الإرهاب السيبراني - خطر يهدِّد العالم

عبدالستار عبدالرحمن

صحفي وباحث

أدت التطورات التقنيَّة التي شهدتها وسائل الاتصال الحديثة إلى دخول الإرهاب حِقبةً جديدة، وأسهمت في إعادة النظر في أشكاله الحالية؛ فلم يعُد يقتصر على نمطه التقليدي الذي يمكن الوصول إليه واستهدافه، ولكنه بات عابرًا للحدود والأوطان على نحو يصعب السيطرة عليه بغلق الحدود أو تأمينها. لقد صار اهتمام الجماعات الإرهابية منصبًّا على انتشار الفكرة، وتجنيد العناصر عبر الإنترنت، بل انتقلت معسكرات التدريب من عالم الواقع إلى العالم الافتراضي، فلم يعُد يشترط تدريب الأفراد في معسكر بأحد الكهوف أو قمم الجبال، بل يكفي للعنصر الجديد أن يحصل على التدريب وما يحتاج إليه من معلومات من المواقع الإلكترونية الخاصة بالجماعات الإرهابية.

لقد تغيرت خُطط الإرهاب وأدواته المستخدَمة بمرور الوقت، ولاح في الأفق شبح الإرهاب الإلكتروني (السيبراني)، الذي يستهدف فيه الإرهابيون البُنى التحتية للدول، وأنظمة معلوماتها، وقواعدها العسكرية. فما الإرهابُ الإلكتروني، وما مخاطره وفرصُ مواجهته والتغلب عليه؟

الإرهاب الإلكتروني

في الثمانينيات الميلادية، صاغ باري كولين Barry Collin، زميل أبحاث أول في معهد الأمن والاستخبارات في كاليفورنيا، مصطلح "الإرهاب الإلكتروني" Cyberterrorism في إشارة إلى التقاء الفضاء الإلكتروني والإرهاب. وفي عام 1998، نشر المشروع العالمي للجريمة المنظمة التابع لمركز الدراسات الإستراتيجية والدَّولية في واشنطن CSIS تقريرًا بعنوان "جرائم الإنترنت والإرهاب الإلكتروني والحرب الإلكترونية: تجنب حدوث ووترلو إلكترونية" 'Cybercrime, Cyberterrorism and Cyberwarfare: Averting an Electronic Waterloo'، كان أولَ مساهمة رئيسة في هذا المجال.

ومع أن الإرهاب الإلكتروني (السيبراني) أصبح شائعًا في السنوات الأخيرة، وبات خطرًا كبيرًا على الصعيد الدَّولي، ولا سيَّما مع التطور السريع لتقنيَّات الاتصال، والاعتماد المتزايد للبشر على (الإنترنت) ووسائل التواصل الاجتماعي، ليس هناك تعريف عالمي متفق عليه للإرهاب الإلكتروني! فقد تعددت تعريفاته ما بين

مكتب التحقيقات الفيدرالي الأمريكي، ووِزارة الدفاع الأمريكية، وحلف الناتو، وغيرها من المؤسسات ومراكز البحوث المعنية، حتى زاد عددها على 27 تعريفًا، القاسم المشترك بينها جميعًا هو أن الإرهاب الإلكتروني يُعَد النقطة التي يتقاطع فيها الإرهاب مع الفضاء الإلكتروني، وهو يختلف عن الجرائم الإلكترونية، كسرقة البيانات، والاحتيال المصرفي، وغيرها.

وسيلة إعلام عالمية

يمثل الفضاء الإلكتروني عنصرَ جذب مهمًّا للتنظيمات الإرهابية على اختلاف أنواعها وتباين أفكارها؛ نظرًا لما يتيحه لها من وسيلة إعلام عالمية هي في الوقت نفسه سلاح خطير فاتك. ويعدُّ تنظيم "داعش" الإرهابي أكثرَ التنظيمات تهديدًا لسلامة الإنترنت؛ باستخدامها في الدعاية والتجنيد والتمويل وجمع المعلومات، وتنسيق الهجمات الإرهابية، وحشد المتعاطفين من مختلِف بقاع العالم. وعمل التنظيم على تجنيد جيش إعلامي متخصص بالإعلام الإلكتروني، يعمل تحت أسماء مختلفة.

وهناك عوامل تُغري التنظيمات الإرهابية باستخدام الإرهاب الإلكتروني، منها أنه يمكن تنفيذه من أي مكان في العالم، ولا يلزم أن يكون الفاعل في موقع العمل الإرهابي؛ إذ تتوافر على نطاق واسع وصلات الإنترنت اللازمة لتنفيذ الهجوم باستخدام أي هاتف محمول حديث.

ولا تعتمد سرعة الهجَمات الإلكترونية على سرعة وصلة الإنترنت التي يستخدمها المهاجم، بل يمكن استغلال السرعة العالية لوصلة الإنترنت التي تستخدمها الحواسيب التي تتعرض للهجوم. ذلك أن (الفيروسات) وغيرها من البرمجيات المؤذية يمكن أن تنتشر بأعلى سرعة ممكنة دون الحاجة إلى مزيد من التدخل من المهاجم.

ويمكن إبقاء الأعمال المرتكبة عبر الشابِكة مجهولةَ المصدر، وغير قابلة لاقتفاء أثرها وتتبُّعها، عن طريق خِدْمات تجهيل المصدر وما شابهها من تقنيات التمويه؛ كاستخدام حواسيب مسيطر عليها عن طريق القرصنة. ويضاف إلى ذلك أن وسائل الإثبات الرَّقْمية يمكن تزييفها عمدًا. ويزيد من الإغراء بالإرهاب الإلكتروني انخفاضُ تكلفة الإنترنت، وكثرة الأهداف التي يمكن قصدها واختيار مهاجمتها، وكثير من تلك الأهداف قد لا يتمتع بحماية كافية.

في ظل هذه المغرِيات سارعت مختلِف الجماعات الإرهابية والمتطرفة إلى امتلاك مواقع على (الإنترنت)، وبخاصة شبكات التواصل الاجتماعي، وبعضها يمتلك أكثر من موقع وبأكثر من لغة، من أجل التعريف بالتنظيم وتاريخه ومؤسسيه وأنشطته، وخلفياته السياسية والاجتماعية، وأهدافه الفكرية والسياسية، وأحدث الأخبار، ومهاجمة خصومه من المفكرين والعلماء، ومن الحكومات والأجهزة الأمنية.

إن تنظيم داعش مثلًا دعم قدراته الإلكترونية بدمج أذرعه (السيبرانية) مثل: "الخلافة الشبح" Ghost Caliphate، و"جيش أبناء الخلافة" Sons Caliphate Army، و"جيش الخلافة السيبراني" The Caliphate Cyber Army، و"كلاشينكوف الأمن الإلكتروني" Kalashnikov E-Security فيما سُمي (مجموعة قراصنة الخلافة السيبرانية المتحدة) The United Cyber Caliphate Hacker Group.

وتمكنت مجموعة من القراصنة التابعين لتنظيم داعش في السنوات الأخيرة من اختراق بعض مواقع الشابِكة لتشويهها، ونشر الدعاية المتطرفة، مثل مواقع وزارة الصحة البريطانية، والشرطة الماليزية الملكية، والخطوط الجوية الماليزية، وشبكة التلفزة الفرنسية TV5 والمحطات التابعة لها، والقيادة المركزية العسكرية الأمريكية.

صِنفان متداخلان

نظرًا لعدم وجود تعريف دقيق ومتفق عليه لمفهوم الإرهاب الإلكتروني، يتداخل صِنفان مختلفان لهذا الإرهاب هما: الإرهاب الإلكتروني الخالص، والإرهاب الإلكتروني الهجين.

أما النوع الأول الإرهاب الإلكتروني الخالص، فيتعلق بالهجَمات المباشرة على البنية التحتية السيبرانية للضحية، مثل: الحواسيب والشبكات، والمعلومات المخزَّنة فيها؛ لتحقيق أهداف مختلفة، كإفساد وظائف أنظمة المعلومات، وإتلاف أو تدمير الأصول الافتراضية والمادية، وحجب المواقع الإلكترونية، وتعطيل الحياة اليومية باستهداف البنية التحتية التي تُدار بأجهزة حاسوبية، كتلك المتعلقة بالمرافق الطبية، والبورصات، والنقل، والأنظمة المالية، وغير ذلك.

وأما النوع الثاني الإرهاب الإلكتروني الهجين، فيشير إلى استخدام الإرهابيين للفضاء الإلكتروني في مختلِف أنشطتهم، ومن أبرز نماذجه:

1 - الدعاية والحرب النفسية. على سبيل المثال: لتنظيم "داعش" سبعُ وكالات إعلامية، إضافة إلى 37 مكتبًا إعلاميًّا في بلدان مختلفة. ولتنظيم "القاعدة" ذراعٌ إعلامية باسم (سحاب) Sahab.

2 - التواصل الآمن. وذلك بهدف إرسال رسائلَ مشفرةٍ أو إخفاء المعلومات للمناقشات السرية، وتخطيط الهجمات والتنسيق لها، كما في حادثة مقتل كاهن فرنسي في نورماندي في يوليو 2016، حيث تلقى قتلتُه توجيهاتهم عبر الشابِكة.

3 - تجنيد أعضاء جدد. لاحظ تقريرٌ لمجموعة العمل المالي الدَّولية FATF عام 2015 أن الشابِكة باتت الأداةَ الأكثر استخدامًا للتجنيد ودعم التنظيمات الإرهابية.

4 - التدريب. بنشر أدلة التدريب التي تشرح كيفية شنّ الهجَمات وتصنيع المتفجرات، في المواقع الخاصة بالتنظيمات.

5 - جمع التبرعات.

6 - جمع المعلومات عن الأهداف البشرية المحتملة.

مخاطر مرعبة

تُعَد القنابل الإلكترونية من أبرز وسائل تنفيذ عمليات الإرهاب الإلكتروني، مثل: تعطيل الاتصالات والتشويش عليها، والتنصُّت على المكالمات، وبث معلومات مضللة، وتقليد الأصوات، وبخاصة أصوات القادة العسكريين لإصدار أوامر خطيرة، واستهداف شبكات الحاسوب بالتخريب عن طريق نشر (الفيروسات)، ومسح الذاكرة الخاصة بالأجهزة المعادية، ومنع تدفق الأموال وتغيير مسار الودائع، وإيقاف محطات الكهرباء عن العمل. وقد أُعدَّت لتلك المهمة قنبلةٌ إلكترونية خاصة أُطلق عليها اسم cbu 49، تنطلق منها عدة قنابلَ في الجوِّ تستهدف محطات الكهرباء وتؤدي إلى احتراقها وتدميرها الكامل.

وفي ورقة بعنوان (مستقبل الإرهاب الإلكتروني) أُلقيت في (الندوة الدَّولية السنوية الحادية عشرة لقضايا العدالة الجنائية) قدَّم الباحث باري كولين قائمةً مرعبة بأعمال الإرهاب الإلكتروني المحتملة التي تهدد مستقبل البشرية أبرزها:

- الوصول عن بُعد إلى أنظمة التحكم بمصانع الحبوب، وتغيير مستويات مكمِّلات الحديد، للإضرار بصحة المستهلكين.

- إجراء تعديلات عن بعد في معالج حليب الأطفال، للإضرار بصحة الأطفال الرضَّع.

- تعطيل المصارف والمعاملات المالية الدَّولية والبورصات، لإفقاد النظام الاقتصادي الثقة فيه.

- تغيير مكونات صناعة الأدوية عن بُعد لدى شركات الأدوية.

- تغيير الضغط في خطوط الغاز، وأحمال شبكات الكهرباء، مما يوقع انفجارات وحرائق مروِّعة.

- مهاجمة أنظمة التحكم في الحركة الجوية، وجعل طائرتين مدنيتين تتصادمان، عن طريق الولوج إلى أجهزة الاستشعار في قمرة القيادة بالطائرة، وهذا ممكن أيضًا في خطوط السكك الحديدية.

وإذا كانت التهديدات السابقة للإرهاب الإلكتروني مجرد تصورات نظرية لم يقع منها شيء بفضل الله، فإن ذلك لا يعني الاستكانة، بل يدعو إلى استباق عقول الإرهابيين والاستعداد لإبطال ما يمكن أن يفكروا فيه من أشكال ذلك الإرهاب.

ضرورة المواجهة

تعود بدايات الجهود الدَّولية لمواجهة الجريمة الإلكترونية والإرهاب الرَّقْمي إلى ثلاثة عقود مضت، حين ناقش "الإنتربول" الدَّولي في عام 1981 إمكانية وضع تشريع قانوني خاص بالجريمة الإلكترونية. ومنذ ذلك الحين كان التقدم بطيئًا، لكنه أخذ في التسارع بعد انتهاء الحرب الباردة. ولعل إنشاء معهد قانون الفضاء السيبراني في جامعة جورج تاون الأمريكية عام 1995 كان مؤشرًا لإدراك المشكلة. وقد اتجهت الدول إلى تبني العديد من المبادرات على المستوى الوطني أو الثنائي أو الإقليمي أو الدَّولي، من أجل العمل على حماية البنية التحتية الكونية للمعلومات من خطر التعرض للتهديدات السيبرانية، وعملت على إيجاد أُطُر تشريعية جديدة تتعامل مع تلك الظاهرة المستحدَثة بصياغة مفهوم جديد للأمن الوطني، ثم الاتجاه إلى التعاون الدَّولي.

ومن حُسن الحظ أن العالم يدرك مخاطر جرائم الإرهاب الإلكتروني ويسعى لمواجهتها والتصدي لها؛ بتبني إستراتيجية دَولية في مجال تأمين الفضاء الإلكتروني، عبر جملة من القوانين والمبادرات أهمها مبادرة الشراكة الدَّولية المتعددة الأطراف لمكافحة الإرهاب الإلكتروني IMPACT التي تهدف إلى حشد الجهود الدَّولية للقطاعات الحكومية والقطاع الخاص والمجتمع المدني لمواجهة التهديدات المتزايدة للإرهاب الإلكتروني، وجمع الرؤى والأفكار عن التدريب وتبادل الخبرات، وإنشاء الكثير من مواقع الإنترنت لمكافحة ذلك الإرهاب، وحماية الأمن الإلكتروني. وقد كانت تلك المواقع نقطةَ التقاء لخبراء أمن المعلومات والسياسيين؛ من أجل التباحث بشأن ماهية خطر الإرهاب الإلكتروني، وكيفية مواجهته، مثل مجموعة "SITE" للاستخبارات، التي تُعَد جهازَ استخبارات متخصصًا في رصد الإرهاب عبر الإنترنت، ودراسة المصادر الأولية للإرهابيين، ورصد أحاديثهم ومراقبة دعاياتهم.

وقدم باري كولين في ورقته المشار إليها آنفًا قائمةً بالعناصر التي يجب توافرها عند إنشاء برنامج مكافحة الإرهاب الإلكتروني، وهي:

- بناء فريق مكافحة الإرهاب الإلكتروني في الوقت المناسب، وبمرونة فائقة.

- تغيير الطريقة التي نتعامل بها مع مكافحة الإرهاب الإلكتروني.

- التعاون ومشاركة المعلومات الاستخباراتية بطرق جديدة.

- الاستعانة بالأفراد الذين يفهمون الحرب التي نواجهها.

- معرفة القواعد الجديدة والتقنيات الجديدة واللاعبين الجدد، فبخلاف الإرهابيين التقليديين، إذا خسر الإرهابي الإلكتروني اليوم، فهو لا يموت بل يتعلم ويزداد خبرة مما لم ينجح فيه، وسيستخدم ما تعلمه في محاولة جديدة ناجحة مستقبلًا.

وتضيف كلٌّ من سوهانيا بونوسامي وغيثا روباسندرام في بحثهما (دراسة دَولية في مخاطر الإرهاب الإلكتروني) (An International Study on the Risk of Cyber Terrorism) المنشور في يناير 2019 عناصرَ أخرى ضروريةً لمواجهة الإرهاب الإلكتروني هي:

- إيجاد إطار دَولي منسق وقوي لمكافحة الإرهاب الإلكتروني تتوافق عليه الحكومات والهيئات التنظيمية؛ لتكون قادرةً على تبادل المعلومات الاستخباراتية وغيرها من أشكال التعاون.

- توفير قدر أكبر من التعليم لمؤسسات القطاعين العامِّ والخاصِّ؛ لتقوم بتطوير التقنيات المستخدمة التي قد تكون عُرضةً للإرهاب السيبراني، والتأكد من أن عنصر الأمن في صدارة الاهتمام عند إنشاء الأنظمة الجديدة، للحد من نِقاط الضعف التي قد تواجهها.

- تطوير تقنية آمنة تكون قادرةً على تحديد الأنشطة المشبوهة بوساطة تحليل البيانات العامة والخاصة، وجعل الحواسيب وأنظمتها أقلَّ عرضة للخطر.

تحدِّيات عاصفة

تزداد تهديدات الإرهاب الإلكتروني مع ازدياد انتشار مستخدمي (الإنترنت) باستمرار واطِّراد. ومع النموِّ السريع لتقنيات الحواسيب، وعلى الرغم من أن الحكومات صعَّدت من الإجراءات الأمنية لمواجهة تلك التهديدات، ومن ذلك المراقبة عبر (الإنترنت)، إن هناك العديد من العقبات التي تواجه ذلك المسعى، منها أن أكثر الشركات والتطبيقات تستخدم التشفير لحماية خصوصية مستخدميها، ويتنقل الإرهابيون بين المنصَّات والتطبيقات التي توفر لمستخدميها أعلى درجات الحماية والتشفير.

وتكاد تُجمع التقارير على زيادة عدد مستخدمي شبكة (الويب) المظلمة والعميقة The Onion Router مقارنةً بالمتصفحات الأخرى؛ بسبب مخاوف الخصوصية وتفضيلات الهوية المجهولة، وهذا ممَّا يزيد من خطر الإرهاب الإلكتروني. ويتصاعد قلق مستخدمي (الإنترنت) ومعه ضغوط منظمات المجتمع المدني في مواجهة التشريعات الصارمة التي تصدرها الحكومات لمحاربة الإرهاب على الشابِكة؛ بحجة حماية الخصوصية وحرية تدفق المعلومات. وعندما أعربت أمبر رود وزيرة الداخلية البريطانية، عن اعتزامها تغيير القانون؛ لزيادة عقوبة السجن من 10 سنوات إلى 15 سنة للأشخاص الذين يشاهدون باستمرار المحتوى الإرهابي على (الإنترنت)، قوبلت باعتراضات كبيرة.

وفي ظل العدد المتزايد من مستخدمي (الإنترنت) في أرجاء العالم لذي بلغ أكثر من 4.5 مليار مستخدم، وافتقار أكثرهم إلى الوعي الأمني، وزيادة الاعتماد على الاتصالات عبر الشابِكة في تقديم الخِدْمات، تزداد صعوبات مكافحة تهديدات الإرهاب الإلكتروني، وتتأكد حتمية مواجهة تلك التهديدات في آن واحد.

أجل إن القطاعات الحكومية في جميع أنحاء العالم أطلقت أنظمةً وبرامجَ وسياساتٍ وقوانينَ صارمةً وإجراءاتٍ أخرى مختلفة، من أجل مكافحة تلك التهديدات، لكنها تظل معركةً صعبة تحتاج باستمرار إلى التحديث والمراقبة، ولا سيَّما مع تطور التهديدات ونموها، وتأثيراتها السلبية على الحكومات والشركات والأفراد من جهة أعمالهم ومعلوماتهم وخصوصياتهم وأمنهم.