تهـديد الإرهـاب السيبراني

وإمكانية تطبيق اتفاقية الجرائم السيبرانية

د. سُني ذو الهدى

باحث إندونيسي وأستاذ مشارك، كلية أحمد إبراهيم للقانون، الجامعة الإسلامية العالمية في ماليزيا.

مع التقدُّم التقني الكبير المعاصر في مجال المعلومات والاتصالات عبر الإنترنت، صار من السهل جدًّا توظيفُ المجرمين والإرهابيين لهذه التقنيات المتطوِّرة في وضع خُططهم الإجرامية والإرهابية وتنفيذها والترويج لها. حتى غدت هذه الوسائلُ العصرية تحدِّيًا جِدِّيًّا خطِرًا يهدِّد المجتمع الدَّولي بأسره.

ويرى الدكتور ناه ليانغ توانغ أستاذُ الدراسات الدَّولية في كلية راجاراتنام في سنغافورة أن هذا التقدُّمَ التقني إنما هو سيفٌ ذو حدَّين؛ فعلى حين يمكن أن يُستخدمَ الحدُّ الأول خطَّ دفاع في وجه الجريمة والإرهاب، فإن الحدَّ الآخر يُستغَل لاقتراف الجريمة وممارسة الإرهاب. إذ إن التقنية المتقدِّمة من مثل تشفير الهواتف الذكية، وإنترنت الأشياء، وانتشار شبكات الحواسيب في القطاعات الحيوية الكافة ولا سيَّما الأمنية والعسكرية منها، وفي الخِدْمات العامَّة الحيوية، تُتيح الكثيرَ من المزايا العملية؛ ولكنها في الوقت نفسه تفتح البابَ على مِصراعَيه للتهديدات السيبرانية الخطِرة، وتتسبب بنشوء نِقاط ضعف سيبرانية .

وتهدف هذه المقالة إلى تحليل طبيعة الإرهاب السيبراني وبيان نطاقه، وتسليط الضوء على آخر التطوُّرات في المبادرة الدَّولية للإجراءات القانونية المضادَّة لهذا التهديد الأمني العالمي، وتولي اهتمامًا خاصًّا باتفاقية الجرائم السيبرانية.

خطر الإرهاب السيبراني

أكَّد تقريرُ المخاطر العالمية لعام 2019م الصادرُ عن المنتدى الاقتصادي العالمي، أن الإرهاب السيبراني بات واقعًا لا مَهربَ منه. ويصف التقرير الهجَماتِ السيبرانيةَ أو البرمجيات الخبيثة بأنها تلك الهجَماتُ التي تتسبَّب في أضرار اقتصادية كبيرة، أو اضطرابات جيوسياسية، أو مشاهدَ ومواقف تتصدَّع فيها الثقةُ بشبكة الإنترنت على نطاق شاسع. وتتمثَّل الهجَماتُ الإرهابية واسعة النطاق بأفراد أو جماعات غير الحكومية ذات أهداف سياسية أو دينية أو اجتماعية تهدف إلى إلحاق أضرار بشرية أو مادِّية واسعة النطاق والأثر.

وكشف تقريرُ المنتدى الاقتصادي العالمي أيضًا عن مخاطرَ عميقة للهجوم الإرهابي السيبراني؛ إذ له صلةٌ وثيقة بانهيار البِنية التحتية للمعلومات المهمَّة، وخطر إطلاق أسلحة الدمار الشامل. ولا سيَّما أننا نعيش اليوم في عالم مترابط إلى حدٍّ كبير ومتَّصل الأجزاء، تجري فيه (رقمنة) المزيد والمزيد من البِنى التحتية

الحيوية للبيانات، ومن ثَم يزدادُ الاعتماد عليها باطِّراد. وهكذا أصبح الإرهاب السيبراني يحظى بشعبية كبيرة في ازدياد مطَّرد؛ نظرًا لسهولة استخدامه، وإمكانية تحمُّل كلفته، ولا يتطلب من الإرهابيين الحصول على أسلحة تقليدية باهظة الثمن، ولا نقلها إلى الموقع المراد، كما لا تَثْني قيودُ الزمان والمكان الإرهابيين عن بطشهم؛ إذ يمكنهم شنُّ الهجَمات في الواقع الافتراضي من أي مكان، وفي أي وقت، إضافةً إلى سهولة إمكانية الاختباء والتخفِّي وراء حجاب التقنية .

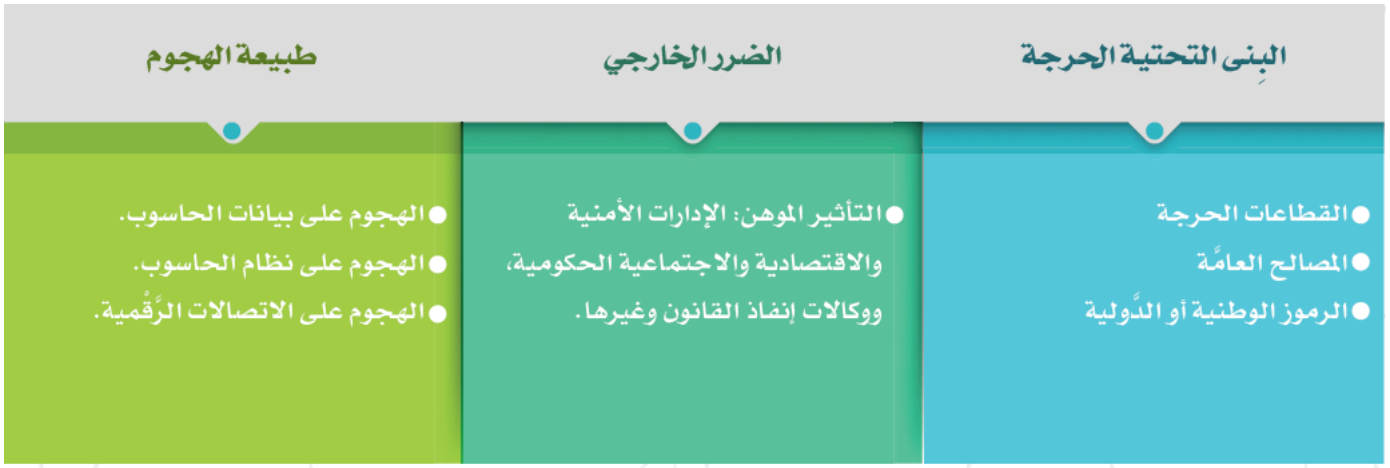
وبذلك يمكن أن يكونَ الأثر ضخمًا ومخيفًا، اعتمادًا على الهدف المراد تحقيقه. وتتعدَّد طرائق العمل من استعمال البرامج التخريبية الخبيثة و(فيروسات) البرامج، إلى حجب الخِدْمات، والأعمال الاستخباراتية التجسُّسية على الشبكة وغيرها.

نطاق الإرهاب السيبراني

ولكنَّ السؤال الذي يُلحُّ هنا هو: ما الإرهابُ السيبراني؟ يعرِّف فورنيل ووارين الإرهابَ السيبراني بأنه استخدامُ الجماعات الإرهابية السيبرانية للفضاء السيبراني. وهذا يشير إلى الانتقال من الإرهاب التقليدي الذي يعتمد على الوسائل المادِّية (من أسلحة وذخائرَ وغيرها) إلى الإرهاب الحديث الذي يعتمد اعتمادًا أكبر على التقنيات غير المرئية. ويعرِّف جيمس لويس الإرهابَ السيبراني بأنه: استخدامُ أدوات الشبكة الحاسوبية لتدمير أو تعطيل البِنى التحتية الوطنية المهمة؛ مثل الطاقة، والنقل، والعمليات الحكومية، بهدف إكراه أو ترهيب الحكومة أو المدنيين.

ويمكن من هذا التعريف وصفُ الإرهاب السيبراني بالنظر إلى جانبين اثنين، هما :

الجانب الأول: أهمية عنصر "التهديد السيبراني"، وهو الهجومُ الذي يهدف إلى تدمير البيئة السيبرانية (أنظمة الحواسيب) أو تعطيلها، ما يؤدِّي إلى الخوف من انتشار خطط الإرهابيين وأفكارهم، أو الهجوم على الأنظمة العسكرية، وعلى البِنية التحتية الحيوية للمعلومات الخاصَّة بدولة ما. كما هو موضَح في الشكل:(1)



الشكل (1) نطاق الإرهاب السيبراني، الجانب الأول (الهجوم على النظام)

الجانب الثاني: أهمية عنصر "مكان الإعداد"، وهو المكان الذي يجري فيه اختراق النظام السيبراني ليكونَ وسيلةً للهجوم، وذلك عندما يستخدم الإرهابيون الإنترنت أو أنظمة معلومات واتصالات؛ نحو إنترنت الأشياء، والأجهزة المتنقلة، والذكاء الاصطناعي، والبيانات الضخمة، والتشفير، والبرمجيات الآلية، بغرض التخطيط والإعداد وشنِّ هجَمات إرهابية مؤثرة. وفي هذا السياق يصفُ بيتر غرابوسكي طريقةَ توظيف تقنية المعلومات الواسعة، وسيلةً لتسهيل الإرهاب، ومن ذلك قرصنة المعلومات الاستخباراتية، واستخراج البيانات، وجمع الأموال، والتوظيف والتعبئة والتدريب عن بعد، مثل التدريب على استخدام تقنية الهجوم ومهاراته، ومشاركة المعلومات، ونشر الأدلة، مثل أدلة صنع الأسلحة وغيرها، كما هو موضح في الشكل:(2)

الشكل (2) أنواع الإرهاب السيبراني، الجانب الثاني

وقد ازداد ظهورُ الجانب الثاني من أنشطة الإرهاب السيبراني بوضوح في ماليزيا في العِقد الماضي، ورُفعت دَعاوى قضائية بموجب قانون العقوبات في البلاد.

وتُصنف الأحكام تحت الرقم (ج-031) والرقم (ي-031) مختلِف الأعمال المرتكَبة في سياق الأعمال الإرهابية، على سبيل المثال: تجنيد الأشخاص للانضمام إلى الجماعات الإرهابية، أو للمشاركة في الأعمال الإرهابية، أو الترويج لها والإغراء بها، وتوفير التدريب والتعليم للجماعات الإرهابية، وتلقِّي التدريب من تلك الجماعات، وتوجيه أنشطتها الفاسدة المؤذية، والتماس دعم الجماعات الإرهابية.

مبادرة مكافحة الإرهاب السيبراني

إن الإرهاب السيبراني يُشكل خطرًا عالميًا ومشكلةً دَولية تتطلَّب حلًّا عالميًّا من جميع الدول، ولقد قال الأمين العامُّ للأمم المتحدة سابقًا بان كي مون: إن الإنترنت مثالٌ رئيسٌ على تصرُّف الإرهابيين بطريقة عابرة للحدود. لذا تحتاج الدول إلى التفكير والعمل معًا عبر الحدود الوطنية، بالرغم من وجود القوانين والسياسات المحلِّية بشأن الإرهاب السيبراني، فإننا بحاجة ماسَّة إلى الاستجابة لهذا الخطر العالمي، بتآزر الجهود وتكاملها دَوليًّا. ومن هنا انطلقت مبادرات دَولية لمعالجة خطر الإرهاب السيبراني. فأصدر مكتب الأمم المتحدة المعني بالمخدِّرات والجريمة عام 2012م بالتعاون مع فرقة العمل المعنية بمحاربة الإرهاب التابعة للأمم المتحدة تقريرَ عمل يتعلَّق بالإرهاب السيبراني .

ومما يبعث على القلق قلّةُ التدريب المتخصِّص في الجوانب القانونية والعملية للتحقيق والمقاضاة في قضايا الإرهاب التي تنطوي على استخدام الإنترنت. لذلك يهدف مكتب الأمم المتحدة المعنيُّ بالمخدِّرات والجريمة إلى تطوير الموارد المتعلِّقة بمكافحة الإرهاب والجريمة السيبرانية؛ لمكافحة هذا التهديد المتطوِّر. ويشدِّد المكتب على أن هناك بعضَ العوامل الأساسية والضرورية في تحديد الاستجابة الدَّولية لتدابير مكافحة الإرهاب، من ذلك :

1. الأُطر السياسية والتشريعية المشتركة .
2. التحقيقات وجمع المعلومات الاستخبارية .
3. التعاون والتآزر الدَّولي .
4. المقاضاة والملاحقة القانونية .
5. تعاون القِطاع الخاص مع الجهات الحكومية .

وتعتمد جميعُ هذه العوامل الأساسية على الالتزام المشترك بين البلدان لمواجهة التهديدات الإرهابية ومكافحتها داخل حدودها الوطنية وخارجها .

اتفاقية الجرائم السيبرانية

هي إحدى الاتفاقيات العالمية المهمَّة، كونها الاتفاقيةَ الدَّولية الوحيدة المتعلِّقة بالإرهاب السيبراني. ونجد أن هذه الاتفاقية مع أنها لا تعالج الإرهابَ السيبراني على وجه التحديد، فقد صيغت بطريقة قادرة على تتبُّع نطاق تهديدات الإرهابيين، لتشملَ جريمة الإرهاب السيبراني.

وأفضل استجابة لمعالجة خطر الإرهاب السيبراني هي تعديل الاتفاقية وإدراج جرائم الإرهاب السيبراني بصورة محدَّدة فيها وبدقة أكبر. ويمكن القول: إن التحدِّيَ الأكبر في إشراك المزيد من البلدان لجعل الاتفاقية أداةً عالمية ودَولية لمكافحة هذا الصِّنف من الجرائم .

وقد أصدرت لجنةُ اتفاقية الجرائم السيبرانية عام 2016م مذكرةً توجيهية تتعلَّق بجوانب الإرهاب السيبراني بموجب اتفاقية بودابست، تعلن فيها أن "الجرائم الموضوعية في الاتفاقية قد تكون أيضًا أعمالًا إرهابية على النحو المحدَّد في القانون المعمول به". وتأتي هذه المذكِّرة الإضافية بموجب الاتفاقية في الوقت المناسب، وتسلِّط المذكِّرة الضوء على أن هذه الاتفاقيةَ ليست معاهدةً مختصَّة بالإرهاب، إلا أنه يمكن القول: إن الجرائم الموضوعية في الاتفاقية يمكن أن تنفَّذَ على أنها أعمال إرهابية، لتسهيل الإرهاب ولدعم الإرهاب، ومن ذلك الجانبُ التمويلي، أو الأعمال التحضيرية .

وإضافة إلى ذلك فإن أدواتِ المساعدة القانونية الإجرائية المتبادلة على الصعيد الدَّولي الواردة في الاتفاقية متاحةٌ للتحقيقات والملاحقات القضائية المتعلِّقة بالإرهاب. وبموجب الاتفاقية يعتمد كلُّ طرف على ما قد يلزم من تدابيرَ تشريعيةٍ وتدابيرَ أخرى لتحديد الصلاحيات والإجراءات؛ لغرض إجراء تحقيقات أو إجراءات جنائية محدَّدة، مع العلم أن هذه الصلاحيات والإجراءات لا تنطبق على الجرائم الإلكترونية المحدَّدة فحسب كما هو مذكور في الاتفاقية، ولكنها تنطبق أيضًا على "الجرائم والانتهاكات السيبرانية الأخرى المرتكَبة بواسطة أنظمة الحواسيب. لذلك، وفقاً للمذكرة التوجيهية لعام 2016م، يمكن أن

يؤدِّي ذلك إلى توسيع نطاق تطبيق اتفاقية الجرائم السيبرانية على أي جريمة إرهابية، طالما أنها ترتكب عن طريق أنظمة الحواسيب .

مع هذا التمديد، قد يرى أحدهم بأن كونه طرفًا في الاتفاقية فإن هذا سيكون مصدرًا مهمًا لتقديم الدعم والمساعدة للدولة في معالجة الإرهاب السيبراني ضمن ولايتها القضائية، مشيرًا إلى أن هذه الدولة ستكون مؤهلة لتبادل الدعم والمساعدة والتعاون بين الدول الأعضاء. ويتعيَّن أولًا على الأطراف (في الاتفاقية) تقديمُ المساعدات المتبادلة فيما بينهم على أوسع نطاق ممكن؛ وذلك لأجل التحقيقات أو الإجراءات المتعلِّقة بالجرائم والانتهاكات السيبرانية ذات الصلة بأنظمة الحواسيب والبيانات، أو لجمع الأدلَّة بصورة إلكترونية لجريمة جنائية. وهذا يعني أيضًا أن الطرفَ في الاتفاقية سيحصل على نصيبه العادل من التعاون الدَّولي، وسيُسمح للطرف بالحصول على المساعدة المتبادلة حتى في غياب الاتفاقيات الدَّولية السارية بين الدول.

ختامًا

نستنتج أن الإرهاب السيبراني هو شكلٌ جديد من أشكالِ العمل الإرهابي، وغالبًا ما يكون له تأثيرٌ كبير، ولكن سياساتِ كثيرٍ من السلطات القضائية وتشريعاتها لا تزال تنأى بنفسها عن هذا الصنف من الإرهاب على أهميته وتأثيره وخطره .

إن الإرهاب السيبراني بات خطرًا عالميًّا يتطلَّب استجابةً دَولية وتعاونًا أمميًّا، والحاجة ملحَّة إلى سياسة مشتركة وإطار تشريعي مشترك، يضعان الحدَّ الأدنى من المعايير وأفضل الممارسات لمواجهته. ومن الضروريِّ تضافرُ الجهود في جمع المعلومات الاستخبارية وتبادلها. وإن التعاون الدَّولي في التحقيقات والملاحقات القضائية، فضلًا عن التعاون بين القِطاعين العام والخاص أمرٌ قد بلغ الغاية في الأهمية.