الشبكة المظلمة والإرهاب

عبد العزيز أغراز

باحث أكاديمي بالاتصالات والشبكات المعلوماتية، بكلية العلوم والتقنيات بمراكش، المغرب

ينشَط الإرهابيون في مواقعَ مختلفة على شبكة الإنترنت منذ أواخر التسعينيات، مما أدَّى إلى فتح جبَهات جديدة لمكافحة الإرهاب في العالم الافتراضي، ولا سيما بعد أحداث الحادي عشر من سبتمبر 2001م. وتُعَدُّ شبكة الإنترنت السطحي مَيدانًا خِصبًا لنشر الأفكار الإرهابية؛ لتوافر آلاف المواقع والمنتديات التي تروِّج للفكر الإرهابي، لكنَّ لهذه الشبكة مخاطرَ كبيرة على الإرهابيين تتعلَّق بالسرِّية وإخفاء الهُويَّة. إذ إن الكثير من مواقع الشبكة الإرهابية ووسائل التواصل الاجتماعي تراقبها وكالاتُ مكافحة الإرهاب، وغالبًا ما تُغلَق أو تُخترَق، فيلجأ الإرهابيون إلى التواصل بسرِّية باستخدام شبكة الإنترنت المظلم «Dark Web».

أنواع الشبكات

العالم الافتراضيُّ يشبه جبلًا جليديًّا ضخمًا معظمه تحت سطح الماء، فما يستعمله جُلُّ الناس هو شبكة الإنترنت السطحي المفهرسة، ولا يمكن لكلِّ مستخدمي شبكة الإنترنت الوصولُ إلى الأجزاء الخفيَّة المعروفة باسم شبكة الإنترنت العميق «Deep Web» التي تُخفي في أعماقها محتوًى خاصًّا، تُسمَّى شبكة الإنترنت المظلم.

1. **الإنترنت السَّطحي «Surface Web»:** هو ما يصلُ إليه المستخدمون في نشاطهم اليومي المعتاد، وتكون متاحةً باستخدام محرِّكات البحث القياسية مثل: Google و Bing، ويمكن الولوجُ إليها باستخدام متصفِّحات مثل: Mozilla Firefox، و Microsoft Internet Explorer، و Google Chrome.
2. **الإنترنت العميق «Deep Web»:** وهو يتكوَّن من مواقع إلكترونية غير المفهرسة، ويتعذَّر الوصولُ إليه عبر محرِّكات البحث القياسية، وحجمُه أكبر من الإنترنت السَّطحي بـ 400 أو 500 مرة. وبعضُ المواقع العميقة هي أسواقٌ غير تقليدية، تُقدِّم مجموعةً خطِرة من المنتجات أو الخِدْمات؛ كالعقاقير غير المشروعة، والأسلحة، والسِّلع المقلَّدة، وبطاقات الائتمان المسروقة، والبيانات المخترَقة، والعُملات الرَّقْمية، والبرمجيات الضارَّة، وبطاقات الهُويَّة الوطنية وجوازات السفر المزوَّرة.
3. **الإنترنت المظلم «Dark Web»:** هو فرع من الإنترنت العميق، ويُتيح إنشاء مواقع إلكترونية، ونشرَ المعلومات، دون الكشف عن هُويَّة الناشر أو موقعه، أو الفهرسة بمحرِّكات البحث، ولا يمكن الوصولُ إليه باستخدام المتصفِّحات العادية. ويُستخدَم فيه مجموعاتٌ من العُقَد الفردية والترميز القوي لحماية البيانات، وعرقلة تتبُّع النشاط الإلكتروني من قِبَل الحكومات وأجهزة الأمن. ويُستعمَل في ممارسة الأنشطة غير القانونية؛ كالاتِّجار بالمخدِّرات، وشراء الأسلحة غير القانونية، والتخطيط

للعمليات الإرهابية، وقد يُوظَّف أحيانًا في بعض الأنشطة المشروعة . ويمكن للأفراد استخدامُ شبكة الإنترنت المظلم ببرامجَ خاصَّة مثل: I2P أو Tor الذي أنشأه مختبرُ البحوث البحرية الأمريكية أداةً للتواصُل المخفيِّ في شبكة الإنترنت. وإن تتبُّع المستخدمين في شبكة الإنترنت المظلم أصعبُ من تتبُّعهم في شبكة الإنترنت السطحي، ففي معظم الحالات لن يعرفَ زائر موقع onion هُويَّة المضيف، ولن يعرفَ المضيف هُويَّة الزائر، خلافًا لما يجري في شبكة الإنترنت السطحي؛ إذ ترتبط المواقعُ غالبًا بشركة أو موقع، ويمكن تحديد هُويَّة الزوَّار ومراقبتهم بتِقنيَّات التتبُّع المختلفة، مثل: مِلفَّات تعريف الارتباط، وتسجيلات الحساب، وعناوينIP ، والموقع الجغرافي.

الإرهاب الإلكتروني

يُعرِّف الدكتور أيسر محمد عطيَّة الإرهابَ الإلكتروني بأنه: العدوانُ أو التخويف أو التهديد ماديًّا أو معنويًّا، الصادر عن الدول أو الجماعات أو الأفراد تجاه الإنسان في دينه، أو نفسه، أو عِرضه، أو عقله، أو ماله، باستخدام الوسائل الإلكترونية. وعرَّفته وِزارةُ الدفاع الأمريكية بأنه: عمل إجرامي يُنفَّذ باستخدام الحواسيب ووسائل الاتصالات، وينتج عنه عنفٌ وتدمير أو تخويفٌ بهدف الضغط على الحكومة أو السكَّان؛ لتحقيق مطالبَ سياسيةٍ أو اجتماعية أو فكرية معيَّنة.

تمكِّن شبكةُ الإنترنت المظلم الجماعاتِ الإرهابيةَ من الاختباء والتجنيد والدعاية، وتبادل المقترحات والمعلومات الميدانية، والحصول على الأسلحة المختلفة، وشراء الموادِّ الضرورية للتغذية والمحروقات، وتعبئة الهواتف النقَّالة، واقتناء تذاكر النقل الجويِّ والبحري، واستئجار السيارات، وحجز الفنادق، إضافةً إلى توفير التعليم والتدريب للإرهابيين الجدُد؛ بتوظيف الموادِّ المصوَّرة التي توضِحُ كيفيةَ استعمال الأسلحة، وإعداد العبوات الناسفة، وغيرها من الأنشطة المتطرفة. ففي أغسطس 2013م اعترضت وكالةُ الأمن القومي الأمريكية الاتصالاتِ المُعمَّاةَ (المشفَّرة) بين زعيم القاعدة أيمن الظواهري وزعيم تنظيم القاعدة في شبه الجزيرة العربية ناصر الوحيشي.

وفي أكتوبر 2013م اعتقل مكتبُ التحقيقات الفيدرالي الأمريكي مديرَ موقع «طريق الحرير» الإلكتروني، روس ويليام أولبريشت المشتبَه في تجارته بالمخدِّرات، وصادر أيضًا عُملات «بيتكوين» رَقْميَّة تصل قيمتها تقريبًا إلى 3.6 مليون دولار. وفي أبريل 2018م صدر تقريرٌ عنوانه «الإرهاب في الظلام» تضمَّن نتائجَ دراسة أجرتها جمعيةُ هنري جاكسون، كشفت ازديادَ استخدام الجماعات الإرهابية الشبكةَ المظلمة، وأوضحت كيف ينمِّي الإرهابيون والمتطرفون الملاذات الآمنة في الشبكة المظلمة؛ للتخطيط لهجَمات مستقبلية، وجمع الأموال، وتجنيد أعضاء جُدد.

مِنصَّات وتطبيقات

استخدم الإرهابيون تطبيقاتٍ محميَّةً تتيح لهم بثَّ رسائلهم إلى عددٍ غير محدود من الأعضاء عبر الهاتف المحمول، ومنها:

1. **تطبيق تيليغرام Telegram:** أنتج هذا التطبيقَ الأخوان الروسيَّان بافل ونيكولاي دوروف عام 2013م، ويتميَّز بالحماية التامَّة للمستخدِمين، ويربطهم بالشبكة المظلمة. وبعد أربعة أيام فقط من إتاحة

تطبيق تيليغرام لخدمة القنوات في 20 سبتمبر 2015م بدأ ناشطون إعلاميون لداعش على موقع تويتر بالإعلان عن القناة الخاصَّة بالتنظيم، وأطلق فرعُ القاعدة في شبه الجزيرة العربية قناته الخاصَّة على تيليغرام في 25 سبتمبر 2015م، ثم أنشأت جماعةُ أنصار الشريعة الليبية قناتها في اليوم التالي. وفي مارس 2016م فُتحت 700 قناة جديدة مناصِرة لهذا التنظيم، وازداد أعضاءُ قناة واحدة تابعة لداعش في أسبوع واحد من خمسة آلاف عضو إلى أكثر من عشرة آلاف. واستخدم هذه القنوات أيضًا تنظيمُ القاعدة وجبهة النصرة وجيش الإسلام.

2. **منصَّة تام تام Tam Tam:** أطلقت وكالةُ «ناشر» للأنباء في 29 نوفمبر 2019م قناةً رسمية لها على منصَّة «تام تام» الروسية، بعد التضييق عليها في تيليغرام، ليحذوَ أنصارُ التنظيم حذوَها؛ بإنشاء عشَرات الحسابات على المنصَّة ذاتها.
3. **تطبيق Hoop:** اختار تنظيمُ داعش منذ أواخر سنة 2019م هذا التطبيقَ لإنشاء قنوات خاصَّة تحمل الأسماءَ المعتادة لحساباته العامَّة، ويُتيح هذا التطبيق خياراتٍ مختلفةً عن بقية منصَّات التواصل الاجتماعي تسمح لمستخدميه بإنشاء معرِّفات مختلفة وقابلة للتغيير؛ لكيلا يُعرَف مكان المستخدم، إضافة إلى خِيار المحادثات المحميَّة التي لا يمكن لأحد الاطِّلاعُ عليها إلا بواسطة رَقْم سرِّي خاص بالمستخدم .

المكافحة والتصدِّي

قامت وكالةُ مشروعات البحوث المتطوِّرة الدفاعية داربا (DARPA) التابعة لوِزارة الدفاع الأمريكية بتطوير محرِّك البحث MEMEX الذي يسمحُ بفهرسة مواقع شبكة الإنترنت العميق، وكشف الجانب الخفي من الشبكة؛ بإتاحة الولوج إلى الشبكة الآمنة (Tor)، والصفَحات والمواقع غير المفهرسة على الشبكة.

وفي عام 2014م كشفت تسريبات إدوارد سنودن عن تحقيق في الترميز المصدري في أحد برامج وكالة الأمن القومي الأمريكية (NSA) يسمَّى XKeyscore أظهر أن أي مستخدم يحاول تنزيل Tor تؤخذ بصَمات أصابعه تلقائيًّا، مما يمكِّن وكالةَ الأمن القومي من معرفة هُويَّة ملايين مستخدمي Tor.

وبعد هجَمات نوفمبر 2015م في باريس، لجأ تنظيمُ داعش إلى الشبكة المظلمة لنشر الأخبار والدعاية، في محاولة واضحة لحماية هُويَّات مؤيِّدي التنظيم وحماية محتواه من ناشطي القرصنة. وتأتي هذه الخطوةُ بعد إزالة مئات المواقع المرتبطة بداعش بحملة ضمن عملية باريس (OpParis) التي أطلقتها مجموعةُ أنونيمس (Anonymous) فنشر إعلامُ داعش روابطَ وتوضيحاتٍ عن كيفية الوصول إلى الموقع الجديد على الشبكة المظلمة.

ونجحت الاستخباراتُ العراقية في اختراق الغرف المظلمة لتنظيم داعش على الشبكة، والإطاحة بأكثر من 400 إرهابي في شهري مايو ويونيو سنة 2020م.

عُملات الإرهابيين

يستخدم الإرهابيون العُملات الرَّقْمية، مثل بيتكوين Bitcoin وغيرها؛ لضمان السرِّية، وجمع الأموال، والشِّراء غير القانوني للمتفجِّرات والأسلحة. وفي عام 2014م نُشر في الإنترنت مقالٌ عنوانه: «بيتكوين وصدقةُ

الجهاد» يروِّج لاستخدام عُملات بيتكوين الافتراضية؛ لتسهيل الدعم الاقتصادي للإرهابيين، والالتفاف على النظام المصرفي الغربي الذي يحدُّ من التبرُّعات بفرض القيود على النظام المالي. ويسرد تقريرُ تقنية المعلومات والاتصالات الصادر سنة 2018م، وعنوانه: «استخدام الجهاديين للعُملة الافتراضية»، عدَّة حالات لجماعات إرهابية تستخدم عُملات رَقْميَّة لجمع التبرُّعات وشراء الأسلحة. ففي ديسمبر 2017م وجهَت محكمةٌ فيدرالية في نيويورك اتهامات لزوبيا شاهناز من لونغ آيلاند بالاحتيال المصرفي وغسل الأموال التي يُزعَم أنها تدعم الإرهاب، وسرقة أكثرَ من 85000 دولار من العائدات غير القانونية باستخدام عُملة بيتكوين الرَّقْمية وغيرها، إضافةً إلى تحويل الأموال إلى خارج البلاد لدعم تنظيم داعش.

ختام القول

إن الشبكة المظلمة على الرغم من مخاطرها لا تخلو من إيجابيَّات ومنافع، فالعديدُ من المؤسسات الإخبارية تستخدمها لحماية المصادر السرِّية، وتوفير حرِّية التعبير عن الرأي، وسهولة الارتباط والوصول إلى المعلومات، ومراعاة الخصوصيَّة. ويجد كثيرٌ من الصحفيين والمدافعين عن الحقوق المدنية وناشطي الديمقراطية ملاذًا آمنًا في الشبكة المظلمة؛ دَرءًا للرقابة أو السَّجن، وإن أول من استخدم شبكة Tor ليسوا إرهابيين أو مجرمين بل منشقُّون.

ويُعَدُّ برنامج Tor جزءًا من سكيور دروب (SecureDrop) وهي منصَّة مفتوحة المصدر تساعد الصحفيين والمؤسسات الإعلامية والإخبارية على تلقِّي الموادِّ الإعلامية وإرسالها؛ كالأخبار والمقاطع المصوَّرة (فيديو)، والصور العادية، بأمان تامٍّ وسرِّية، مع الحفاظ على جهالة المرسل. وقد تحوَّل عددٌ كبير من المواطنين مستخدمي الهواتف المحمولة إلى تطبيقات المراسلة المحميَّة؛ للمحافظة على خصوصيتهم، وحماية معلوماتهم ومراسلاتهم.