

ندوة بعنوان الوسائل الإلكترونية المستخدمة في التطرف العنيف/ وحدة الارشاد والتوجيه اعداد: أ.م.د. أنعام عبد الرضا سلطان العكابي

اسهم تطوير التكنولوجيا وسهولة استخدام مواقع التواصل الاجتماعي في خلق بيئة خصبة للجماعات المتطرفة من أجل الترويج لأجنداتها وأفكارها المتطرفة. ومن ثم صارت هذه المواقع مثل، فيسبوك وتويتر ويوتيوب وتلغرام وغيرها بمثابة أدوات فعالة للجماعات المتطرفة لتجنيد المتعاطفين مع قضيتها من خلال التلاعب بالمعلومات ونشر الأخبار المزيفة. وعادة ما تستهدف التنظيمات المتطرفة الفئات الأصغر سناً عبر الإنترنت بسبب سهولة التأثير فيهم وكسب تعاطفهم؛ مما يجعل التطرف عبر الإنترنت تهديداً ملحاً أمام الحكومات والمجتمع عليهم مواجهته. وبناءً عليه، ظهرت مبادرات كمنتدى الإنترنت العالمي لمكافحة الإرهاب (من قبل فيسبوك، ومايكروسوفت، وتويتر، ويوتيوب)، ومبادرة "Tech Against Terrorism" (التي تدعمها الأمم المتحدة) من أجل مكافحة استخدام تكنولوجيا المعلومات والاتصالات الجديدة لأغراض إرهابية، بما في ذلك التجنيد والتحريض على ارتكاب أعمال إرهابية فضلاً عن التمويل والتخطيط والإعداد. في هذا الإطار، يستعرض تقرير "مكافحة التطرف العنيف على الإنترنت" الصادر عن مؤسسة راند "RAND" في العام 2023 للباحثين: جوان نيكلسون، وشون كيلينغ، وماريغولد بلاك الإجراءات والسلوكيات ومنصات التكنولوجيا التي يستخدمها المتطرفون عبر الإنترنت، كما يبحث التقرير الآثار المترتبة وكيفية مواجهة الأنشطة العنيفة عبر الإنترنت ولاسيما التطرف العنيف بدوافع أيديولوجية، مثل، تنظيمي القاعدة وداعش. ويعتمد التقرير على نموذج متشابه من خمس مراحل يوضح سلوكيات مثل: الاستهلاك العام عبر الإنترنت الذي يتضمن إمكانية تضمين محتوى متطرف، وتحديد أولويات المحتوى المتطرف، وتخفيف المخاطر، وإيضاح الهوية المتطرفة، والتركيز على نشر محتوى التطرف العنيف.

بيئة مرنة:

أسهم عاملان رئيسيان في جعل الفضاء الإلكتروني نظاماً بيئياً محفزاً للأنشطة المتطرفة هما: النزعة الديمقراطية للاتصالات والتقنيات الناشئة، والوعي المتزايد للإرهابيين المعاصرين بإمكانية استخدام الإنترنت كأداة لتحقيق أغراضهم. وهكذا، صار الإنترنت ملاذاً للمتطرفين، حتى قبل انتشاره في العالم. وبمرور السنوات، اتسعت أنشطة التطرف العنيف على الإنترنت بشكل أكبر، ولاسيما مع ظهور الشبكات اللامركزية والمشفرة والشبكة المظلمة "Dark web". ويشير تقرير "راند" إلى تبني المتطرفين لوسائل التواصل الاجتماعي من أجل إنشاء أو نشر المواد الإعلامية الخاصة بهم، وجذب الأتباع وتنظيم الأنشطة الافتراضية والواقعية، بل وأحياناً تعزيز مواردهم وجمع التبرعات. لكن، يكمن التحدي هنا في أن التطورات السريعة والمستمرة في المنصات والتطبيقات صارت تتجاوز قدرات البحث، ومن ثم القدرة على مواجهة أنشطة المتطرفين على الإنترنت. بالتالي، صارت هناك فجوة بين السياسات الحكومية وغير الحكومية لمواجهة التطرف وبين سرعة تكيف المتطرفين العنيفين مع التطور التكنولوجي.

علاوةً على ذلك، قد يساعد الإنترنت على تحول المستخدمين العاديين إلى متطرفين نتيجة التعرض المستمر للأفكار أو السلوكيات المتطرفة عبر المواقع الإلكترونية ولاسيما وسائل التواصل الاجتماعي، بالتالي يتم تجنيد العديد من المستخدمين لا إرادياً أو تلقائياً، أي حتى من دون تدخل مباشر من قبل الجماعات المتطرفة المعروفة.

سلوكيات التطرف:

أشار تقرير "راند" إلى مراسلات تعود لمؤسس تنظيم القاعدة وزعيمه السابق أسامة بن لادن في يونيو 2002، والذي شدد خلال هذه المراسلات على أهمية الحرب الإعلامية ضمن الاستعداد الكلي للمعارك، مما يعكس إدراك قيادة "القاعدة" مبكراً للإمكانيات الاتصالية الهائلة للإنترنت، ومن ثم سعت إلى تسخير هذه الإمكانيات لتعزيز الأهداف الاستراتيجية لتنظيماتها، وفيما يلي شرح تطور الأنظمة البيئية للأنشطة المتطرفة تزامناً مع تطور التقنيات والتطبيقات على الإنترنت:

(1) المواقع الإلكترونية والمنتديات: من بين أولى المحاولات لاستغلال الإنترنت من قبل المتطرفين هي إنشاء موقع Azzam.com في عام 1997 من قبل طالب في إمبريال كوليدج بلندن. وقد ركز الموقع على الصراعات القائمة في هذه الفترة في مختلف أنحاء العالم الإسلامي، مثل البوسنة والشييشان وكشمير وأفغانستان، وفي 2000، أنشأ تنظيم القاعدة موقع maalemaljihad.com، والذي كان نشطاً حتى منتصف يوليو 2002. وفي إبريل 2003، ظهر موقع القاعدة مجدداً ولكن ولم تقتصر الأنشطة المتطرفة لتنظيم القاعدة على مقره الرئيسي، بل انتقلت إلى خلاياه النشطة في المنطقة العربية والتي ركزت على إمكانية إشراك الرأي العام عبر غرف الدردشة والمنتديات. ففي أواخر 2003، ظهرت موجة من المواقع الإلكترونية المتطرفة أغلبها كان مرتبطاً بالحرب على العراق، مثل منتديات: الأنصار، والإخلاص، والبراق، والفردوس، والغلوجة، وشموخ الإسلام.

(2) مواقع التواصل الاجتماعي: بادر المتطرفون باستغلال منصات التواصل الاجتماعي كالفايس بوك وتويتر والإنستغرام منذ ظهورها. إذ قدمت هذه المنصات للمتطرفين العنيفين طرقاً جديدة لإحداث التأثير وبناء الشبكات والتواصل مع الجماهير على نطاق أوسع. ويُشار في هذا الصدد إلى تنظيم داعش والذي استثمر في بناء ذراع إعلامي متطور في الفترة بين عامي 2013 و2015، بما يضمن للتنظيم مخرجات عالية الجودة، وتواصلًا فعالاً مع الجمهور، ومن ثم تجنيد أعداد كبيرة من المقاتلين والحفاظ على اتصال غير مسبوق مع جمهوره عالمياً.

(3) تطبيق التلغرام: منذ نشأة التطبيق، حرصت التنظيمات المتطرفة وعلى رأسها داعش على إنشاء مجموعات وقنوات عامة داخله (أي يمكن الوصول إليها بشكل مفتوح للجميع)، ومجموعات وقنوات أخرى خاصة تتطلب دعوة أو رابط انضمام حتى يتمكن المستخدم من دخولها. بل، واستخدم المتطرفون خاصية الروبوتات المجهولة في التلغرام لنشر المحتوى. وخلال عامي 2016 و2017، صار التلغرام منصة أساسية لداعش والمتطرفين العنيفين المرتبطين به. ولاسيما وأن المجموعات الخاصة في التطبيق قادرة على الاستمرار في النشاط المتطرف لفترات طويلة دون اكتشافها أو حذفها. ومع ذلك، لا زال تويتر بيئة قوية ظاهرياً للمتطرفين من أجل الوصول السريع والواسع إلى الجمهور مقارنة بالتلغرام.

(4) الشبكة اللامركزية والشبكة المظلمة: توفر طبيعة الشبكة اللامركزية (التي تتكون من تقنيات تهدف إلى إضعاف التحكم المركزي في الإنترنت باستخدام كود مفتوح المصدر وشبكات موزعة) وسيلة فعالة للتنظيمات المتطرفة العنيفة. إذ إن المحتوى المضاف على الشبكة لا يمكن إزالته بسهولة لأنه لا يخضع لسيطرة سلطة مركزية. فعلى سبيل المثال، أنشأ تنظيم داعش في 2014 سلسلة من الحسابات على ثلاث منصات لامركزية منخفضة المستوى وهي: "Friendica" و "Diaspora"

و"Quitter". وفي سبتمبر 2017، أنشأ تنظيم داعش أيضاً حسابات على شبكة وسائط اجتماعية لامركزية أخرى هي "Element"، ثم شبكات "Rocket.Chat" و"ZeroNet" في 2018.

وفي سياق متصل، توفر الشبكة المظلمة "Dark Web" للمتطرفين مستوى أعلى من الأمان الشخصي والقدرة على استضافة المحتوى في مساحة غير منظمة. ولذلك، استمرت وسائل الإعلام الداعمة لتنظيم داعش حتى 2021 في الاعتماد على مواقع الويب على "Surface Web" و"Dark Web" لأرشفة وتوزيع البيانات الرسمية للتنظيم، والصور والفيديوهات. هذا ومن أمثلة قنوات داعش على الشبكة المظلمة أساس إعلام، وأخبار المسلمين، والرائد.

تكتيكات إلكترونية:

تتنوع تكتيكات التنظيمات المتطرفة من أجل زيادة فرص الوصول إلى الجمهور وإشراكه في قضية التطرف العنيف ذات الصلة، وتتيح هذه التكتيكات للمتطرفين حرية المناورة ضد الإجراءات المضادة، كما تعزز مرونة النظام البيئي للتطرف العنيف وقدرته على البقاء، ومن هذه التكتيكات:

(1) التشبث: وهو يهدف إلى حماية حسابات المتطرفين أطول وقت ممكن عن طريق التحايل على خوارزميات الذكاء الاصطناعي، ويُصنف إلى تشبث نصي (استخدام الرموز بدلاً من الحروف مثل استخدام @ بدلاً من a) وتشبث بصري (استخدام صور مضللة لتجنب كشف الهوية) وتشبث الحساب (استخدام اسم مضلل لحساب فيديو للخوارزميات أنه يحارب الجماعات المتطرفة بدلاً من نشر أفكارها).

(2) عامل الأمن واختيار المنصة: يفضل المتطرفون تكتيكات إخفاء الهوية مثل الشبكات الخاصة والبريد الإلكتروني المشفر و"TOR" والمنصات الأقل تقييداً مثل، تطبيق التلغرام والشبكات اللامركزية لتحسين الأمان وتسهيل المشاركة.

(3) الربط البيئي للشبكات: يُفضل المتطرفون التنقل عبر المنصات للحفاظ على النظم البيئية المعقدة (على سبيل المثال يتم نشر فيديو على Odysee و Archive في نفس الوقت)، وذلك من أجل تجنب إجراءات أي منصة والحفاظ على المحتوى أطول فترة. ويحرص المتطرفون على إنشاء محتوى متنوع ومستمر للحفاظ على الجمهور المستهدف وجذب الآخرين، من خلال التوسع في إشراك الجمهور في المحتوى، إذ إن الهدف الأكبر هو خلق مساحات تفاعلية أكثر أماناً لأغراض التجنيد. وبالنسبة للجمهور، عادة ما تكون عملية الانتقال من مستخدم عادي إلى متطرف تدريجية وغير ملحوظة بل وتجارب فردية.

سبل المواجهة

يوصي تقرير "راند" بضرورة إجراء مزيد من الفحص لسلوكيات الفاعلين المتطرفين على الإنترنت لاكتساب نظرة ثاقبة تجاه السمات المحددة التي تظهر خلال مراحل المشاركة. وأيضاً، شدد على أهمية توسيع واختبار سلوكيات المتطرفين على الإنترنت في فترات النشاط والركود لفهم كيفية تغييرها بشكل أفضل. كذلك، لا بد من توسيع نطاق الفئات المستهدفة من خلال بحث العناصر المتطرفة داخل النظام البيئي أو خارجه.

وأخيراً، من الضروري تعزيز التعاون بين المجموعات المتباينة لتحسين الوعي بالتداخل بين قضايا الإرهاب والتطرف والتدخل الأجنبي والمعلومات المضللة. ولاسيما وأن أنشطة التطرف العنيف على الإنترنت لا تحدث بمعزل عن الأحداث والقضايا الأخرى. وبالتالي أي استراتيجيات متوقعة لمواجهة التطرف على الإنترنت لا بد وأن تعالج موضوعات مثل نشر المعلومات المضللة وانعدام الثقة في المؤسسات.

وبالرغم من أن التطرف العنيف بدوافع أيديولوجية أكثر تطوراً في استغلال التكنولوجيا الرقمية وعالم الإنترنت مقارنةً بالتطرف العنيف بدوافع عنصرية وعرقية. إلا أنه من الممكن الاستفادة من نتائج التقرير بشأن أنشطة "التطرف العنيف بدوافع أيديولوجية" على الإنترنت في تحديد المسارات المحتملة لأنشطة "التطرف العنيف بدوافع عنصرية وعرقية" أثناء تطوره والدفع بردود أفعال أفضل ولاسيما وأن النمط الأخير من التطرف يحظى باهتمام الحكومات في الغرب في الوقت الحالي. ختاماً، سعى تقرير "راند" لفهم كيف يتصرف المتطرفون العنيفون في نظام إيكولوجي متزايد التعقيد على الإنترنت، حيث يوفر هذا النظام (الذي يتميز بالابتكار التكنولوجي وتنوع المنصات) مزايا كبيرة للمتطرفين العنيفين، من خلال توفير مجموعة متنوعة من التدابير والسلوكيات التي يستخدمها المتطرفون العنيفون كاستكشاف منصات للتكنولوجيا البديلة يكونون فيها أقل تحدياً وأكثر أماناً.

وينتهي التقرير بالتركيز على ضرورة فهم أكبر وأكثر تفصيلاً لمشهد التطرف العنيف عبر الإنترنت سواءً أكان "التطرف العنيف بدوافع أيديولوجية" أم "التطرف العنيف بدوافع عنصرية وعرقية"، وبدوره يدفع ذلك الفهم صانعي القرارات إلى التفكير في حلول مختلفة وجديدة وربما أكثر فاعلية للتعامل مع التطرف العنيف عبر الإنترنت وتحديه.