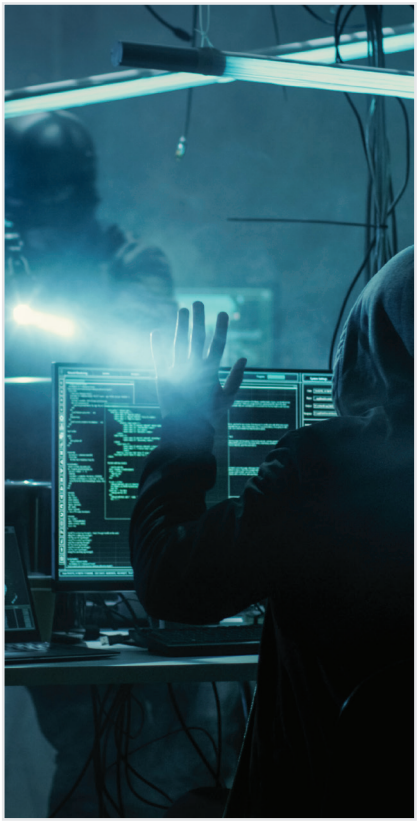
Security Policy Papers
أوراق السياسات الأمنية
https://spp.nauss.edu.sa/index.php/spp
ورقة تحليل سياسات أمنية

سياسات مكافحة تواصل التنظيمات الإرهابية عبر الإنترنت

Policies to Combat the Communication of Terrorist Organizations Online



المخرجات الرئيسة:

- تستهدِفُ سياساتُ مكافحةِ تواصلِ التنظيماتِ الإرهابيةِ عبر الإنترنت وضعَ اللوائحِ والتشريعات التنظيمية للحد من نشر المحتوى الإرهابي، سواء بالحذف، أو الحجب، أو نشر الرسائل المضادة التي تُفَنِّد الأساليب الإقناعية المستخدمة من قِبَل التنظيمات الإرهابية.
- تواجه سياسات المكافحة عددًا من التحديات، أبرزها: التحدي الخاص بالتطور التقني المتلاحق الذي تُوَظِّفُه التنظيمات الإرهابية في عمليات النشر، والدعاية، والتجنيد، وتنفيذ العمليات الإرهابية، والتحدي الثاني هو ضرورة وضع تدابير تنظيمية للمحتوى على شبكة الإنترنت دون المساس بمبادئ حقوق الإنسان كحرية النشر والتعبير، والحق في الحصول على المعلومة، وحماية البيانات الشخصية.
- تحتاج سياسات المكافحة إلى الخروج من حيز اللوائح والقوانين والتدابير التشريعية إلى تصميم خطةِ عملٍ بآليات تنفيذية من خلال مسارين: الأول مسار السياسات طويلة الأمد الإيجابية، وتستهدف بناء العنصر البشري للمجتمعات؛ ليصبح على وعي ودراية بكيفية التعامل الآمن مع البيئة الرقمية، والثاني هو مسار السياسات قصيرة الأمد للرد على المحتوى الإرهابي المنشور حفاظًا على الأمن العام للدول.

المستخلص

تناولت الورقةُ في البداية تطورَ أسلوبِ التواصلِ داخل التنظيمات الإرهابية وصولًا إلى استخدامها للإنترنت في أغلب أنشطتها، ثم ناقشت الورقة بعد ذلك بعضًا من سياسات مكافحة تواصل التنظيمات الإرهابية

Abstract

The paper initially discussed the evolution of communication methods within terrorist organizations, leading to their use of the internet in most of their activities. The paper then discussed some of the policies adopted by international

عبر الإنترنت، التي تَبَنَّتْهَا المنظمات الدولية والإقليمية موضحةً نقاط القوة والضعف بها.

وأخيرًا، أوصت الورقة بضرورة الدمج بين سياسات المكافحة طويلة الأمد «سياسات إيجابية»، والسياسات قصيرة الأمد مع إعطاء الأولوية للسياسات طويلة الأمد؛ لكونها سياسات مُعَزِّزة لمتغيرات إيجابية بالمجتمعات، كما أنها تغطي أكثر من جانب ويتشارك في تنفيذها عدد من المؤسسات. ولم تغفل الورقة التأكيد على أن تستمر السياسات قصيرة الأمد، ولكن مع التركيز بصورة أكبر على النهج التشاركي مع شركات مُقَدِّمي خدمات الإنترنت؛ للوصول إلى خططِ عملٍ تساعد على الحد من انتشار المحتوى الإرهابي بما لا يُخِلّ بمبادئ حقوق الإنسان.

and regional organizations to combat online communication by terrorist groups, highlighting their strengths and weaknesses.

Finally, the paper recommended the need to integrate long-term "positive" policies with short-term policies, prioritizing long-term policies as they reinforce positive variables in communities and cover multiple aspects, shared by multiple institutions in their implementation. The paper emphasized the importance of continuing short-term policies, but with a greater focus on a collaborative approach with internet service provider companies to develop action plans that help limit the spread of terrorist content while upholding the principles of human rights.".

سياق القضية وأهميتها

يمكننا توصيف قضية مكافحةِ تواصلِ التنظيمات الإرهابية عبر الإنترنت بأنها «السهل الممتنع»، حيث يَسْهُل تَتَبُّع المحتوى الإرهابي وحذفه وحجبه والرد عليه، إلا أنه في الوقت ذاته يمكن لهذه التنظيمات الإرهابية بسهولة ويسر أن تُغَيِّر قنوات الاتصال وتنطلق من منصات أخرى، وصولًا إلى مستخدمي الإنترنت الذين تصل نسبتهم إلى 64.6% من إجمالي سكان العالم (We are social,2023).

لقد كان تواصل التنظيمات في بادئ الأمر داخليًّا يعتمد على الشكل الرأسي للاتصال بين القادة وأعضاء التنظيم؛ فيتم نشر الكتب والخطب كمرجعيات فكرية مُوَضِّحة للفكر والإطار الأيديولوجي للتنظيم الذي تُستَمد منه آليات الإقناع، ويتم بثها لأعضاء التنظيم حثًّا على تنفيذ الأهداف والإستراتيجيات، كما استُخدمت المواد المكتوبة في تواصل قادة التنظيمات بعضهم مع بعض وتسجيل المناظرات الفكرية بينهم.

وظل الأمر هكذا حتى ظهور الإنترنت، وهنا شرعت التنظيمات الإرهابية في تغيير شكل الاتصال من التواصل الرأسي إلى التواصل الأفقي، في محاولة منها لاستهداف قاعدة أوسع من الجمهور حول العالم على اختلاف اللغة، والنوع، والعقيدة، والجنسية.

وأصبح الإنترنت عنصرًا مهمًّا في عمل التنظيمات الإرهابية المعاصرة؛ فموجات الإرهاب ارتبطت تاريخيًّا بالتقنيات الاتصالية الجديدة التي استطاعت أن تنشر الأفكار المختلفة على نطاق واسع. لا سيما أن الدعوات المختلفة من جانب التنظيمات الإرهابية على شبكة الإنترنت بالعالم الافتراضي - كان لها مردود في العالم الواقعي. فقد شهدت بلدان مختلفة ارتفاعًا طفيفًا في مغادرة بعض العائلات لها، بعد دعوات الهجرة إلى أرض الخلافة. كما انتشرت أنواع مختلفة من الهجمات الإرهابية كرد فعل للمحتوى المُحَرِّض على تنفيذ عمليات الذئب المنفرد «Lone wolf»، مثل: دهس الأشخاص بالسيارات في الأماكن المزدحمة، والطعن بالسكين (Conway, 2017).

ويشير تحليل بيانات الشباب من مرتكبي العمليات الإرهابية بالولايات المتحدة الأمريكية (في الفترة من 2001 حتى 2016) إلى أن 43% من الشباب تم تجنيدهم عبر شبكة الإنترنت، وأن غالبية المتورطين في عمليات إرهابية يوجد بين أفراد عائلاتهم من هم على اتصال بالجماعات المتطرفة من خلال الإنترنت (Abrahams, 2017).

ولقد أسهمت وسائل التواصل الاجتماعي والإنترنت في رفع وتيرة السرعة وزيادة التعقيد وخفض تكلفة مشاركة المعلومات. وقد دعم هذا بدوره العديد من المنظمات الإرهابية، بل لقد عمل على إتاحة إعادة تنظيم بعضها، وترتيب أوراقها من جديد، وتعزيز قدرة كل خلية وكل فرد على العمل بشكل أكثر استقلالية (Cruickshank & Ali, 2007).

ويمكننا تقسيم نشاط التنظيمات الإرهابية عبر الإنترنت إلى ثلاث مراحل (Bamsey & Montasari, 2023):

- المرحلة الأولى (من عام 1990 إلى 2006 «الويب 2.0»)؛ بحلول عام 1995 بلغ عدد المستخدمين 16 مليون مستخدم، وكان الإرهابيون من أوائل من تَبَنّوا استخدام الإنترنت؛ لأنه غير مكلف، ويتيح الوصول لأعداد متزايدة من الجماهير.
- المرحلة الثانية (من عام 2007 إلى 2015)؛ وهنا بدأ دور منصات التواصل الاجتماعي مع بزوغ تكنولوجيا الهاتف المحمول Smart phone، وتزامن ذلك مع صعود أشهر التنظيمات الإرهابية المعاصرة التي استخدمت منصات، مثل: YouTube وTwitter في دعم وتوزيع دعايتها.
- المرحلة الثالثة مع بداية عام 2016؛ حيث اتخذت المنصات نهجًا نشطًا في إزالة محتوى التنظيمات الإرهابية المتطرفة على منصات التواصل الاجتماعي، وقامت منصة تويتر في هذا العام بتعليق أكثر من 200 ألف حساب متطرف.

ومع تصاعد وتيرة الأعمال الإرهابية خارج مناطق النزاع، ونجاح التنظيمات الإرهابية في تجنيد عناصر بداخل المجتمعات الآمنة عبر الإنترنت، وانتشار التفجيرات وغيرها من أعمال العنف التي باتت التنظيمات الإرهابية تدعو إليها عبر موادها الدعائية على الإنترنت، وتوضح كيفية التخطيط والتنفيذ، وهو الأمر الذي يُرهق المؤسسات الأمنية. أدى ذلك إلى استشعار الدول أن الملاحقات الأمنية ستؤدي إلى مزيد من المعارك التي لا نهاية لها، وبدأت مرحلة التفكير في سياسات بديلة لمكافحة تواصل تلك التنظيمات عبر الإنترنت.

وجاءت البداية في تطبيق النهج التشاركي مع مُنَفِّذِي أو مُطْلِقِي الخدمات عبر الإنترنت، والعمل على ضبط منصات التواصل الاجتماعي والوصول بالخوارزميات إلى حجب ومنع المنشورات المُحَرِّضة على العنف والتطرف، حيث أعلنت شركات تويتر، وفيسبوك، ومايكروسوفت، ويوتيوب في ديسمبر **2016** عن تعاون مشترك، مؤكدين في بيان لهم العمل على وضع خطة لتطوير أدوات مبتكرة لتحديد مقاطع الفيديو الإرهابية مع الالتزام بحذف صور العمليات الإرهابية وإزالتها من منصاتهم (Facebook, 2016).

وتوالى تطبيق النهج التشاركي في مكافحة التنظيمات الإرهابية على الإنترنت، حيث أدركت الشركات العاملة في المجال أن الصناعة باتت مهددة. وبالفعل تم تأسيس منتدى الإنترنت العالمي لمكافحة الإرهاب GIFCT في عام 2017، بواسطة Facebook و Microsoft وTwitter وYouTube مع وجود خبراء من الحكومات والمجتمع المدني وشركات أخرى في

المجال التكنولوجي؛ بهدف التعاون التقني والمعرفي لمعاجلة المحتوى الإرهابي عبر الإنترنت، وتمويل الأبحاث لمواجهة الاستخدام المتطور للإنترنت من قِبل الجماعات الإرهابية (GIFCT,2018).

وساعدت قاعدة بيانات المنتدى على إنشاء بصمات رقمية لأي محتوى إرهابي يتم نشره، ومشاركته مع الشركات الأخرى في الائتلاف؛ وهو ما يسهم في اكتشاف محتوى مشابه ومراجعته بسهولة أكبر لإزالته. إضافة إلى التعاون مع المنظمات الدولية والمنظمات غير الحكومية في جميع أنحاء العالم، بما في ذلك مكتب مكافحة الإرهاب التابع للأمم المتحدة، والاتحاد الأوروبي (GIFCT,2018).

وتعددت استخدامات التنظيمات الإرهابية للإنترنت؛ ولذلك اهتمت الأدبيات بوضع تصور للأشكال المختلفة لهذه الاستخدامات، وكيف استفادت تلك الجماعات من شبكة الإنترنت، وما أتاحته لها من سرعة في الانتشار، وسهولة الوصول للجماهير العريضة من الخلفيات الثقافية والاجتماعية والاقتصادية المختلفة. واتضح من تحليل تواصل التنظيمات الإرهابية عبر مواقع الإنترنت المختلفة، والمنتديات، وغرف الدردشة إمكانية تلخيص عدد من الأهداف التي استطاعت تلك التنظيمات تحقيقها جراء استخدامها واعتمادها على شبكة الإنترنت (Weimann, 2004).

- الحروب النفسية: عملت تلك التنظيمات على نشر المعلومات المضللة؛ لنشر الفوضى، بالإضافة إلى بث التهديدات.
- الدعاية: اعتبرت تلك التنظيمات أن الإنترنت بمثابة مكان آمن للدعاية، واعتمدت عليه في غرس فكرة تبرير العنف الذي تقوم به استنادًا إلى أنه رد فعل لأفعال من دول قوية، مستخدمةً الأسلوب الدعائي الخاص بـ «شيطنة العدو».
- جمع المعلومات: حيث تمد شبكة الإنترنت التنظيمات الإرهابية بالعديد من المعلومات اللازمة لها بشأن المواقع المستهدفة في عملياتها.
- جمع التبرعات: اهتمت التنظيمات الإرهابية بإنشاء شبكة من الجمعيات الخيرية والمنظمات غير الحكومية؛ لتشجيع الآخرين على التبرع لخدمة أهداف تلك التنظيمات.
- التجنيد والتعبئة: عملت التنظيمات الإرهابية على التقاط المعلومات حول المستخدمين، والدخول في مناقشات خاصة مع الشباب؛ لإقناعهم بالانضمام لصفوفهم.
- التخطيط والترتيب والتنظيم: تعتمد التنظيمات الإرهابية بشكل أساسي على شبكة الإنترنت في التخطيط للعمليات المختلفة، بل تنفيذها أيضًا.
- التشبيك Networking: ساعد الإنترنت على تغيير الشكل التنظيمي للتنظيمات الإرهابية، فلم تعد تتبع تسلسلًا هرميًّا متدرجًا، بل ساعد الإنترنت على خلق خلايا عنقودية، تتصل فيما بينها بشكل أفقي.

كما سيطر استخدام التدريب والدعاية على تواصل التنظيمات الإرهابية على الإنترنت، خاصة بعدما فقدت التنظيمات الإرهابية الغالبية العظمى من معاقلها، ومعسكراتها التدريبية من ناحية، ومع توافر الكثير من التطبيقات، ومواقع التواصل من ناحية أخرى. فهذه التطبيقات والمنصات يمكن لها أن تؤدي الغرض بنجاح، وتُمَكِّن المجموعات والأفراد من الالتقاء وتبادل المعلومات، والتعلم، وجمع المعلومات، وتقوية معتقداتهم وعلاقاتهم مع من لديهم معتقدات مماثلة (Siqueira & Arce, 2020).

ويتضح، مما سبق، تعدد الأدوار التي تقوم بها التنظيمات الإرهابية عبر الإنترنت، وهو ما يلقي الضوء بدوره على أهمية مكافحة تواصل التنظيمات الإرهابية عبر الإنترنت، وضرورة وضع إستراتيجيات المكافحة ضمن أولويات الدول. آخذين في الاعتبار أمرين: الأول: إن بعض هذه الاستخدامات توارت إلى حدٍّ بعيد نظرًا لعمليات التضييق الأمني، مثل: التمويل وجمع التبرعات، وفي المقابل تم تعظيم البعض الآخر من الاستخدامات كالدعاية والحروب النفسية التي تسهم بدورها في عمليات التجنيد والتعبئة. إذن يمكننا القول إن الاستخدامات الدعائية، والعمل على غرس الأفكار والترويج للأيديولوجيات المتطرفة هو الهم الأكبر والشاغل الأساسي للتنظيمات الإرهابية المعاصرة، حيث يحرصون على توظيف الأساليب الدعائية لصالح أهدافهم وللحفاظ على وجودهم في العالم الواقعي والافتراضي من خلال أفكارهم.

أما الأمر الثاني؛ فعلى الرغم من عمليات المنع والحجب وإزالة المحتوى المتطرف من على شبكة الإنترنت، والتي تعد آليات مهمة لمكافحة تواصل التنظيمات الإرهابية عبر الإنترنت، فإن السيطرة على الفكر المتطرف أصبح أكثر تعقيدًا. فلم تَعُد المواد الدعائية واضحة النشر، بل متوارية في ثنايا المناقشات وشبكات التواصل الاجتماعي، ومغلفة بطابع اجتماعي يجعل من الصعب تعقبها حتى على خوارزميات الذكاء الاصطناعي التي تحتاج إلى تحليل السياق الثقافي والاجتماعي واللغوي للوصول إلى نتائج دقيقة في تحديد المحتوى المتطرف.

وهو ما ينقلنا إلى الحديث عن أهمية إستراتيجيات المكافحة التي تحاول جاهدة أن تواكب تغير أنماط واستخدامات التنظيمات الإرهابية للإنترنت، وتعمل على الخروج عن المألوف والتفكير خارج الصندوق مثلما لجأت بعض الحكومات في فترة زمنية سابقة إلى ما أُطلِق عليه آنذاك المراجعات الفكرية في محاولة لتصحيح أفكار بعض قادة التنظيمات الإرهابية المؤثرين بدورهم في بقية أعضاء التنظيم. وعلى الرغم من أن الحديث عن تلك الفترة ينصب على العالم الواقعي إلا أن بعض الدول في الوقت الراهن حاولت وضع إستراتيجيات يمكننا أن ندرجها تحت مسمى "النهج الوقائي"، وتهدف تلك الإستراتيجيات طويلة الأمد إلى إشراك أفراد المجتمع بكافة قطاعاته من أجل تحقيق المرونة في التعامل المستقبلي مع الفكر.

إن وضع إستراتيجية لمكافحة الإرهاب عبر الإنترنت بمثابة خطة عمل مستقبلية طويلة الأمد لحماية المجتمعات من الفكر المتطرف، وسيطرة الجماعات الإرهابية بإستراتيجياتها المبنية على خطاب العنف والكراهية.

ولقد اهتمت بعض الدول بوضع نهج وقائي لمكافحة الإرهاب، وتحديد الفئات المعرضة لخطر التجنيد من قِبل التنظيمات الإرهابية عبر الإنترنت؛ بهدف منع تنفيذهم لأية عمليات إرهابية في المستقبل. وتعتبر تلك المرونة في التفكير بمثابة تَكَيُّف مع الكوارث من خلال وضع أهداف مستقبلية إيجابية. وتعمل الدول على تحقيقها من خلال نهجين مترابطين: النهج الأول هو من أعلى إلى أسفل، وبالتالي تقوده الدولة وينطوي على الاعتقال والاحتجاز والتفتيش والمراقبة وغيرها من الأساليب الأمنية. أما النهج الثاني فهو من أسفل إلى أعلى بالاعتماد على المشاركة المجتمعية باعتبارها جهات فاعلة مهمة في التنمية، وتنفيذ ومراقبة السياسات

والممارسات التي تهدف إلى مكافحة الإرهاب. إذن هذان النهجان بمثابة حوكمة لإستراتيجيات مكافحة الإرهاب (Spalek & El-Awa, 2023).

ولا شك في أننا بحاجة إلى أخذ خطوات استباقية لمكافحة الإرهاب، إلا أن البعض يخشى من المساس بعدد من الأمور، فعمليات حجب وإزالة المحتوى تحتاج إلى الإدماج الواسع والمتزايد للذكاء الاصطناعي في الممارسات الرقابية لحماية أغراض الأمن القومي، وهو الأمر الذي يترجمه البعض إلى عدد من المخاوف منها (Dieu & Montasari, 2022):

- أن توسيع نطاق استخدام الذكاء الاصطناعي يمكن أن يتسبب في تهديد حقِّ المواطن في الخصوصية.
- قد تؤثر عمليات المراقبة من أجل أغراض الشرطة التنبؤية على حق المواطنين في محاكمة عادلة.
- المساس بحق مستخدمي المنصات الإعلامية المختلفة في حرية التعبير عن الرأي والحصول على المعلومة.

إن إستراتيجيات إزالة المحتوى والتعامل الأمني والتقني مع المحتوى المتطرف مهمة للغاية، ولها آثارها الإيجابية في حجب كثير من المواد الدعائية الخاصة بالتنظيمات الإرهابية المعاصرة، وتأمين قواعد بيانات الدول، وحمايتها من تنفيذ العديد من العمليات الإرهابية. ولكن تلك الإستراتيجيات قصيرة الأمد تتسم ببعض العوار الناتج عن توسيع نطاق استخدام الذكاء الاصطناعي الذي يخشى البعض من أن يتسبب في انتهاك بعض حقوق المواطنين، بالإضافة إلى أن تلك التقنيات تفتقر إلى الشفافية والدقة في العمل.

وعلى صعيد آخر، تستغل التنظيمات الإرهابية المعاصرة عددًا من التطبيقات التي تحظى بالقليل من الحظر والرقابة، وميزة الخدمات المجهولة أو عدم الكشف عن الهوية أثناء النشر، والحسابات المزيفة، وغيرها من الثغرات. فهذه التنظيمات لا تتوقف عن استغلال أية فرصة للنفاذ من خلالها على شبكة الإنترنت. وسيظل الدوران في دوائر مفرغة طالما أننا لا نضع حدًّا أو فاصلًا لهذه العملية التي يمكن أن يتم إبطاؤها بشكل كبير عبر الثقافة الرقمية المتعمقة، وبناء القدرات البشرية، وإصلاح المجتمعات، وخاصة أوضاع الشباب حول العالم، واحتواء أفكارهم، وأحلامهم، وطموحاتهم.

إن الإستراتيجيات الإيجابية طويلة الأمد هي البديل الأمثل على المدى البعيد خاصة في ظل التطور المتلاحق لمنصات التواصل الاجتماعي، والبحث المستمر للتنظيمات الإرهابية على مخرج لاستخدام تلك المنصات بعيدًا عن الرقابة والتعرض لحذف المحتوى. إن الأمر يتطلب التحول للجمهور المستهدف، والعمل على وضع آليات وإستراتيجيات لحمايته من الأفكار الهدامة التي لا تبغي تَقَدُّم وتنمية المجتمعات، بل تعمل على إفسادها. وهي إحدى أخطر الآليات الدعائية للتنظيمات الإرهابية Spoiling أو إفساد كل ما يدعو للسلام والتنمية ونهضة المجتمعات. وهو ما ينقلنا إلى مناقشة سياسات المكافحة التي تَبَنَّتْها المنظمات الدولية والإقليمية إدراكًا منها لأهمية اتخاذ التدابير والتشريعات.

السياسات والبدائل المطروحة

تنقسم جهود مكافحة الإرهاب إلى جزئين: الجزء الأول: سياسات عامة لمكافحة الإرهاب، والجزء الثاني: سياسات محددة نحو مكافحة الإرهاب عبر الإنترنت.

أولًا: سياسات عامة لمكافحة الإرهاب

أ- جهود الأمم المتحدة في مكافحة الإرهاب

في عام 2006، تَبَنَّتْ جميع الدول الأعضاء في الأمم المتحدة إستراتيجية مكافحة الإرهاب، التي تتألف من أربع ركائز (منظمة الأمم المتحدة، 2006):

- التصدي للظروف التي يمكن أن تؤدي إلى انتشار الإرهاب.
- اتخاذ تدابير لمنع الإرهاب ومكافحته.
- اتخاذ خطوات عملية لبناء قدرة الدول على تنفيذ ذلك.
- اتخاذ التدابير اللازمة لضمان احترام حقوق الإنسان في مكافحة الإرهاب.

وعُنِيَت الإستراتيجيةُ بمكافحة الإرهاب عن طريق حرمان الإرهابيين من الوصول إلى الوسائل التي تُمكِّنُهم من شن اعتداءاتهم، ومن بلوغ أهدافهم؛ من خلال تنسيق الجهود المبذولة على الصعيدين الدولي والإقليمي لمكافحة الإرهاب بجميع أشكاله ومظاهره على الإنترنت، ومساعدة الدول على استخدام الإنترنت كأداة لمكافحة تفشي الإرهاب (منظمة الأمم المتحدة، 2006).

كما اهتمت الإستراتيجية بتناول بناء قدرات الدول لمنع ومكافحة الإرهاب بتغطية الجزء التقني، ووضع خطة عمل تهدف إلى دعم التعاون بين الدول والمنظمات الدولية والإقليمية بغرض تبادل المعلومات حول المساعدات التقنية في مجال مكافحة الإرهاب (منظمة الأمم المتحدة، 2006).

إذن يمكننا القول إن إستراتيجية الأمم المتحدة اهتمت في طياتها بجانب مكافحة الإرهاب عبر الإنترنت، وإن كانت لم تُفْرِدْ جزءًا للأمر في إطار خطة العمل، بل أدرجته في ركائز الإستراتيجية من زاوية التنسيق بين الدول والمنظمات المختلفة لمكافحة الإرهاب عبر الإنترنت، وتبادل المعلومات التقنية. ولكن جاءت العبارات في البنود السابقة فضفاضة، وغير محكمة، ودونما تحديد لطبيعة الأدوار في هذا الصدد، أو تسمية محددة للمنظمات والجهات المنوطة بالتنفيذ.

ب - الإستراتيجية العربية لمكافحة الإرهاب

توصلت الجهود والمشاورات إلى وضع اتفاقية عربية لمكافحة الإرهاب وَقَّعَها وزراء الداخلية العرب تحت مسمى «الإستراتيجية العربية لمكافحة الإرهاب». وتشير ديباجة الاتفاقية إلى أن الدول العربية الموقعة قد أبرمتها التزامًا منها بالمبادئ الأخلاقية والدينية السامية، ولا سيما أحكام الشريعة الإسلامية. وفيما يخص الجزء المتعلق بمكافحة الإرهاب عبر الإنترنت، فقد اهتم المؤتمر العربي الحادي عشر في تونس عام 2008 بوضع عددٍ من التوصيات، التي من شأنها أن تُفعِل الإستراتيجية العربية لمكافحة الإرهاب لمواجهة تطور أساليب التنظيمات الإرهابية من خلال: دعوة الجهات المعنية إلى سَنِّ تشريعات خاصة بالاستخدام غير المشروع للإنترنت والتقنيات الحديثة، وإعطاء مزيد من الاهتمام للدراسات والأبحاث اللازمة حول الأجيال الجديدة من الجماعات الإرهابية وما تستخدمه من أدوات وتقنيات حديثة (مكتب الأمم المتحدة للمخدرات والجريمة، 2009).

وتعد هذه الإستراتيجية من الخطوات المهمة في مجال التعاون العربي لمكافحة الإرهاب، إلا أنه تم انتقاد التعريف الوارد عن الإرهاب؛ لأنه فضفاض للغاية، إضافة إلى أن الاتفاقية ربطت تجريم الأعمال الإرهابية بالتشريعات الداخلية للدول الأعضاء، والتي يتحدد بموجبها ما يُعَدّ أو لا يُعَدّ من قبيل الأعمال الإرهابية (الوافي، 2017).

ثانيًا: سياسات محددة نحو مكافحة الإرهاب عبر الإنترنت

أ - جهود الاتحاد الأوروبي

سعى الاتحاد الأوروبي بشكل محدد إلى إصدار لائحة خاصة بالتصدي لنشر المحتوى الإرهابي على الإنترنت في إبريل 2021، ويمكن ملاحظة عدد من النقاط في إطار تحليل هذه اللائحة (Official Journal of the European Union, 2021):

- طغت الصبغة الإقليمية التوافقية على نصوص اللائحة التي حاولت جاهدة التنسيق بين سبل التصدي للمحتوى الإرهابي على الإنترنت، وإستراتيجيات الدول الأعضاء للتصدي للإرهاب.
- وضع القيود والضوابط التي تحول دون نشر محتوى إرهابي، ولكن دون الإخلال بمبادئ حقوق الإنسان، واحترام الحياة الخاصة، وحماية البيانات الشخصية، وحرية إجراء الأعمال التجارية. إضافة إلى التأكيد على ضمان حرية التعبير، وحرية تلقي وتبادل المعلومات والأفكار في مجتمع ديمقراطي مفتوح تتعدد به وسائل الاتصال.
- وضعت اللائحة تعريفًا لـ«المحتوى الإرهابي» بأنه المواد التي تُحَرِّض أو تَحَثُّ شخصًا ما على ارتكاب جرائم إرهابية أو المساهمة في ارتكابها، أو تَحُثُّ شخصًا ما على المشاركة في أنشطة جماعة إرهابية، أو تمجيد الإرهابيين.
- اهتمت اللائحة بالإشارة إلى عدم اعتبار المواد التعليمية، أو الصحفية، أو الفنية، أو البحثية، التي يتم نشرها لأغراض التوعية ضد النشاط الإرهابي، محتوى إرهابيًّا.
- كما تميزت بوضع إجراءات للتعامل مع المحتوى الإرهابي في نقاط محددة قابلة للتنفيذ وفق خطة عمل المؤسسات المعنية، فألزمت اللائحة مقدمي خدمات الإنترنت بحذف المحتوى الإرهابي خلال ساعة من إبلاغها، كما حرصت على توضيح أسباب الحذف لمقدمي خدمة الاستضافة، وتزويدهم بمعلومات عن إجراءات الإزالة، مع التأكيد على فكرة الاحتفاظ بالمحتوى للاستفادة منه فيما بعد في عمليات التتبع، والرقابة، والتحقيقات.
- ويمكننا القول إن اللائحة تتميز بنظرة بعدية، حاولت توظيف المحتوى الإرهابي وتحويله إلى ركيزة إيجابية تُمَكِّن الأجهزة الأمنية بالدول الأعضاء في الاتحاد الأوروبي من الاستفادة من بيانات الهوية الخاصة بمُوَفِّر المحتوى الإرهابي.
- اهتمت اللائحة بركيزتين أساسيتين، هما: المتابعة والتنفيذ من ناحية، والتقييم من ناحية أخرى، انطلاقًا من أهمية العنصرين كأساس لنجاح السياسات الفاعلة التي تساعد على التطوير وتُعَزِّز من تطبيق الضوابط واللوائح. وفيما يخص المتابعة والتنفيذ، ألزمت اللائحة المفوضية بحلول 7 يونيو 2023 بتقديم تقرير حول تطبيق هذه اللائحة إلى البرلمان الأوروبي يتضمن معلومات عن رصد مدى الالتزام بتطبيق مواد اللائحة، والأداء بشفافية. أما التقييم، فبحلول 7 يونيو 2024 يتعين على المفوضية إجراء تقييم لهذه اللائحة وتقديم تقرير إلى البرلمان الأوروبي بشأن أداء وفعالية آليات الحماية، ومدى تأثير تطبيق هذا النظام على الحقوق الأساسية، وحماية الأمن العام، على أن يكون التقرير مصحوبًا بمقترحات تشريعية عند الاقتضاء.

- تم توجيه الانتقاد للائحة الاتحاد الأوروبي بأنها تعتمد على أدوات غير مفهومة جيدًا للتصدي للمحتوى الإرهابي عبر الإنترنت، وأن عواقب استخدام المواقع والمنصات لهذه الأدوات قد تؤدي إلى انتهاكات غير مقصودة لحقوق الإنسان (Open Letter to the European Parliament, 2019).

وذلك على الرغم من أن اللائحة في مجملها اتخذت منحًى حقوقيًّا واضحًا، حاول أن يحافظ على مكتسبات الديمقراطية والمجتمعات المفتوحة بالدول الأوروبية الأعضاء.

ب- جهود منظمة الشرطة الجنائية الدولية

في إطار التعاون المشترك مع مركز الأمم المتحدة لمكافحة الإرهاب، قام الإنتربول بعمل كُتيِّب بعنوان: Using Internet and Social Media for Counter-Terrorism Investigations (استخدام الإنترنت وشبكات التواصل الاجتماعي في التحقيقات المتصلة بمكافحة الإرهاب). ويزود الكتيب المحققين بإرشادات عملية عن أفضل السبل لاستخراج الأدلة الإلكترونية المفيدة للتحقيقات وجمع وحفظ هذه الأدلة؛ من أجل الإسهام في نجاح التحقيقات والملاحقات القضائية (Interpol,2021).

وتتميز هذه المساهمة بالشكل العملي أو التطبيقي في مجال مكافحة استخدام تكنولوجيا المعلومات والاتصالات لأغراض إرهابية، حيث أورد هذا العمل أفضل الممارسات، وخبرات الإنتربول في مجال مكافحة الإرهاب والجرائم الإلكترونية. فنحن نتحدث في هذا الصدد عن تسخير التكنولوجيا في مكافحة جرائم الإرهاب، وكيفية كشف الأنشطة المتصلة بالإرهاب على الإنترنت، إضافة إلى التعرف على طرق جمع الأدلة الإلكترونية خاصة في جرائم الإرهاب العابرة للحدود، ولكن يمكن الاستفادة من هذا الإسهام في مرحلة مكافحة ما بعد ارتكاب الجرائم الإرهابية على شبكة الإنترنت، وليس في المرحلة القبلية.

ج- إستراتيجية أستراليا للأمن السيبراني (Australia's Cyber Security Strategy, 2020)

عملت أستراليا على وضع إستراتيجية وطنية للأمن السيبراني عام 2020، وأدرجت استخدام الجماعات الإرهابية للتقنيات الأساسية بالإنترنت، والحسابات المزيفة على مواقع التواصل الاجتماعي كأحد عوامل التهديد السيبراني.

وحددت الإستراتيجية الإجراءات من جانب ثلاثة فاعلين، هم: الحكومة وعليها أن تقوم بحماية المواطنين، وتوفير البنية التحتية الأساسية، ومكافحة الجريمة السيبرانية، وحماية البيانات الحكومية والشبكات، وتعزيز قدرات الأمن السيبراني. ثم الشركات العاملة في مجال الأمن السيبراني، والمنوط بها تأمين البنية التحتية للمؤسسات الحيوية، وتنمية القوى العاملة في مجال الأمن السيبراني. وأخيرًا الأفراد بالمجتمع الذين يجب توعيتهم بكيفية الوصول إلى المعلومات على الإنترنت بشكل آمن، وطرق الإبلاغ عن الجرائم الإلكترونية، وتعريفهم بكيفية الوصول إلى المساعدة والدعم عند الاحتياج.

د- تقرير استخدام الذكاء الاصطناعي لمكافحة الإرهاب على الإنترنت في جنوب آسيا وجنوب شرق آسيا (Unicri,2021)

جاء هذا التقرير كَرَدِّ فعلٍ لارتفاع معدلات دمج التقنيات الرقمية في الحياة اليومية في جنوب آسيا

وجنوب شرق آسيا في السنوات الأخيرة، خاصة مع استخدام وسائل التواصل الاجتماعي من قِبَل سكان المنطقة بشكل ملحوظ تجاوز المعدل العالمي.

ويضع العمل نظرة شاملة لتطبيق الذكاء الاصطناعي في مجال مكافحة الإرهاب عبر الإنترنت شارحًا بعض المصطلحات الأساسية، والتقنيات، والعمليات ذات الصلة بالموضوع من منظور تقني، مثل: التحليلات التنبئية للأنشطة الإرهابية، والكشف عن المعلومات الخاطئة والمضللة التي ينشرها الإرهابيون، والإشراف الآلي على المحتوى وإزالته.

وتَمَيَّزَ التقريرُ بمواكبةِ التطورات التكنولوجية الحالية، وطَرْحِ خططِ عملٍ قابلةٍ للتنفيذ في إطار الإلمام باستخدامات التنظيمات الإرهابية للإنترنت، ومنصات التواصل الاجتماعي، وهو ما أتاح تقديم مسارات تطبيقية لمكافحة الإرهاب عبر الإنترنت، ولم يغفل التقريرُ في الوقت نفسه الجانبَ الحقوقي، كما تميز بالاهتمام بالجانب التنبئي للأنشطة الإرهابية، وهو الأمر الذي يمكن لتطبيقات الذكاء الاصطناعي أن تُحَقِّقَه بفعالية.

توصيات وسياسات مقترحة لمكافحة تواصل التنظيمات الإرهابية عبر الإنترنت

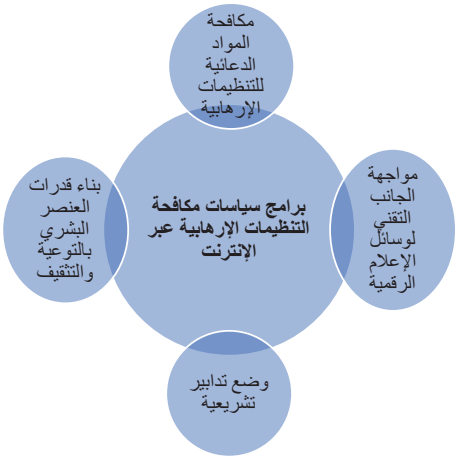
يمكن تقسيم السياسات المقترحة إلى قسمين:

القسم الأول: يُمثل السياسات طويلة الأمد ويمكن تسميتها بالسياسات الإيجابية ؛ لأنها سياسات مُعزِّزة لمتغيرات إيجابية في المجتمعات عبر أكثر من مدخل (تعليمي، وثقافي، وأكاديمي).

القسم الثاني: يُعَبِّر عن السياسات قصيرة الأمد التي تتخذ الأجهزة المعنية من خلالها ردود أفعال نحو المحتوى الإرهابي على الإنترنت سواء بحجب المحتوى، أو تَتَبُّعه، أو حذفه حفاظًا على الأمن العام للمجتمعات. ونخلص مما سبق إلى أن الإستراتيجية المقترحة تستهدف التخطيط على مستويين: مستوى طويل الأمد، ومستوى قصير الأمد.

وذلك لتنفيذ عددٍ من البرامج تتعلق بـ:

- مكافحة المواد الدِّعَائِيَّة للتنظيمات الإرهابية المُقَدَّمة عبر الإنترنت.
- مواجهة الجانب التقني لوسائل الإعلام الرقمية.
- بناء قدرات العنصر البشري، وتوعيته، وتثقيفه.
- وضع تدابير تشريعية منضبطة.



الشكل رقم (1): برامج سياسات مكافحة التنظيمات الإرهابية عبر الإنترنت

أولًا: السياسات طويلة الأمد «سياسات إيجابية»، وتهتم بالأمور الآتية:

أ - سياسات تتخذها المؤسسات التعليمية:

- وضع مناهج لمحو الأمية الإعلامية، وتنمية الثقافة الرقمية بما يتناسب مع الأعمار، والمراحل التعليمية المختلفة مع الاهتمام بتنمية التفكير النقدي، والتحليلي لدى النشء والشباب.

المؤسسات التعليمية:

- إعداد مناهج لمحو الأمية الإعلامية.
- تعريف أفراد المجتمع بآليات التَّحَقُّق من البيانات على الإنترنت.
- تنوير عقول النشء والشباب ضد الأفكار المتطرفة.
- توظيف مناهج التربية الوطنية لتنمية مشاعر الانتماء.

المؤسسات الإعلامية:

- تنمية قدرات الكوادر الإعلامية ودمج الشباب في المؤسسات الإعلامية.
- إنشاء مراكز التحقُّق من البيانات والمعلومات.
- تفعيل حملات توعية بآليات الإبلاغ عن التنظيمات الإرهابية والمحتوى المتطرف على شبكة الإنترنت.
- استهداف الجمهور في حملات الرد على الدعاية المضادة عبر طرق التسويق الإلكتروني.

المؤسسات الأكاديمية:

- تصميم برامج بحثية متكاملة يتم تطبيقها على عينات ممثلة لقياس رجع الصدى الخاص بدعاية التنظيمات الإرهابية على الإنترنت.
- عمل دراسات تحليل مضمون للمحتوى المتطرف أولًا بأول.
- الاهتمام بإعداد المناقشات والتحاور مع النشء والشباب لتحديد احتياجاتهم أولًا بأول خاصة فيما يتعلق بأشكال المحتوى الإعلامي المفضل لهم.

الشكل رقم (2): الإستراتيجيات طويلة الأمد

- الاهتمام بتضمين آليات التَّحَقُّق من المعلومات على شبكة الإنترنت في مناهج محو الأمية الإعلامية، خاصة أن الأبواق الدعائية للتنظيمات الإرهابية صارت تعتمد بشكل كبير على آليات نشر المعلومات المضللة، وخلط الحقائق بالشائعات.
- استخدام محو الأمية الإعلامية لمكافحة تطرف الشباب على وسائل التواصل الاجتماعي لما يتمتع به هذا النهج من نجاح في معالجة المحتوى الضار والعنيف، ومواجهة الخطابات المتطرفة العنيفة على الإنترنت، ودمج ذلك مع الروايات المضادة التي تم تطويرها داخل المجتمعات المستهدفة (Vermeersch et al., 2020).

- توظيف «المناهج الخفية» أو مناهج التربية الوطنية في عملية التنشئة الاجتماعية، وتنمية مشاعر الانتماء والأمان، فالأمر يحتاج إلى تحويل السياسات إلى ممارسات تربوية تعمل على منع العنف والتطرف (Niemi et al., 2018).

ب - سياسات المؤسسات الإعلامية:

- تنمية قدرات الكوادر الإعلامية حتى تستطيع التعامل مع البيئة الرقمية، وتُوَظِّف كافة أدواتها للوصول إلى الجمهور والتأثير فيه، وحتى تتمكن من اختيار قنوات الاتصال المناسبة، وتكون مؤهلة

لصنع محتوى إعلامي مؤثر يغرس القيم الإيجابية في الأطفال والنشء والشباب بشكل خاص.

- في إطار السياسات الإعلامية للدول والمنظمات، يجب الاهتمام بشكل أوسع بإنشاء مراكز للتحقق من المعلومات والبيانات Fact Checkers حتى تصبح ظهيرًا أساسيًّا للقائمين على العمل الإعلامي، يتحققون فيه من المعلومات والبيانات قبل النشر؛ للحفاظ على الأمن العام للمجتمعات، ودرءًا للآثار السلبية لآليات الدعاية الخاصة بالتنظيمات الإرهابية.
- تفعيل حملات توعية للإعلام بآليات الإبلاغ عن التنظيمات الإرهابية على المواقع والمنصات، والمحتوى المتطرف على الإنترنت. وذلك على غرار حملات توعية «Action counters terrorism ACT» ببريطانيا، التي تستهدف توعية المواطنين بكيفية الإبلاغ عن المحتوى الإرهابي (Action Counter Terrorism, 2023).
- تعمل التنظيمات الإرهابية على تفتيت الرسائل الإعلامية وفقًا للمنطقة التي يتم البث إليها، وبالتبعية تراعي المجتمع الموجود في تلك المنطقة وخصائصه المختلفة، فتذهب بعض التنظيمات الإرهابية إلى تقسيم الدول إلى ولايات، كل ولاية أو منطقة لها مكتب إعلامي خاص بها، حتى إن المواد المنشورة تصبح مصبوغة بطبيعة المنطقة، ويمكن للمحلل أو الباحث في المجال أن يميز المنطقة المستهدفة من المادة الإعلامية بمجرد مشاهدة اللقطات أو الكلمات الأولى من المادة المُقدَّمة، ومن هنا تجدر الإشارة إلى أن الرد على دعاية التنظيمات الإرهابية لا بد أن يكون بنفس كفاءة سير العمل، ومن خلال آليات التسويق الإلكتروني المتعارف عليها. وأن يتم استهداف الجمهور وفقًا لخصائصه وسماته الديموجرافية من نوع، وسن، ومستوى اجتماعي واقتصادي وثقافي مع الاهتمام باللهجة والأشخاص المؤثرين في المجتمع المستهدف.
- يجب إعادة صياغة أدوات الاتصال والإعلام لخدمة احتياجات الشباب، فبدلاً من معاملاتهم على أنهم جمهور، يتم العمل على فهم وجهات نظرهم وخبراتهم، وإشراكهم في مناصب لحل المشكلات، واستبعادهم من خانة صانعي المشكلات، ومحاولة تغيير السلوك من خلال الإقناع والأساليب الأكثر تشاركية (Freear & Glazzard, 2020).

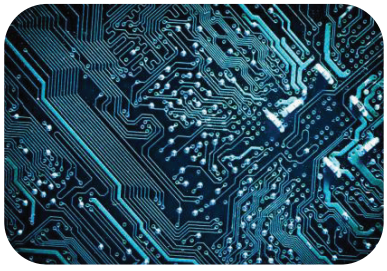
ج- سياسات المؤسسات الأكاديمية:

- إنشاء برامج بحثية بغرض إجراء مسوح على عينات قومية داخل المجتمعات على فترات زمنية محددة؛ لقياس مدى نجاح التنظيمات الإرهابية في توظيف الإنترنت للوصول إلى الجماهير، بالإضافة إلى تحليل المحتوى الإرهابي المنشور على الإنترنت بشكل دوري؛ لمعرفة المضامين التي يتم تصديرها إلى المجتمعات، وللتمكن من قياس مردود وتأثير هذه المواد الإعلامية.
- إجراء حوار مجتمعي دوري للتعرف على وجهات نظر النشء والشباب في الرسالة الإعلامية التي يفضلونها، والمتابعة والتقييم المستمر للرسائل الإعلامية التي يتم بثها ردًّا على الدعاية الخاصة بالتنظيمات الإرهابية.
- وهو ما ينقلنا إلى ضرورة الاهتمام في هذا الصدد بتوظيف مدخلات علم النفس المعرفي في

حملات الرد على الدعاية المتطرفة للتنظيمات الإرهابية؛ فقياس الفهم والإدراك والتذكر على سبيل المثال يفيد القائمين على الاتصال في معرفة مدى تأثير المواد الإعلامية في اتجاهات الفئات المستهدفة التي تعرضت لتلك الرسائل، وتأثيراتها الإقناعية على مكونات الاتجاه من مستوى معرفي، وأوتار عاطفية، ومخرجات سلوكية، وهو ما ينتج عنها اتجاه إيجابي أو سلبي بعد ذلك داعم أو رافض. تلك العمليات المعرفية المعقدة تأتي في سياق دراسات التأثير النفسي والمعرفي لوسائل الاتصال، وتعد من أبرز الدراسات البَيْنِيَّة التي يتشارك فيها علم النفس وعلم الاتصال؛ للوصول إلى فهم جيد لمدى تأثير الرسائل الإعلامية وكيفية صياغة الرسائل بدقة وفاعلية. ويأتي ذلك في إطار عمليات التقييم والمتابعة سواء لتأثير الرسائل المتطرفة أو رسائل الدعاية المضادة للجهات المَعْنِيَّة بمكافحة الإرهاب.

حجب وإزالة المحتوى المتطرف من شبكة الإنترنت

وضع سياسات تشاركية مع شركات منفذي الخدمات لتنسيق سياسات الحجب والمنع والإزالة



إعداد كوادر قادرة على العمل بكفاءة في مجال تكنولوجيا المعلومات والذكاء الاصطناعي والأمن السيبراني

وضع تدابير تشريعية منضبطة

الشكل رقم (3): الإستراتيجيات قصيرة الأمد

ثانيًا: السياسات قصيرة الأمد

نَعْنِي بها سياسات الحجب، وإزالة المحتوى، وردع منتجي المحتوى الإرهابي لمنع انتشاره؛ بغرض حماية الأمن العام، وذلك من خلال عدد من الآليات:

- وضع تدابير تشريعية وقانونية منضبطة، ومُلِمَّة بالتقنيات والتطبيقات الحديثة التي تعمل على تنقية المحتوى على الإنترنت، وحجبه، وإزالته، وتَتَبُّع صانع المحتوى.
- ضرورة إعداد كوادر قادرة على العمل بكفاءة في مجال تكنولوجيا المعلومات والذكاء الاصطناعي والأمن السيبراني.
- وتجدر الإشارة إلى أن منع انتشار المحتوى المتطرف عبر الإنترنت ينطوي على الاستفادة من التكنولوجيا والمنصات التي يمتلكها عادة القطاع الخاص؛ لذا فإن الشراكة والتعاون بين القطاعين العام والخاص أمر حاسم (Zeiger & Gyte, 2020).
- منع الإرهاب عبر الإنترنت من خلال الخطاب المضاد من الانخراط المباشر مع حجج الجماعات الإرهابية وتفكيكها وتفنيدها، ونزع الشرعية عن الجماعات الإرهابية (Neumann & Stevens, 2009).
- من الناحية التجريبية لمشاركة Google و-Face book وTwitter في مكافحة الإرهاب، تفيد الدراسات بأن هذه الشركات تنتقل من الموقف التفاعلي إلى موقف استباقي بشكل متزايد، بل يظهرون التزامًا بالتنظيم الذاتي والإبداع في تطوير وتنفيذ نظم مكافحة الإرهاب على الإنترنت. وهو ما يشير إلى منطق جديد للحوكمة في مجالات سياسة مكافحة الإرهاب، حيث أصبحت شركات المنصات حلقة أساسية في مكافحة المحتوى الإرهابي على الإنترنت (Borelli, 2021).
- يجب وضع مزيد من السياسات التشاركية مع شركات مُقَدِّمِي الخدمات، خاصة مع قدوم منصات جديدة كالميتافيرس، التي تتطلب قدرات هائلة من أجل تحديد المحتوى الضار، وقد أعلنت بالفعل شركة Meta أنها طورت حاسوبًا عملاقًا سيكون واحدًا من أسرع الأجهزة الخارقة للذكاء الاصطناعي في العالم (Hollowell, 2022).
- توجيه صانعي السياسات باستخدام التقنيات الرقمية كآلية لتنفيذ تدخلات مكافحة الإرهاب من خلال نفس الإمكانات الرقمية والوصول إلى نفس جماهير التنظيمات الإرهابية، مع العمل على تطوير قدرات الكوادر المنوطة بالتنفيذ (Bertram, 2016).

الخاتمة

«بالبنادق يُمْكِنُكَ قَتْل الإرهابيين، ولكن بالتعليم يُمْكِنُكَ قَتْل الإرهاب ذاته» هذه العبارة للناشطة الباكستانية ملالا يوسفزاي التي تُلَخِّص بها أهمية غرس القيم الإيجابية من خلال المؤسسات التعليمية والتثقيفية، كما توضح ضرورة اتباع السياسات الإيجابية في مواجهة فكر التنظيمات الإرهابية. وهو ما تؤكده الورقة في اقتراحها للسياسات المناسبة لمكافحة تواصل التنظيمات الإرهابية عبر الإنترنت؛ فالسياسات الإيجابية طويلة الأمد تستثمر بالأساس في العنصر البشري، وتعمل على دراسة احتياجاته بشكل مستمر.

ويبدأ اعتناق الأفكار المتطرفة بمرحلة الوعي والمعرفة بتلك الأفكار، ثم تأتي مرحلة الاهتمام بها، وأخيرًا قبولها والشروع في تنفيذها (Helfstein, 2012)، وهنا يجب على واضعي السياسات أن يتدخلوا بخططِ عملٍ

في مرحلتي المعرفة والاهتمام حتى لا نصل إلى مرحلة القبول والتنفيذ. فالتوعية بخطورة الأفكار المُقدَّمة عبر شبكة الإنترنت، والتعامل الآمن مع البيئة الرقمية هو حجر الزاوية في سياسات المكافحة الإيجابية، إضافة إلى تعزيز قيم التسامح وتَقَبُّل الآخر، واتباع النهج التشاركي مع المؤسسات الإعلامية، ومنظمات المجتمع المدني، وشركات مُقَدِّمي الخدمات عبر الإنترنت.

المراجع

أولاً: المراجع العربية:

- منظمة الأمم المتحدة. (2006). متاح على https:// www.un.org/counterterrorism/ar/ un-global-counter-terrorism-strategy
- مكتب الأمم المتحدة للمخدرات والجريمة. (2009). دراسات حول تشريعات مكافحة الإرهاب في دول الخليج العربية واليمن، https://www.unodc.org/documents/ terrorism/Publications/Study_CT_Legislation_Gulf_Yemen/Arabic.pdf
- الوافي، سامي. (2017). الإرهاب: بين الاتفاقيات الدولية والتشريعات الوطنية، المركز الديمقراطي العربي. https://democraticac. de/?p=43304#_ednref21

ثانيًا: المراجع الأجنبية:

- Abrahams, J. A. (2017). Ideological radicalization: a conceptual framework for understanding why youth in major us metropolitan areas are more likely to become radicalized (Doctoral dissertation, Monterey, California: Naval Postgraduate School).
- Action Counter Terrorism (2023). Report Suspicious Activity. Available at: https://act.campaign.gov.uk/
- Australia's Cyber Security Strategy. (2020). Available at:https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.
- Bamsey, O., & Montasari, R. (2023). The Role of the Internet in Radicalisation to Violent Extremism. In Digital Transformation in Policing: The Promise, Perils and Solutions (pp. 119-135). Cham: Springer International Publishing.
- Bertram, L. (2016). Terrorism, the Internet and the Social Media Advantage: Exploring how terrorist organizations exploit aspects of the internet, social media and how these same platforms could be used to counter-violent extremism. Journal for deradicalization, (7), 225-252..
- Borelli, M. (2021). Social media corporations as actors of counter- terrorism. New Media & Society, 25(11). Available at:https://doi.org/10.1177/14614448211035121.
- Conway, M. (2017). Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research. Studies in Conflict & Terrorism, 40(1), 77-98.
- Cruickshank, P., & Ali, M. H. (2007).

- Hollowell,A. (2022). Meta's RSC supercomputer brings revolutionary power — and privacy and bias concerns. Venturebeats. Available at: https://venturebeat.com/ai/metas-rsc-supercomputer-brings-revolutionary-power-and-privacy-and-bias-concerns/.
- Interpol.(2021). Analysing Social Media. Available at: https://www.interpol.int/en/Crimes/Terrorism/Analysing-social-media.
- Neumann, P., & Stevens, T. (2009). Countering online radicalisation: a strategy for action. International Centre for the Study of Radicalization and Political Violence (ICRS).
- Niemi, P. M., Benjamin, S., Kuusisto, A., & Gearon, L. (2018). How and why education counters ideological extremism in Finland. Religions, 9(12), 420.
- Official Journal of the European Union (2021). Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online. V. 6. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?Uri=OJ:L:2021:172:FULL&from=EN.
- Open Letter to the European Parliament (February 2019). Available at:https://cdt.org/wp-content/uploads/2019/02/Civil-Society-Letter-to-European-Par-

Abu Musab Al Suri: Architect of the New Al Qaeda. Studies in Conflict & Terrorism, 30(1), 1-14..
- Dieu, O., & Montasari, R. (2022). How States' Recourse to Artificial Intelligence for National Security Purposes Threatens Our Most Fundamental Rights. In Artificial Intelligence and National Security (pp. 19-45). Cham: Springer International Publishing..
- Facebook (2016) Partnering to help curb spread of online terrorist content, Facebook News, 5 December. Available at https:// newsroom.fb.com/news/2016/12/partnering-to-help-curb-spread-of-online-terrorist-content/
- Freear, M., & Glazzard, A. (2020). Preventive Communication: Emerging Lessons from Participative Approaches to Countering Violent Extremism in Kenya. The RUSI Journal, 165(1), 90-106.
- GIFCT .(2018). Global Internet Forum to Counter Terrorism: an update on our efforts to use technology, support smaller companies and fund research to fight terrorism online, Global Internet Forum to Counter Terrorism Press, 8 June. Available at https://gifct.org/press
- Helfstein, S. (2012). Edges of radicalization: Ideas, individuals and networks in violent extremism. Military Academy West Point NY Combating Terrorism Center.

- Vermeersch, E., Coleman, J., Demuynck, M., & Dal Santo, E. (2020). Social media in Mali and its relation to violent extremism: A youth perspective. International Counter-Terrorist Centre (ICCT). Retrieved from https://icct.nl/app/uploads/2020/03/Social-Media-in-Mali-and-Its-Relation-to-Violent-Extremism-A-Youth-Perspective.pdf
- We are social. (2023). Available at: https://www.slideshare.net/datareportal/digital- 2023-april-global-statshot-report-v01- april-2023.
- Weimann, G. (2004). How modern terrorism uses the Internet. V. 31. United States Institute of Peace.
- Zeiger, S., & Gyte, J. (2020). Prevention of Radicalization on Social Media and the Internet. International Centre for Counter-Terrorism (ICCT).
liament-on-Terrorism-Database.pdf.
- Siqueira, K., & Arce, D. (2020). Terrorist training: Onsite or via the Internet? European Journal of Political Economy, 63, 101878. Advance online publication. Doi:10.1016/j.ejpoleco.2020.101878
- Spalek, B., & El-Awa, S. (2023). Governance and counter-terrorism: Engaging moderate and non-violent extremist movements in combatting jihadist-linked terrorism. International journal of law, crime and justice, 72, 100367.
- Unicri.(2021). Counter Terrorism online with Artificial Intelligence “An overview for Law enforcement and counter terrorism agencies in South Asia and South-East Asia,New Yourk, Available at:https://unicri.it/News/-Countering-Terrorism-Online-with-Artificial-Intelligence

Received 23 May 2023; Accepted 17 July 2023; Available Online 10 Oct. 2023.

Heba Atef Labib
National Center for Social and Criminal Research

هبة عاطف لبيب
المركز القومي
للبحوث الاجتماعية والجنائية

Keywords: security studies, online terrorism, terrorist groups, digital culture.

الكلمات المفتاحية: الدراسات الأمنية، الإرهاب عبر الإنترنت، التنظيمات الإرهابية، الثقافة الرقمية.

Production and hosting by NAUSS

* Corresponding Author: Heba Labib
Email: HebaAtef10121978@gmail.com
doi: 10.26735/TERY2818