباحث إلى مجموعة من الاستنتاجات أكدت على أن "الإرهاب الرقمي" يعتبر شكل حديث من أشكال الإرهاب ومصدر تهديد مباشر قد يكون خفي في معظم الحالات، كما ختم الباحث بتوصيات أهمها ضرورة توحيد الجهود بين أجهزة الدولة المختلفة لتبيان ومواجهة خطورة الإرهاب الرقمي.

الكلمات المفتاحية:

الإرهاب، الإرهاب الرقمي، تكنولوجيا الإرهاب، الانترنت المظلم، تهديد عابر الحدود، الجريمة الالكترونية، التعاون الأمني.

keywords: Terrorism, digital terrorism, terrorist technology, dark web, cross-border threat, security cooperation.

المقدمة:

لا يختلف أحد على أهمية الثورة التكنولوجية الرقمية التي شهدها القرن الحادي والعشرين في خدمة البشرية والنهوض بأداء مجتمعي يساهم بتلبية الاحتياجات المناطه في دول العالم، والعمل على استثمار هذا التقدم في المجال المعلوماتي السياسي والاقتصادي والاجتماعي والأمني بما يخدم الفرد والمجتمع والحكومات والدول على حد سواء.

وبالرغم من هذا التطور التكنولوجي والذي تحول مما يسمى بالإعلام التقليدي إلى الإعلام الرقمي أو الثورة الرقمية إلا انه قد واجه العديد من التحديات بالنسبة إلى المجتمعات والدول في التكيف معه ومواكبة تطور التكنولوجيا الحديثة في إحداث وصنع أنماط جديدة من المضامين والمفاهيم العامة، وأصبح العالم كله قرية صغيرة يتشارك في هذا التطور وحيثياته والتفاعل معه.

يمكن الإشارة إلى أن هذا التطور والذي من شأنه أن يخلق بيئة ايجابية تخدم مصالح الأفراد والمجتمعات والدول، إلا أن هناك جانب مظلم منه أيضا موجود وقد تم استغلاله بالشكل السلبي، حيث نشير إلى مفهوم الجانب السلبي من خلال استغلال هذا التطور الرقمي من قبل الجماعات الإرهابية

موسوما بمفهوم "الإرهاب الرقمي"، حيث أنه أصبح يشكل خطرا وجوديا في الفضاء الرقمي من خلال استثمار هذه الجماعات للتحول الرقمي في خدمة أجنداتها ونشر أيديولوجياتها، بل وأكثر من ذلك بحيث حولت هذا العالم الافتراضي إلى ساحة حرب تقدم من خلالها نفسها في رسم السياسات، وتحديد الأهداف لكياناتها المختلفة.

أولا: مفاهيم عامة:

"الإرهاب":

الاتفاقية العربية لمكافحة الإرهاب" عرفت الإرهاب بأنه: "كل فعل من أفعال العنف أو التهديد به أياً كانت دوافعه أو أغراضه يقع تنفيذاً لمشروع إجرامي فردي أو جماعي ويهدف إلى إلقاء الرعب بين الناس أو ترويعهم بإيذائهم أو تعريض حياتهم أو حرياتهم أو أمنهم للخطر أو إلحاق الضرر بالبيئة أو بأحد المرافق أو الأملاك العامة أو الخاصة أو احتلالها أو الاستيلاء عليها أو تعريض الموارد الوطنية للخطر". [1]

كما عرفت الاتفاقية الدولية لمكافحة الإرهاب في جنيف عام 1937م الإرهاب بأنه "الأفعال الإجرامية الموجهة ضد إحدى الدول، والتي يكون هدفها أو من شأنها إثارة الفزع أو الرعب لدى شخصيات معينة أو جماعات من الناس أو لدى العامة".[2]

---

[1] - http://www.mokarabat.com

[2]- موقع السياسة الدولية ، دور المجتمع الدولي في مكافحة الإرهاب ،د.مفيد شهاب ،2015
https://www.siyassa.org.eg/News/5106.aspx

- **"الإرهاب الرقمي"**: والذي أصبح ظاهرة في ظل ثورة تكنولوجيا المعلومات واستخدامات الحواسب الآلية والإنترنت، وهو الأمر الذي دعا 30 دولة إلى التوقيع على "الاتفاقية الدولية الأولى لمكافحة الإجرام عبر الإنترنت"، في بودابست، عام 2001،"وتم تعريفه "بأنه هجمات غير مشروعة، أو تهديدات بهجمات ضد الحاسبات أو الشبكات أو المعلومات المخزنة إلكترونياً، توجه من أجل الانتقام أو ابتزاز أو إجبار أو التأثير في الحكومات أو الشعوب أو المجتمع الدولي بأسره لتحقيق أهداف سياسية أو دينية أو اجتماعية معينة".[3]

مركز حماية البنية التحتية القومية الأمريكية عرفه: الإرهاب الالكتروني هو 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 أو أيدلوجية.

يرى الباحث أن "الإرهاب الرقمي" هو كل عمل يقوم به فرد أو مؤسسة أو دولة باستخدام الفضاء الرقمي لإحداث ضرر معنوي أو مادي أو تحريض مباشر أو غير مباشر من شأنه أن يهدد سلامة الفرد أو المجتمع أو الدولة على حد سواء.

[3] - https://www.politics-dz.com

ثانيا: أسباب الإرهاب الرقمي وخصائصه وعوامل الانتشار

يتمثل السلوك الإرهابي المتعلق بالجانب الرقمي جملة من الخصائص وجملة من الأسباب الجوهرية والتي تندرج من قبل المبررات لممارسة العمل الإرهابي عبر الوسائل التقنية والمعلوماتية المتطورة التي أصبحت ظاهرة العصر الحالي، حيث يعتبر تأثيره المباشر على المجتمع وتخويفه وشل إرادة أفراده ونشر الذعر ومشاعر عدم الأمان عبر تكرار المعلومات حول تهديدات العنف والحفاظ على حالة من الخوف المستمر لأجل تحقيق أهداف سياسية أو أهداف أخرى (1) وسيتم تناول العناصر التالية:

1. أسباب الإرهاب الرقمي ودوافعه.
2. خصائص الإرهاب الرقمي وأهدافه.
3. عوامل انتشار الإرهاب الرقمي.

❖ **الأسباب العامة للإرهاب الرقمي:**

إن أسباب الإرهاب ودوافعه تختلف في درجة أهميتها حسب الاتجاهات السياسية والظروف الاقتصادية والأحوال الاجتماعية وكذلك الاختلاف الديني والعقائدي ويمكننا إيجاز أسباب ظاهرة الإرهاب فيما يأتي:

أولاً: الدوافع الشخصية للفرد

تتعدد الدوافع الفردية المؤدية للإرهاب، ويمكن بيان أبرزها في ما يلي:

1. افتقاد الشخص لأهمية دوره في الأسرة والمجتمع وفشله في الحياة الأسرية مما يؤدي إلى اكتساب بعض الصفات السيئة ومن ضمنها عدم الشعور بالانتماء والولاء للوطن.

(1)حسن، تركي عمير، الإرهاب الالكتروني ومخاطره في العصر الراهن، جامعة ديالي،ط،1.2016

2. الرغبة في الظهور وحب الشهرة بحيث لا يكون الشخص مؤهلا فيبحث عما يؤهله باطلاً فيشعر ولو بالعدوان والتخريب والتدمير.

3. نظرة الفرد السلبية للمجتمع الذي يعيش فيه نتيجة للظلم وإهدار الحقوق.

ثانياً: الدوافع الفكرية:

تتنوع الدوافع الفكرية المؤدية لظاهرة الإرهاب ويمكن بيان أهمها في ما يلي:

1. الجهل بمقاصد الشريعة الإسلامية المتمثل بالظن لا باليقين والتثبت، والفهم الخاطئ للدين، وتفسيره تفسير خاطئ، والجهل بقواعد الدين الحنيف وآدابه وسلوكه.

2. الانقسامات الفكرية المختلفة بين التيارات المتنوعة والمختلفة.

3. التطرف وهو أمر بالغ الخطورة في أي مجال من المجالات وخاصة المجالات الفكرية.

ثالثاً: الدوافع السياسية:

من أبرز الأسباب والدوافع السياسية لظاهرة الإرهاب ما يلي:

1.غياب العدالة الاجتماعية وعدم المساواة في توزيع الثروة الوطنية والتفاوت في توزيع الخدمات والمرافق العامة والتقصير في أمور الرعية.

2.معاناة بعض المجتمعات والشعوب الدولية من الظلم والاضطهاد والسيطرة الاستعمارية وسلب الأموال وخرق القوانين والمواثيق الدولية مما يدفع الشعوب إلى التشدد والتطرف.

رابعاً: الدوافع الاجتماعية:

1. التفكك الأسري الذي يؤدي إلى انتشار الأمراض النفسية والانحراف عن الطبيعة.
2. إهمال التربية الحسنة التي توجه الشخص بالتحلي بفضائل الأخلاق وتعزيز حب الأوطان في الوجدان وبيان ما هو صالح مما هو فاسد.

3. الفراغ، فإذا تمكن الفراغ من الشخص ولم يستغلّه فيما ينفعه ومجتمعه، أصبح داءً مهلكاً يغذي هذا العقل الخاوي بأفكار هدّامة فاسدة.

❖ **خصائص الإرهاب الرقمي:**

مما لا شك فيه أن الإرهاب الإلكتروني ينفرد بعدد من الخصائص التي يختص بها دون سواه، ويتميز بها عن غيره من الظواهر الإجرامية الأخرى، كما يسعى إلى تحقيق جملة من الأهداف والأغراض غير المشروعة.

يتميز الإرهاب الرقمي بعدة خصائص وسمات:

1.الإرهاب الرقمي لا يحتاج عند ارتكابه إلى العنف والقوة بل يتطلب حاسب آلي متصل بالشبكة المعلوماتية ومزود ببعض البرامج اللازمة. [1]

2.يتميز الإرهاب الرقمي بأنه جريمة إرهابية متعدية الحدود وعابرة للدول والقارات وغير خاضعة لنطاق إقليمي محدود.

3.صعوبة اكتشاف جرائم الإرهاب الرقمي ونقص الخبرة لدى بعض الأجهزة الأمنية والقضائية في التعامل مثل هذه الجرائم.

4.صعوبة الإثبات في الإرهاب الرقمي نظرا لسرعة غياب الدليل الرقمي وسهولة إتلافه وتدميره.

5.يتميز الإرهاب الرقمي بأنه يتم بتعاون أكثر من شخص على ارتكابه.

6.مرتكب جريمة الإرهاب الرقمي عادة يكون من ذوي الاختصاص في مجال تقنية المعلومات أو من شخص لديه على الأقل قدر من المعرفة والخبرة في التعامل مع الحاسب الآلي والشبكة المعلوماتية.

[1] - د.ألضيفي، ميثاق، بيات، الإرهاب الرقمي...هل بات الأكثر خطورة ؟2019

❖ **أهداف الإرهاب الرقمي:**

يهدف الإرهاب الرقمي إلى تحقيق جملة من الأهداف غير المشروعة ويمكننا بيان أبرز تلك الأهداف في ضوء النقاط الآتية:

1.مصالح ذاتية، إما مادية أو نفوذ (حكم) أو الاثنان معا.

2.مصالح أجنبية لتحقيق أجندة خارجية تستفيد منها الدول التي قد تستغل هذه الجماعات.

3.تحقيق أهداف أيديولوجية كمفهوم الخلافة الإسلامية، وفي هذه الحالة تكون الجماعات ذات فكر وإن كان منحرف.

4.إلحاق الضرر بالبنى المعلوماتية التحتية وتدميرها، والإضرار بوسائل الاتصالات وتقنية المعلومات، أو بالأموال والمنشآت العامة والخاصة للانتقام من الخصوم.

❖ **عوامل انتشار الإرهاب الرقمي:**

العديد من العوامل ساهمت بانتشار الإرهاب الرقمي منها ما يمكن أن يكون تقني والأخر رقابي أو اجتماعي وفقاً للعناصر التالية:

أولاً: ضعف بنية الشبكات المعلوماتية وعدم خصوصيتها وقابليتها للاختراق بسهولة، لأنّ شبكاتِ المعلومات مصممة في الأصل بشكلٍ مفتُوحٍ دون قيود أو حواجز أمنية عليها، بهدف التوسع وتسهيل دخول المستخدمين، وتحتوي الأنظمة الإلكترونية والشبكات المعلوماتية على ثغرات معلوماتية، ويمكن للمنظمات الإرهابية استغلال هذه الثغرات.

ثانياً: غياب الرقابة الذاتية عن طريق التربية، وخصوصية الثقافة المجتمعية، وإلغاء الحدود الجغرافية مما يؤدى إلى تدني مستوى المخاطرة، فيستطيع محترف الكمبيوتر أن يقدِّم نفسه بالهوية والصفة التي يرغب بها، و من ثم بعد فترة يستطيع أن يشن هجومه الإلكتروني وهو مسترخٍ في منزله من دون مخاطرة مباشرة، أو يعمل على التجنيد و الاستقطاب.

ثالثاً: سهولة الاستخدام التقني وقلة التكلفة المادية فقد أصبحت وسائل التواصل الاجتماعي، وجميع وسائل التواصل الالكتروني زهيدة التكلفة ومتوفرة في جميع دول العالم، مما هيأ للإرهابيين فرصة ثمينة للوصول إلى أهدافهم غير المشروعة، ومن دون الحاجة إلى مصادر تمويل ضخمة.

رابعاً: الفراغ التنظيمي والقانوني وغياب جهة السيطرة والرقابة على الشبكات المعلوماتية:

إن الفراغ التنظيمي والقانوني لدى بعض المجتمعات العالمية حول الجرائم المعلوماتية والإرهاب الإلكتروني يعتبر من الأسباب الرئيسة في انتشار الإرهاب الإلكتروني، وكذلك لو وجدت قوانين تجريمية متكاملة فإن المجرم يستطيع الانطلاق من بلد لا توجد فيه قوانين صارمة ثم يقوم بشن هجومه الإرهابي على بلد آخر يوجد به قوانين صارمة، وهنا تثار مشكلة تنازع القوانين من خلال استغلال ضعف التنسيق بين الدول وخاصة فيما يخص الجرائم الرقمية وتخطيها للحدود.

ثالثا: مظاهر الإرهاب الرقمي

شكل استخدام الفضاء الرقمي وسيلة للإرهاب كأداة استراتيجية من قبل الجماعات الإرهابية أخطر أنواع الإرهاب، حيث يلحق الضرر بعدة أنماط مقارنة بالإرهاب التقليدي، كما يوفّر كافة القدرات اللازمة للجماعات الإرهابية، مما يتسنى لها تحقيق أهدافها بسهولة.

تعددت الأساليب والمظاهر التي تنتهجها الجماعات الإرهابية من أجل غايات غير مشروعة، ويشتمل الإرهاب الرقمي على العديد من التقنيات التي من خلالها تتم هذه العملية، حيث تستهدف التخطيط، والتحريض، والتجنيد، وزيادة التطرف، والتمويل، والتنفيذ من خلال الهجمات الإلكترونية أو السيبرانية، (وتتعمد الجماعات الإرهابية على تصميم الجريمة لتكون رقميّة من الأساس شكلاً ومضموناً وانتشاراً وترهيباً ذلك أنها أرادت الاستفادة من خصائص الرقمنة)،[4] ويمكن بلورة وسائل استخدام الجماعات الإرهابية على النحو الآتي:

1. تبادل المعلومات الإرهابية ونشرها من خلال الشبكة المعلوماتية:

إذا كان التقاء الإرهابيين والمجرمين في مكان معين لتعلم طرق الإجرام والإرهاب، وتبادل الأفكار والمعلومات صعباً في الواقع فإنه عن طريق الشبكات المعلوماتية سهلت هذه العملية كثيرا، إذ يمكن أن يلتقي عدة أشخاص في أماكن متعددة وفي زمن معين ويتبادل الحديث والاجتماع لبعضهم عبر الشبكة المعلوماتية، بل يمكن أن يجمعوا لهم أتباعاً[5]، وأيضاً عبر نشر أفكارهم ومبادئهم من خلال المواقع والمنتديات وغرف الحوار الالكتروني.

يعد من أعظم الوسائل المستخدمة في الإرهاب الإلكتروني، وذلك من خلال استخدام البريد الالكتروني في التواصل بين الإرهابيين وتبادل المعلومات فيما بينهم بل إن كثيرا من العمليات الإرهابية التي وقعت في الآونة الأخيرة كان البريد الالكتروني فيها وسيلة من وسائل تبادل

[4] - ملكاوي، اسماء، الارهاب الرقمي، السؤال الاخلاقي الاصعب، 2019.

[5] - د.المرسي، وجيه الدسوقي، "الأساليب الإلكترونية الحديثة التي تستخدمها التنظيمات الإرهابية"، ص148-149.

المعلومات وتناقلها بين القائمين بالعمليات الإرهابية والمخططين لها ويقوم الإرهابيون كذلك باحتلال البريد الالكتروني، والاستفادة منه في نشر أفكارهم والترويج لها والسعي لتكثير الأتباع والمتعاطفين معهم عبر الرسائل الالكترونية.[6]

2.التدريب الإرهابي:

تحتاج العمليات الإرهابية إلى تدريب خاص ويعد التدريب من أهم هواجس التنظيمات الإرهابية وقد أنشأت معسكرات تدريبية سرية كما ظهر بعضها في وسائل الإعلام لكن مشكلة معسكرات التدريب الإرهابية أنها دائماً معرضة للخطر ويمكن اكتشافها ومداهمتها في أي وقت لذا فان الشبكة المعلوماتية بما تحتويه من خدمات ومميزات أصبحت وسيلة مهمة للتدريب والتخطيط والتنفيذ، كما قامت بعض الجماعات الإرهابية بإنتاج أدلة إرشادية للعمليات الإرهابية وهذه الأدلة يمكن نشرها عبر الشبكة المعلوماتية لتصل إلى الإرهابيين في مختلف أنحاء العالم وغني عن البيان ما تشتمل عليه الشبكة المعلوماتية من كم هائل من المواقع والمنتديات والصفحات التي تحتوي على كتيبات وإرشادات تبين كيفية تصنيع القنابل والمتفجرات والمواد الحارقة والأسلحة، يستخدم «يوتيوب» بصورة أساسية من جانب الجماعات الإرهابية بهدف التدريب، فالوظيفة الأساسية للموقع هي استضافة الفيديوهات التي يقوم المشتركون بتحميلها على الموقع (Upload) وبعد ذلك تصبح متاحة للرؤية من قبل الجميع. وعلى الرغم من وجود عدد من القيود على الفيديوهات التي يمكن وضعها على الموقع، فإن نظام المراقبة في الموقع يتم بعد وضع الفيديو على الموقع، وهو ما يعني أنه لن يتم حذف الفيديو، إلا إذا قام المشاهدون على الموقع بالإبلاغ عنه، ثم تتم بعد ذلك مراجعته وإزالته من قبل القائمين على الموقع، ما يجعل هناك إمكانية لتوظيفه من قبل الجماعات الإرهابية، إذ يمكن تحميل فيديو لكيفية تصنيع قنبلة، وتتم مشاهدته مئات المرات قبل أن يتم حذفه من قبل إدارة الموقع.[7]

---

[6]- Dogrul ,Murat and Aslan ,Adil, and Celik, Eyyup, (2011) "Developing an International Cooperation on Cyber Defense and Deterrence against Cyber Terrorism", 3rd International Conference on Cyber Conflict, Tallinn, Estonia, P.32.

[7] - وسائل الارهاب الالكتروني ، المكتبة الشاملة ، http://shamela.ws/.

3.التعبئة وتجنيد الإرهابيين:

تستخدم الجماعات والمنظمات الإرهابية الشبكة المعلوماتية العالمية في نشر ثقافة الإرهاب والترويج لها، وبث الأفكار والفلسفات التي تنادي بهم كما تسعى جاهدة إلى توفير أكبر عدد ممكن من الراغبين في تبني أفكارها ومبادئها، ومن خلال الشبكة المعلوماتية تقوم التنظيمات الإرهابية بتكوين قاعدة فكرية لدا من لديهم ميول واستعداد للانخراط في الأعمال التدميرية والتخريبية، مما يوفر لديها قاعدة ممن تجمعهم نفس الأفكار والتوجهات فيسهل تجنيدهم لتنفيذ عمليات إرهابية في المستقبل.

إن استقدام عناصر جديدة داخل التنظيمات الإرهابية يحافظ على بقائها واستمرارها لذا فإن الإرهابيين يقومون باستغلال تعاطف بعض أفراد المجتمع مع قضاياهم، فيجتذبونهم بأسلوب عاطفي وعبارات حماسية براقة، وذلك من خلال غرف الحوار والمنتديات والمواقع الالكترونية.

4.التهديد والترويع الرقمي:

تقوم المنظمات والجماعات الإرهابية بالتهديد عبر وسائل الاتصالات ومن خلال الشبكة العالمية للمعلومات، وتتعدد أساليب التهديد وتتنوع طرقه، وذلك من أجل نشر الخوف والرعب بين الأشخاص والدول والشعوب محاولة الضغط عليهم للرضوخ لأهداف تلك التنظيمات الإرهابية من ناحية، ومن أجل الحصول على التمويل المالي لإبراز قوة التنظيم الإرهابية من ناحية أخرى.

وقد يلجأ إرهابي (الإرهاب الالكتروني) إلى التهديد وترويع الآخرين عن طريق الاتصالات والشبكات المعلوماتية، بغية تحقيق النتيجة الإجرامية المرجوة، ومن الطرق التي تستخدمها الجماعات الإرهابية للتهديد والترويع الالكتروني إرسال الوسائل الالكترونية المتضمنة للتهديد (e-mails) وكذلك التهديد عن طريق المواقع والمنتديات وغرف الحوار والدردشة الإلكترونية.

ولقد تعددت الأساليب الإرهابية في التهديد فتارة يكون التهديد بالقتل لشخصيات سياسية بارزة في المجتمع، وتارة يكون التهديد بالقيام بتفجير منشآت وطنية، ويكون تارة أخرى بنشر فيروسات من أجل إلحاق الضرر والدمار بالشبكات المعلوماتية والأنظمة الالكترونية في حين يكون التهديد تارة بتدمير البنية التحتية المعلوماتية ونحو ذلك.

5.التجسس الرقمي:

يقوم الإرهابيون بالتجسس على الأشخاص أو الدول أو المنظمات أو الهيئات أو المؤسسات الدولية أو الوطنية، ويتميز التجسس الالكتروني بالطريقة العصرية المتمثلة في استخدام الموارد المعلوماتية والأنظمة الالكترونية التي جلبتها حضارة التقنية في عصر المعلومات، وتستهدف عمليات التجسس الإرهابي في عصر المعلومات ثلاثة أهداف رئيسية وهي: التجسس العسكري والتجسس السياسي والتجسس الاقتصادي. [8]

وفي عصر المعلومات ومع وجود وسائل التقنية الحديثة فإن حدود الدولة مستباحة بأقمار التجسس والبث الفضائي، وقد تحولت وسائل التجسس من الطرق التقليدية إلى الطرق الالكترونية خاصة مع ظهور الشبكات المعلوماتية وانتشارها عالمياً، ومع توسع التجارة الالكترونية عبر الشبكة العالمية للمعلومات تحولت مصادر المعلومات التجارية إلى أهداف للتجسس الاقتصادي.

يرى الباحث أن توظيف الإرهاب الرقمي أصبح مكثفاً من قبل الجماعات الإرهابية، لتجاوز حاجز الزمان والمكان والرقابة الأمنية، وتوفير الوقت والجهد، وتعددت أساليب توظيف تلك الجماعات لهذه الوسائل ما بين الحصول على الدعم، وتجنيد الأفراد، ونشر الأفكار، حتى أصبحت هناك حروب غير تقليدية تدار عبر شبكات التواصل الاجتماعي.

6. الحصول على التمويل:

من خلال الشبكة المعلوماتية العالمية وعن طريق الاستعانة ببيانات إحصائية منتقاة من المعلومات الشخصية التي يدخلها المستخدمون على الشبكة المعلوماتية من خلال الاستفسارات والاستطلاعات الموجودة على المواقع الالكترونية يقوم الإرهابيون بجمع التبرعات ، ويتم ذلك بواسطة رسائل البريد الالكتروني أو من خلال مساحات الحوار الالكترونية بطريقة ذكية وأسلوب مخادع بحيث لا يشك المتبرع بأنه سيساعد إحدى التنظيمات الإرهابية.

[8] - kenanaonline.com/users/ahmedkordy/posts/328932

رابعا: الانترنت المظلم والتطبيقات المشفرة

شكل الانترنت المظلم للجماعات الإرهابية مساحة شاملة وآمنة أكثر بواقع خفي عن مسارات المراقبة والتتبع من قبل الحكومات والأجهزة الأمنية، بسبب إبقاء المعلومات وتبادلها من قبل قيادات وأفراد هذه الجماعات بشكل محمي لا يمكن الوصول إليها، ويرى الباحث أن هذه الأداة ساهمت إلى تحقيق عامل مهم للجماعات الإرهابية من حيث الترابط العنقودي بين الجماعات والخلايا بهدف تبادل المقترحات والتوجيهات واليات تنفيذ العمليات من حيث تحديد الأهداف المراد تنفيذها.

يعتبر الإنترنت المظلم جزءاً مهماً من منظومة الإنترنت، حيث يسمح بإصدار المواقع الإلكترونية ونشر المعلومات بدون الكشف عن هوية الناشر أو موقعه، ويمكن الوصول إلى الإنترنت المظلم من خلال خدمات معينة مثل خدمة Tor، يستخدم العديد من مستخدمي الإنترنت نظام تور(Tor) وخدمات مماثلة كطريقة لتوفير حرية التعبير عن الرأي والارتباط والوصول إلى المعلومات وحق الخصوصية.[9]

هذه المواقع تستخدم تقنيات مشفرة بحيث يصعب جداً تحديد ومعرفة أصحاب هذه المواقع، أيضاً التعامل بين المستخدمين في هذه المواقع يكون باستخدام تقنيات تشفيرية أيضاً، بحيث يصعب جداً تحديد مكان أو هوية المستخدمين.

استخدمت الجماعات الإرهابية هذه التقنيات في العديد من الصور والأشكال، ويشير الباحث كمثال لهذا الاستخدام من خلال الاختراق، حيث شكل "جيش الخلافة الإلكتروني" أحد التشكيلات التي تناصر تنظيم داعش، الذي قام باختراق مواقع إلكترونية أمريكية هامة، فقد أكد البنتاغون في 12 كانون الثاني/ يناير باختراق حساب القيادة العسكرية الأمريكية للمنطقة الوسطى على موقع تويتر، حيث عنون أنصار الجهاد الإلكتروني الصفحة بـ "الخلافة الإلكترونية"، مضيفين عنواناً فرعياً: "نحن نحب الدولة الإسلامية"، وكتبوا على الصفحة: "أيها الجنود الأمريكيون "نحن قادمون..احذروا"، كما أنهم نشروا أرقام هواتف تابعة لعسكريين أمريكيين وصوراً على برنامج "PowerPoint"، وبعض

[9] - https://www.icann.org/news/blog/ar-421519a4-57e7-48d4-ab40-885920dc281a

الخرائط، كما قام أنصار الدولة باختراق صفحة القيادة الوسطى الأمريكية على موقع اليوتيوب، وذلك عبر نشر تسجيلات مصورة من قبل التنظيم لعمليات ميدانية.[10]

يشير الباحث انه كلما زادت التكنولوجيا تقدما زاد التهديد الأمني، ومن ذلك يمكن معرفة الأسباب المتعددة للنشاط الرقمي للجماعات الإرهابية من خلال التطبيقات المشفرة والتي تعتبر مساحة قادرة على أن توفر ديمومة لنشاطها والاستجابة لأهدافها من خلال التجنيد والاستقطاب والتوعية والتحذير والإرشاد، التحريض، التجييش، الاستعطاف، كما أنها استخدمت استراتيجيات معينة كرست من خلالها توظيف التكنولوجيا الرقمية من حيث الإبداع في التصوير، استخدام المؤثرات الصوتية، التلاعب بالصور، التأثير بعملية "غسل الدماغ"، وكانت الفئة المستهدفة من الأطفال، الشيوخ، النساء، الشباب، من حيث التنوع في طرح القضايا التي تهم الأفراد، وأوقات النشر، جلها عوامل يتم التعامل معها بكل حذر و حرفية حتى تؤتي ثمارها وتجني مرادها بحسب متطلبات هذه التنظيمات سواء على المستوى الفردي أو الجمعي و لكل مسمى عوامل التعامل معه.

[10] - حسن أبو هنية ، الآلة الإعلامية لتنظيم الدولة الإسلامية: جيش الخلافة الإلكتروني،19 يناير 2018 م.

الخاتمة:

نظرا للتطور التكنولوجي والذي كان في بداية الأمر ينظر له بالشكل الايجابي في التعامل بين الأفراد والمجموعات إلا انه وعلى نقيض الايجابية فقد تم استثمار هذه الايجابية من قبل المجموعات الإرهابية بما يخدم مصالحها الأيدلوجية، الأمر الذي ساهم بسلبيته على البشرية جمعاء، حيث أنه تم الاستثمار فيه كأداة فاعلة في العمل الإرهابي من ناحية الهجوم والاختراق لمؤسسات حكومية بهدف التخريب وجمع المعلومات، وكما شكل جانبا لهذه الجماعات من حيث نشر إصدارات ومنشورات تساهم بعمليات التجنيد والاستقطاب للانضمام إليها و العمل تحت رايتها كمثال (تنظيم داعش، القاعدة).

استطاعت الجماعات الإرهابية إلى القدرة على التأثير في الجمهور من خلال استراتيجيات نفسية واجتماعية كان لها الأثر المباشر في إحداث عمليات غسل الدماغ والتي ساهمت في العديد من تنفيذ العمليات الإرهابية كاستجابة لقوة العامل المستخدم من قبل الجماعات الإرهابية كوسيلة تنفيذ لمخططاتها الإرهابية.

تكمن خطورة الأعمال الإرهابية الرقمية في اعتمادها على تقنيات متقدمة مثل أجهزة تصنت على شبكات الاتصال، وبرمجيات التشفير، وبرمجيات اختراق أنظمة أمن الشبكات والحاسبات.

النتائج:

توصل الباحث إلى جملة من النتائج كما يلي:

1. يعتبر "الإرهاب الرقمي" أحد أخطر أنواع الإرهاب على المستوى العالمي.
2. استطاعت الجماعات الإرهابية أن تحافظ على تواجدها بعد خسارتها على الأرض مقارنة مع بداياتها في العراق وسوريا، في الفضاء الرقمي من خلال التأقلم مع هذه التقنيات وتسخيرها لخدمة أجنداتها ومخططاتها، وكأداة لنشر أفكارها وترويج منشوراتها.
3. تعدد مظاهر الإرهاب الرقمي، الأمر الذي يساهم بازدياد التهديدات الأمنية للأفراد والمجتمعات والحكومات.

4. ضعف الإنتاج الفكري والإعلامي في مواجهة إصدارات الجماعات الإرهابية، مقارنة بامتلاك هذه الجماعات ترسانة إعلامية ضخمة ومتطورة يشرف عليها متخصصين في التكنولوجيا التقنية والحرب النفسية.
5. استخدمت الجماعات الإرهابية استراتيجيات الأسلوب الاستدراج النفسي والاجتماعي كأداة تأثير على المشاهد بهدف التجنيد والاستقطاب والمناصرة.
6. شكلت مواقع التواصل الاجتماعي حاضنة للجماعات الإرهابية ونخص بالذكر تطبيق التليغرام، والتطبيقات المشفرة.

التوصيات:

أوصى الباحث جملة من النقاط كما يلي:

1. تكثيف الندوات والمحاضرات لتبيان خطورة الإرهاب الرقمي على الفرد والمجتمع.
2. رصد ودراسة نشاط الجماعات الإرهابية في قدراتها على استثمار التطور التكنولوجي بما يخدم أجنداتها وأهدافها.
3. العمل على إصدار نشرات توعوية للأفراد بخطورة جرائم الإرهاب الرقمي والتعامل معها من الجهات المختصة.
4. تعزيز عمل المراكز الأمنية المختصة ورفدها بالدراسات والبحوث التحليلية المختصة بمتابعة إصدارات الجماعات الإرهابية.
5. تشريع قوانين تساهم بالحد من التهديدات الأمنية المتعلقة بالإرهاب الرقمي.