كورونا وانتشـار الهجَــمـات السِّيبرانية الإرهابية

سني ذو الهدى

أستاذ مساعد بكلية أحمد إبراهيم للحقوق – الجامعة الإسلامية العالمية بماليزيا.

منذ أعلنت منظمةُ الصحة العالمية في مارس 2020 م أن فيروس كورونا المستجدَّ «كوفيد »19 بات جائحةً عالمية، زاد الحذرُ من انتشار المرض والحرصُ على احتوائه، فعمَد كثيرون إلى استخدام الشبكات الإلكترونية للحصول على معلومات أكثر عن الجائحة، وانشغل آخرون بمشاركة الرسائل على مواقع التواصل الاجتماعي. وصارت الأنشطةُ الإلكترونية مثل إقامة اجتماعات عبر الإنترنت أو التعلُّم من بُعد، أو مشاركة المقاطع المصوَّرة، عادةً جديدة، ولا سيَّما في مرحلة الحَجْر التي فرضتها كثيرٌ من الدول.

أمن الفضاء السِّيبراني

مع تفاقُم الخوف والقلق الاجتماعي من الجائحة، ومن إجراءات الحَجْر الصارمة، بات هذا الهلعُ سببًا في ظهور تصرُّفات خطِرة غير منطقية، وينطبق هذا أيضًا على أمن الفضاء السِّيبراني. فقد اضطُرَّ مئاتُ الملايين من الأشخاص إلى العمل أو الدراسة من المنازل، وبذلك أصبح الفضاءُ السيبراني مساحةً مغرية للقراصنة والإرهابيين السيبرانيين ليعيثوا في الأرض فسادًا .

هذا ما تؤكِّده الأخبارُ والتقارير التي تفيد بظهور كثير من الممارسات المسيئة، والهجَمات الإلكترونية في الفضاء السيبراني في أثناء الجائحة. وأشارت منظمةُ الصحة العالمية في أبريل الماضي إلى أن عدد الهجَمات السيبرانية المستهدِفة للهيئات الدَّولية قد ارتفع إلى خمسة أضعاف. وتجاوزت نسبةُ التهديدات السيبرانية في ماليزيا 80%، ووصل عددُ الهجَمات السيبرانية في إندونيسيا إلى 88 مليون هجومًا من يناير إلى أبريل 2020م. وصرَّحت الهند بارتفاع عدد الهجَمات الأمنية السيبرانية المدعومة من الدول المستهدِفة للهيئات الحكومية في أثناء هذه المدَّة. كل ذلك يؤكِّد أن أزمة كورونا سببٌ رئيس في انتشار الهجَمات السيبرانية.

اكتشاف مواطن الضعف

يمكن النظرُ إلى الارتفاع الكبير في الهجَمات السيبرانية التي تؤثِّر في المنظمات والأفراد على حدٍّ سواء أنه إنذارٌ بالخطر تجاه العاملين في مكافحة الإرهاب. فهذا الارتفاعُ يدلُّ على مواطن ضعف في البنية التحتية للمعلومات المتصلة بالشؤون العامَّة أو الخاصَّة للدولة (مثل الإنترنت والبيانات الضخمة) التي تستغلُّها المنظمات الإرهابية لشنِّ هجَماتها السيبرانية. ويؤكِّد الدكتور أليكس شميد من المركز الدَّولي لمكافحة الإرهاب (ICCT) في لاهاي أن نموَّ المنظمات الإرهابية في الوقت الحاضر يُعزى إلى كثير من

العوامل، ومنها الآثارُ الناتجة عن العولمة، مثل تحرير الأسواق المالية، والخِدْمات المصرفية الخارجية والإلكترونية، واستغلال شبكات الإنترنت في أغراض مسيئة.

ولطالما كانت المنظماتُ الإرهابية والجماعات الإجرامية السيبرانية تتقصَّد استغلالَ مواطن الخلل أو الضعف في أنظمة الحوكمة، وهذا ما دفع الحكومةَ الأمريكية إلى التصريح بأنها لن تسمحَ للجماعات الإجرامية باستغلال هذه الجائحة لتهديد حياة الأمريكيين. ومن المؤكَّد أن هؤلاء الإرهابيين يحرِصون على الاستفادة من الضغوط الناتجة عن الجائحة الواقعة على كاهل مؤسَّسات الدولة؛ لاستغلال الفجَوات الأمنية الناشئة التي تتعرَّض لها البنيةُ التحتية للفضاء السيبراني، لتحقيق مصالحهم وأهدافهم التخريبية والإرهابية.

استغلال الفضاء السِّيبراني

يستغلُّ الإرهابيون شبكات الإنترنت بشتَّى الوسائل، وهناك أسبابٌ رئيسة لزيادة استغلال الإرهابيين الفضاءَ السيبراني في أثناء جائحة كورونا، نظرًا لتوافُر العوامل التي تسهِّل هذا الاستغلال، ومن أهمِّها:

أولًا: عطَش الناس إلى المعلومات؛ إذ يحرِصُ كثيرٌ منهم على تحصيل مزيد من المعلومات عن الجائحة.

إن سلوك الأفراد في التعامل مع الإنترنت يتغيَّر في أثناء الجوائح؛ لأنهم يصبحون أكثرَ حرصًا على الحصول على المعلومات ونشرها، ويكونون أكثرَ قابلية للنقر على أيِّ روابطَ أو مصادرَ في الويب. والواقع أن المجرمين والإرهابيين السيبرانيين يتكيَّفون مع هذا السلوك الطارئ بسرعة، وينتهزون الفُرَص لنشر البرامج الخبيثة؛ باستغلال الروابط غير المرخَّصة، أو الرسائل الإلكترونية المزيَّفة، أو الرسائل المضلِّلة .

ثانيًا: العمل من بُعد (في المنازل) يُتيح للمجرمين السيبرانيين استغلالَ أنظمة الحواسيب غير المحميَّة.

إن قوانين التباعُد الاجتماعي الجديدة والحظر والعزل الذاتي قد أرغمَت ملايينَ الأشخاص على العمل والدراسة من منازلهم، باستخدام حواسيبَ أقل حمايةً، وفي بيئة أقل دعمًا من الناحية الفنية، مقارنةً بمرافق العمل المثالية المتوافرة، والدعم الفنِّي المقدَّم قبل الجائحة .

ثالثًا: استخدام تطبيقات خارجية في مدَّة الحجر، ولا سيَّما التطبيقات غير المرخَّصة .

إن الاستخدام الزائدَ لمنصَّات إلكترونية خارجية مثل مواقع التواصل الاجتماعي، ومنصَّات الاجتماعات الإلكترونية، والخِدْمات السَّحابية التي لا تجدُ الحمايةَ الكافية، أو التي تكون خارجَ نطاق سيطرة صاحب العمل، يؤدِّي إلى مواجهة كثير من المخاطر الأمنية الحسَّاسة، ويتسبَّب في كثير من المشكلات الأمنية الأخرى.

جائحة كورونا والإرهاب

من الأسئلة الملحَّة في هذا الشأن، هل تُتيح جائحة كورونا المجالَ لانتشار الهجَمات الإرهابية؟ وللإجابة عن هذا السؤال ينبغي النظرُ في عدَّة أمور:

1 (يحرِصُ الإرهابيون دائمًا على استغلال مواطن الضعف في الفضاء السيبراني. وقد أدَّت العاداتُ الجديدة

التي ظهرت في مدَّة الحَجْر إلى إقبال كثيرين على الفضاء السيبراني، ومن ثمَّ بات من السهل إخفاء هُويَّة الإرهابيين، أو بعض الأنشطة الإرهابية في الفضاء السيبراني، نظرًا للزيادة الكبيرة في الاعتماد على شبكات الإنترنت .

2 (ليس ثمةَ أيُّ مؤشِّرات لتراجع نشاط الإرهاب السيبراني في أثناء الجائحة، وأشارت عدَّة تقاريرَ إلى أن الإرهابيين بدؤوا يسخِّرون كلَّ ما لديهم للاستفادة بأقصى درجة ممكنة من هذه الأزمة الوبائية، وذكر رئيسُ قوات حفظ السلام التابعة للأمم المتحدة في أوائل يونيو 2020م أن جائحة كورونا تفرض كثيرًا من التحدِّيات الأمنية المعقَّدة في منطقة الساحل وإفريقيا؛ لأن الجماعات الإرهابيةَ تبذل كل ما في وسعها للاستفادة من الجائحة بشنِّ هجَمات على القوى الوطنية والدَّولية. وتشير عدَّة مصادرَ إلى أن الإرهابيين يستفيدون من المشقَّة التي تفرضها الجائحةُ؛ لتقويض سلطات الدولة وزعزعة استقرار الحكومات.

3 (يستهدف كثيرٌ من الهجَمات السيبرانية البنيةَ التحتية الحرجة للمعلومات (الخِدْمات الحيوية أو الخِدْمات الأساسية)، التي تُعَدُّ مصدرًا أساسيًّا للحفاظ على الوظائف الاجتماعية الضرورية، أو على الجانب الصحي أو الاقتصادي أو الرفاهية الاجتماعية. وإذا ما عُطِّلت هذه البنيةُ فإن ذلك يخلِّف أضرارًا جمَّة؛ لعدم القُدرة على حماية هذه الوظائف والحفاظ عليها .

أمثلة من الواقع

من الأمثلة على هذه الهجَمات التي تستهدف البنيةَ التحتية الحرجة للمعلومات، ما حصل في جمهورية التشيك عندما شنَّت جماعةٌ إرهابية هجومًا إلكترونيًّا على نظام الحواسيب لأحد المستشفيات الجامعية في مدينة برنو، ما تسبَّب في تعطيل أحد أكبر مختبرات فحص فيروس كورونا في الجمهورية. وتسبَّب برنامج الفِدية الذي استهدف نظامَ معلومات إدارة الصحة العامَّة في مدينة تشامبين بمقاطعة إلينوي بالولايات المتحدة، في التهديد بتعطيل نظام الصحة العامَّة المستخدَم لإدارة المعلومات المتعلِّقة بجائحة كورونا .

وذُكر في تايوان أن شركة الطاقة المملوكة للدولة قد تعرَّضت لهجوم برنامج الفِدية. وذكرت شركةُ الاتصالات اليابانية أن بعض المجرمين اخترقوا شبكتها الداخلية وسرقوا بيانات 621 عميلًا. وحذَّرت بعضُ المصادر من أن البنية التحتية الحرجة لألمانيا معرَّضة لخطر القرصنة الروسية. وفي إندونيسيا تعرَّض اجتماعٌ رفيع المستوى عبر الإنترنت للمجلس الوطني لتقنية المعلومات إلى التخريب على يد مخترق قام بالاطِّلاع على الملفَّات غير اللائقة والمسيئة للمشاركين الآخرين. وقد تسبَّبت هذه الحادثةُ في كثير من الحرج، وأثارت ضجَّةً كبيرة بين المشاركين، وعرَّضت المعلومات الحسَّاسة التي نوقشت في الاجتماع إلى خطر تسريبها.

وتؤكِّد جميعُ هذه الحوادث أن البنيةَ التحتية الحرجة للمعلومات تستهدفها الهجَماتُ السيبرانية بإحكام في أثناء الجوائح التي يمكن أن تكونَ خطوةً أولى لشنِّ المزيد من الهجَمات الإرهابية.

حوكمة المعلومات

إن أبرز عوامل الخطر الناتجة عن تفشِّي فيروس كورونا المستجدِّ أدَّت إلى نشوء كثير من مواطن الضعف

التي تقدِّم بيئةً جاذبة للهجَمات الإرهابية. ويؤكِّد شميد في تحليله أن المنظماتِ الإرهابيةَ تحتاج إلى تمويل هجَماتها من مختلِف المصادر، وأن ازدحام الفضاء السيبراني من شأنه أن يكونَ مصدرًا تمويليًّا ممتازًا، وفرصة سانحةً لسرقة البيانات، والابتزاز، وإقامة مخططات احتيال إلكترونية، وخرق المرافق المصرفية عبر الإنترنت .

فضلًا عن ذلك يستغلُّ الإرهابيون شبكات الإنترنت للترويج لأهدافهم الفكرية والسياسية، واستقطاب الأفراد، واستمالة قلوبهم، وتعزيز غاياتهم. ولذلك يحرِصون على توسيع شبكاتهم عبر الإنترنت؛ لما في ذلك من فوائدَ تُسهم في تحقيق مصالحهم، ويمكن استغلالُ انتشار وسائل الإعلام لخدمة هذا الغرض.

وتؤكِّد عمليات شنِّ الهجَمات الإلكترونية على البنية التحتية الحرجة، قوةَ إصرار هذه الجماعات على إلحاق الضرر بأهدافها، ومواصلة أعمالها الإرهابية، وكلُّ ذلك يمكن أن يتحوَّل إلى تهديد إرهابي سيبراني خطِر.

إن جائحة فيروس كورونا المستجد تفرضُ صعوبات على الأفراد والحكومات في تفادي التهديدات الإرهابية، وهناك حاجة ماسَّة إلى تطوير إطار شامل لحوكمة المعلومات، وبذل جهود مستمرَّة لضمان سلامة الفضاء السيبراني وأمنه ومتانته. وقد أدَّت التبِعاتُ المدمِّرة لجائحة كورونا إلى تفاقُم هذه التهديدات المستعصية، ممَّا يوجب على المسؤولين عن البنية التحتية الحرجة للمعلومات أو الخِدْمات الضرورية، والجهات الحكومية والمنظمات الخاصَّة؛ تقوية تدابيرهم الأمنية والوقائية وتدابير الحماية والاستجابة؛ لتفادي التهديدات الإرهابية والحدِّ منها. ويجب أن يستندَ ذلك إلى أساس ثابت لحوكمة المعلومات، وأن يكون متوافقًا مع الجوانب القانونية والتقنية.