مركز الجزيرة للدراسات
ALJAZEERA CENTRE FOR STUDIES

تقارير

قتال غير مرئي: الحرب السيبرانية في الأزمة الخليجية

محمد الدوراني*

ترجمة: كريم الماجري**

13 مايو/أيار 2018

Al Jazeera Centre for Studies
Tel: +974-44663454
jcforstudies@aljazeera.net
http://studies.aljazeera.net

هجوم سيبيري تمهيدًا لإجراءات الحصار (رويترز)

مقدمة

بات شنُّ هجمات سيبرانية وباءً منتشرًا على نطاق واسع بين البلدان الساعية للانتقام أو تلك التي تتبنى أجندة عدائية ضد بلد آخر. وأصبح تشويه الوقائع، وتقديمها على أنها حقيقة، أمرًا واقعًا عبر اللجوء إلى استخدام التكنولوجيا، خاصة في مجال القرصنة ووسائط التواصل الاجتماعي(1)، حيث تسعى دولة ما إلى شن هجمات سيبرانية عبر توظيف وسائط التواصل الاجتماعي على نطاق واسع لرمي دولة أخرى بتهمة الإرهاب، أو تصويرها كدولة معتدية أو وصفها بأي وصف آخر مشين بهدف خدمة أجندة خاصة. بات هذا السلوك -شن هجمات إلكترونية- تقليدًا دوليًّا، وقد وقعت بلدان مجلس التعاون الخليجي، التي تتشارك شعوبها قواسم مشتركة، في براثن هذا الشَّرَك بشكل فاق كل ما هو متعارف عليه في مثل هذا المجال. فعندما تشعر دولة، أو مجموعة من الدول، بأن دولة جارة في مجلس التعاون الخليجي لا تسير في ركابها ولا تتبع نفس نهجها فإنها تعلن ضدها حربًا من نوع خاص. تلك هي الحرب التي نشهدها اليوم متمثلة في الحصار الحالي لقطر والذي تفرضه ثلاث من دول مجلس التعاون الخليجي، هي: السعودية والإمارات والبحرين، بالإضافة إلى مصر. وبالرغم من أن مصر ليست عضوًا في مجلس التعاون الخليجي إلا أنها التحقت بالثلاثي الخليجي بسبب الخصومة بين النظام العسكري الجديد ودولة قطر.

لماذا تكتسي هذه الحرب طابعًا خاصًّا؟ في الواقع، يجب أن يكون كاتب سيناريو هذه الحرب ملمًّا جدًّا بالممارسات الغربية، وغيرها من البلدان، التي أُعدَّت فيها وانطلقت منها تلك الحروب. فحتى هوليوود كانت قد أنتجت الكثير من الأفلام التي تعرض كيفية شن الحروب وإسقاط الحكومات.

في حالة قطر، كان السيناريو يتطلب أكثر من فصل أو جزء؛ حيث كانت البداية أولًا مع القمة الإسلامية المنعقدة في الرياض، التي حضرها الرئيس الأميركي، دونالد ترامب، في أول زيارة خارجية له قادته إلى عاصمة المملكة العربية السعودية. وبالتنسيق مع الولايات المتحدة الأميركية، دعت السعودية كل الزعماء المسلمين لحضور القمة، التي ألقى فيها ترامب خطابًا والتقى خلالها قادة البلدان المسلمة. بالتأكيد لم تغب عن ذاكرة الجميع عدوانية ترامب التي أظهرها ضد المسلمين أثناء حملته الانتخابية، حيث وُصف بأنه شخص مهووس بالخوف من الإسلام واعتُبرت حملاته الانتخابية الأشد عدوانية ضد المسلمين في تاريخ أميركا. كانت رسالة قمة الرياض الإسلامية واضحة، فهي تدعو إلى تقديم الدعم في مواجهة الإرهاب وتجفيف مصادر تمويل الجماعات الجهادية. وقد وضعت القمة على رأس أجندتها، ضمن مطالب أخرى، ضرورة جمع أكبر قدر ممكن من الأموال، خاصة من البلدان الغنية، وبشكل أخص، من بلدان مجلس التعاون الخليجي. ولم يظهر خلال القمة، وما طرحته من القضايا وأعلنته من مخاوف، أي شيء يتعلق بأي من دول مجلس التعاون الخليجي، ولا بقطر على وجه خاص. ولم يرشح عن القمة شيء يخرج عن المألوف، على الأقل بالنسبة للمراقب العادي.

أما الفصل الثاني من السيناريو فهو ضرورة وجود سبب أو دافع لإعلان الحرب، والطريق الأفضل لفعل ذلك هو اختلاق تصريحات لأمير قطر، الشيخ تميم بن حمد آل ثاني. وكان يجب أن يتم ذلك عبر وكالة الأنباء الحكومية القطرية الرسمية (قنا). أما نسج خيوط تلك المؤامرة فتطلب إخراجًا هوليوديًّا مستوحى من فيلم قديم تحت عنوان "ذيل الكلب" أو " Wag the Dog"(2). وهو فيلم أُنتج في العام 1997، من بطولة الممثلَيْن الأميركيَيْن الشهيرين، داستن هوفمان (Dustin Hoffman) وروبرت دي نيرو (Robert De Niro)، اللذين عملا معًا، في الفيلم، على تدبير حرب افتراضية في ألبانيا بهدف إلهاء الناخبين وإبعاد أنظارهم عن فضيحة أخلاقية كانت تهدد الرئيس الأميركي جديًّا. بدأ عرض الفيلم قبيل ظهور فضيحة لوينسكي وكذلك قبيل وقوع الهجوم الأميركي على مصنع الشفاء للأدوية في السودان وتدميره. وقد عقدت وسائل الإعلام مقارنة بين الفيلم والأحداث التي جدت حينها.

في سيناريو مشابه، وبعد أن قررت اتخاذ إجراءات ضد قطر، لجأت البلدان الخليجية الثلاث، صحبة حليفتها مصر، إلى اختلاق فيلم هوليوودي الطابع، وكان عملهم من المهنية بمكان، ليس فقط في حبك مراحل القصة، بل أساسًا في إخفاء مختلف حلقاتها وإبقائها طي السرية المطلقة. استهدفت المؤامرة، بالطبع، أمير قطر بشكل مباشر، ومن ثم البلد بأكمله. وبالطبع أيضًا فإن الاختلاف بين الفيلم وهذه المؤامرة يكمن في السبب والدافع، حيث كان في حالة قطر ذلك التصريح المفبرك المنسوب لأميرها هو السبب وراء إعلان الحرب. أما ما هو مشترك بين فيلم "ذيل الكلب" والمؤامرة ضد قطر فهو أن السيناريوهين اختُلقا وجُهّزا قبل أشهر من تسريبهما في استباق للنتائج المخطط بلوغها، والتي كانت بمثابة آخر مرحلة على أجندة معديهما.

تتمثل المرحلة الثالثة من السيناريو في آلية التسويق له؛ ففي حين كانت الخطة بشأن فيلم "ذيل الكلب" تقتضي عرضه على شاشات قاعات السينما في أميركا وعبر العالم، كانت في حالة قطر بث التسريب على أنه صادر عن الجهة التي تتحدث باسم دولة قطر، أي وكالة الأنباء القطرية. بالتأكيد، كانت المرحلة الثالثة من هذا السيناريو هي الأصعب لأنها تتطلب مهارات تقنية متطورة غير متوفرة سوى لعدد محدود من الدول؛ إذ إن شن هجوم سيبراني، وتحميل مضمون شريط صوتي مفبرك لخطاب أمير قطر ووضعه مكان الشريط الصوتي الأصلي، هي عملية معقدة لا يمكن تنفيذها إلا على أيدي خبراء متخصصين مدعومين ومُمولين من قبل دُول.

لماذا تلجأ الدول إلى الهجمات السيبرانية؟

يعني مصطلح الهجوم السيبراني قيام فرد أو مجموعة من الأفراد أو كيانات ممولة من قبل دولة ما، سواء أكانت تعمل مع أم تتلقى دعمًا من حكومة ما، بإطلاق فيروسات أو "ديدان إلكترونية " -أو أي نوع آخر من الهجمات السيبرانية التي لا تقتصر فقط على شيفرة ما يسمى بحصان طروادة أو التطبيق السري المعروف تحت مسمى "الأبواب الخلفية" أو برنامج "حجب الخدمة" وغيرها من البرمجيات الفيروسية- بهدف زعزعة أو شل الضحية سواء أكانت فردًا أم مجموعة من الأفراد أم منظمة أم شركة أم وكالة حكومية.

في عصرنا هذا، باتت تلك الفيروسات و"الديدان الإلكترونية " تُستخدم على نطاق واسع في شن الهجمات السيبرانية. حيث يتم إرسال فيروس أو ديدان إلكترونية عبر عمل تقني منجز بطريقة احترافية ويشمل الهندسة الاجتماعية؛ حيث بات نشر الفيروسات والديدان الإلكترونية أيسر بكثير مع ازدياد الإقبال على استخدام وسائط التواصل الاجتماعي والهواتف الجوالة المختلفة. فقد أصبحت الشعوب مدمنة على وسائط التواصل الاجتماعي ويذهب كل تركيزها إلى امتلاك هاتف جوال أو جهاز كمبيوتر محمول ليكون جزءًا من عاداتهم اليومية يقضون معه ساعات مديدة. وهكذا أصبح نشر وإرسال الفيروسات والديدان الإلكترونية هو القاعدة المتبعة والسهلة التي يلجأ إليها القراصنة لإرسال مختلف أنواع تلك الفيروسات وبأعداد مهولة تفوق عددها في السنوات الماضية.

ما انفك عدد الهجمات الإلكترونية يرتفع كل يوم من بلد إلى بلد آخر ليتضاعف آلاف بل وملايين المرات. ومع أن الراجح هو عدم تمكن أغلب تلك الفيروسات المرسلة من الاختراق، إلا أن نسبة مئوية ضئيلة منها قد تتمكن في النهاية من الاختراق، ومن شأن ذلك أن يُحدث آثارًا مدمرة. قد يأتي الخطر من الفيروسات والديدان الإلكترونية التي تم إنشاؤها حديثًا أو كانت مخزنة لاستعمالها وقت الحرب في هجمات مستقبلية. تمتلك تلك الفيروسات والديدان الإلكترونية، الجديدة أو المعدلة، بصمات رقمية يصعب على جدران الصد والحماية أو البرمجيات المضادة للفيروسات اكتشافها ومن ثم صدها، ذلك لأنها غير مخزنة في جدران الصد والحماية أو ضمن قواعد بيانات البرمجيات المضادة للفيروسات. وقد أصبحت تلك الفيروسات، على اختلاف أنواعها، أسلحة حديثة تستخدم في شن هجمات إلكترونية على البنى التحتية الإلكترونية التابعة للدول. وفي أغلب الحالات لا يدرك الضحايا وجود فيروسات أو ديدان إلكترونية داخل أنظمة الحوسبة التي يستخدمونها، بل إنهم لن يدركوا ذلك إلا بعد أن يكون قد فات الأوان. وبحسب الهدف من وراء الهجوم، فإن لفت الانتباه إلى الفيروسات يمكن أن يصدر آنيًّا، لكن في حالات أخرى فإن للفيروسات والديدان الإلكترونية أهدافًا وأغراضًا تتحقق دون علم الضحايا بها. فبعض تلك الهجمات يمكن التعافي منه مثل حجب الخدمة، لكن أغلبها تستعصي على العلاج. في حالات التجسس، أو حملة التضليل المعلوماتي أو تشويه السمعة وغيرها من الأهداف العسكرية مثل شل الرادارات، للتمكن من إرسال الطائرات وشن حرب مادية، فإن هذه الهجمات قد تتم في سرية مطلقة لا يتفطن لها ضحاياها.

الهجوم على وكالة الأنباء القطرية الرسمية

إن تاريخ الهجوم السيبراني على وكالة الأنباء القطرية، المعلن على كل وسائل الإعلام وكذلك في البيان الصادر عن حكومة دولة قطر، وهو 24 مايو/أيار 2017، ليس التاريخ الحقيقي للهجوم، إنه فقط التاريخ الرسمي لاكتشاف تسريب الشريط الصوتي المفبرك، على غرار إخراج الفيلم الهوليوودي المشار إليه أعلاه، والذي رُكِّب على شريط خطاب أمير قطر الأصلي

الذي ألقاه خلال حفل تخريج عناصر من الجيش في 23 مايو/أيار 2017. ما لا يُعرف هو الوقت الذي استغرقه التخطيط لهذا الهجوم قبل إطلاقه على أنظمة الحاسوب التابع للوكالة القطرية للأنباء.

ألقى أمير قطر خطابًا في الثالث والعشرين من مايو/أيار 2017، إلا أن بث الخطاب على وكالة الأنباء القطرية كان في اليوم الموالي، أي في 24 مايو/أيار 2017، وكان خطابًا مختلفًا تمامًا عن الأصل، فقد كان مفبركًا وتم تركيب الصوت على الشريط الأصلي، وجاء فيه أن علاقة قطر بالرئيس الأميركي، دونالد ترامب، غير جيدة وأن حماس هي الممثل الشرعي للشعب الفلسطيني، كما وُصفت إيران في الشريط المفبرك، على لسان أمير قطر، بأنها قوة إقليمية كبيرة ومهمة في استقرار المنطقة(3). وكانت كل تلك التصريحات مُفبركة ومركبة من قبل مهندس تركيب الصوت على الشريط الأصلي. المثير للاهتمام في هذا العمل هو ذلك التشابه بينه وبين سيناريو فيلم "ذيل الكلب"؛ حيث إن التنفيذ كان على أيدي فريق من الخبراء فائقي التحكم في التقنيات عالية التعقيد والجودة، والتي لا يمكن لأية جهة أخرى تنفيذها غير جهات تتلقى دعمًا من قبل الدول.

كانت الغاية وجود فرصة مواتية أولًا، وقد لاحت تلك الفرصة في خطاب الأمير، وثانيًا: كانت عملية تركيب الصوت على الشريط الأصلي، وهو ما تم بسرعة وحرفية. أما الخطوة التالية فتمثلت في إرسال الشريط المفبرك إلى نظام خادم التشغيل الرئيسي ومسح الصوت الأصلي ومن ثم بثه في اليوم التالي. أما التخطيط لهذا السيناريو وإعداده وتفعيل الخطة فقد أُنجزت قبل أشهر من انعقاد قمة الرياض الإسلامية، المشار إليها سابقًا، وتم كل ذلك دون أن يشعر أي طرف بشيء ما غير طبيعي ودون توقع ما سيحدث لاحقًا، طبعًا باستثناء الدول الأربعة التي أعدَّت السيناريو وفعَّلته، فهي كانت تدرك ما سيحدث لاحقًا إذا ما نُفذ المخطط بمختلف مراحله وكانت مستعدة للخطوة التالية؛ فالهدف النهائي هو فرض حصار بحري وجوي وبري على قطر مع احتمال تدخل عسكري، إذا تطلب الأمر، واجتياح قطر. هكذا إذن تم وصف قطر بالدولة الإرهابية وأعلنت أربع دول حصارًا كاملًا عليها، وللمفارقة الغريبة فإن ذلك الحصار لم يشمل المقاطعة التجارية فحسب، بل تعدى ذلك لينسحب حتى على العلاقات بين شعوب بلدان الحصار والشعب القطري. بل إن الأدهى من ذلك هو أن كل ذلك التخطيط وتلك التحركات وتفعيل المخطط وما يستتبعه من آثار لم تكن لتتم من دون موافقة بعض القوى العظمى مثل الولايات المتحدة الأميركية، وبمعرفة الرئيس ترامب نفسه؛ فقد أُعطي لهم الضوء الأخضر لتنفيذ مخططهم.

تنفيذ الهجوم السيبراني على قطر

تعتبر طريقة التصيد الإلكتروني الاحتيالي (phishing Spear) من أكثر الآليات فعالية في عالم القرصنة. ويعني هذا المصطلح أن ضحية معينة تم تحديد هويتها ومن ثم إرسال الفيروس أو الدودة الإلكترونية لاستهدافها. ومع ذلك، فإن القيام بمثل هذه العملية على مستوى فبركة شريط صوتي ومن ثم بثه من على منصة وكالة الأنباء القطرية يتطلب إعدادات مكثفة سابقة على تنفيذ البث. فالتخطيط لتنفيذ أية عملية قرصنة إلكترونية يستدعي معرفة واسعة بالنظم الحاسوبية للضحية المستهدفة؛ إذ يتوجب على القراصنة معرفة أنواع مختلف التطبيقات البرمجية والتعرف إلى آليات الحماية الموجودة لدى الضحية، أي التعرف إلى جدران الصد وبرامج الحماية ضد الفيروسات، بالإضافة إلى معرفة أي أنواع برمجيات كشف القرصنة أو التسلل التي يستخدمها نظام خادم التشغيل الرئيسي للموقع المستهدف.

فالتخطيط وتفعيل المخطط يجب أن يتمَّا انطلاقًا من إحدى الدول الأربعة المشاركة في حصار قطر. وهذه الدول الأربعة لا تتساوى من حيث المهارات التقنية المكتسبة على مستوى تنفيذ عمليات القرصنة الإلكترونية، فقط دولة واحدة لديها الإمكانيات لفعل ذلك، وهي دولة الإمارات العربية المتحدة، وهو ما تم تأكيده الآن من طرف عدد من الصحف، وأساسًا صحيفة الواشنطن

بوست التي نقلت عن جهاز الاستخبارات الأميركية أن الإمارات العربية المتحدة هي التي خططت ونفذت عملية القرصنة التي استهدفت وكالة الأنباء القطرية. بل إن الصحيفة فصَّلت القول وذكرت أن عددًا كبيرًا من المسؤولين في حكومة الإمارات خططوا ونفذوا، بالتزامن، لفبركة وتسريب بث الشريط الخاص بأمير قطر(4)(5)، على الرغم من نفي الحكومة القطرية وعدد من المسؤولين القطريين الرسميين نسبة تلك الأقوال للأمير وأصدرت بيانًا يؤكد تعرض وكالة الأنباء القطرية إلى الاختراق. وفي الواقع، فإن قطر استدعت كلًّا من وكالة الاستخبارات الأميركية و"الإف بي آي" (مكتب التحقيقات الفيدرالي) والإنتربول اللذين أكدا تعرض وكالة الأنباء القطرية للقرصنة الإلكترونية، إلا أن دول الحصار تجاهلت نتائج تلك التحقيقات كما تجاهلت من قبل بيان حكومة قطر الرسمي وواصلت المضي في تنفيذ مخططها.

تتم عملية التصيد الإلكتروني الاحتيالي عبر رابط إلكتروني ضعيف الحماية، وفي حالة قرصنة وكالة الأنباء القطرية فإن القرصان أو المتسلل الإلكتروني كان عليه تحديد هوية الشخص الذي يملك خاصية النفاذ عن بعد إلى نظام خادم الحاسوب الرئيسي. ويعتبر نظام منح الدخول عن بعد إلى الحاسوب الرئيسي أمرًا متعارفًا عليه في عديد الأماكن، وهو يعني أن يقوم أحد مستخدمي تطبيق ما، مثل موقع وكالة الأنباء القطرية، بالدخول عن بعد إلى الخادم الرئيسي للموقع. ويكون المطلوب من القرصان معرفة هوية ذلك المستخدم الذي يملك حق الدخول عن بعد إلى الحاسوب الرئيسي، وكذلك معرفة نوع الجهاز الذي يستخدمه في ذلك سواء أكان هاتفًا جوالًا أم جهاز كمبيوتر محمول. وفي حالتنا هذه، وهو السيناريو الأرجح، أنه جهاز هاتف جوال المُستخدم، والذي كان إما من نوع آي فون أو سامسونغ. وتستخدم تقنيات التصيد الاحتيالي الإلكتروني عندما يتم إنشاء رابط في شكل ملف مرسل عبر رسالة إلكترونية أو مستنَد، وعندما يقوم أحد مستخدمي جهاز الهاتف الجوال بالنقر على ذلك الرابط يتم تحميل الفيروس أو الدودة الإلكترونية التي بداخله لتُرسل في شكل رسالة إلكترونية إلى المستند. ثم يكون الهدف التالي هو تحويل الدودة الإلكترونية من جهاز الهاتف الجوال إلى الخادم الرئيسي ومن ثم يصبح متحكَّمًا فيه. لكن قبل ذلك، وعندما يتم تحميل الدودة الإلكترونية، وهذا يعتمد على ما تحمله من خصائص، فإن تلك الدودة الإلكترونية تقوم بجمع وفك تشفير كلمات المرور فيصبح بإمكانها تسريع ميزة الوصول إلى منصة التحكم الإداري عبر حصولها على كلمات السر لمستخدم الخادم الرئيسي، ومن ثم السيطرة على النظام الحاسوبي بالكامل. ذلك هو السيناريو الذي وقع مع وكالة الأنباء القطرية.

بل أبعد من ذلك، فإن للدودة الإلكترونية القدرة على إنشاء ما يسمى قدرات الأبواب الخلفية التي تمكن القرصان من تنفيذ الهجمة السيبرانية داخل نظام الخادم الرئيسي لموقع وكالة الأنباء القطرية في أي وقت، بالإضافة إلى أنه بإمكان الدودة الإلكترونية خلق القدرة على توفير التغذية العكسية ونسخ المستندات والسيطرة عن بعد من دولة أخرى كما حدث مع النظام الحاسوبي للوكالة القطرية للأنباء، وذلك في سرية تامة ودون علم موظفي الوكالة.

إن وقوع الهجوم على وكالة الأنباء القطرية لا يعود إلى تقصير أو عجز في القدرات التقنية للوكالة بل أساسه تفوق القدرات التقنية التي تمتلكها الجهة التي شنت الهجوم السيبراني، والتي كانت مدعومة من طرف دولة هي الإمارات العربية المتحدة التي تمكنت حكومتها، في وقت سابق، من شراء فيروسات وديدان إلكترونية من جهة ثالثة في السوق السوداء ثم خزنتها لاستعمالها في هجمات مستقبلية. كما أقامت دولة الإمارات علاقة عمل مع جهة ثالثة مكونة من فريق من القراصنة بهدف شن هجمات سيبرانية آنية وأخرى مستقبلية.

كانت وزارة الداخلية القطرية قد ذكرت بعض عناوين برتوكول الإنترنت التي تم استخدامها في الهجوم. ولعناوين بروتوكول الإنترنت تلك أرقام معينة تنتمي إلى الأجهزة المستخدمة في الهجوم السيبراني، وإذا كان قد تم استخدامها فعلًا لإرسال الرابط

الحامل للدودة الإلكترونية مع الملف المرسل للموظف المستهدف داخل وكالة قنا، فإن السيناريو الموصوف أعلاه يكون صحيحًا، وهكذا تمكن المهاجم من السيطرة الكاملة على نظام الحاسوب الرئيسي لوكالة قنا. من ناحيتها، أكدت وزارة الداخلية القطرية أن عناوين بروتوكول الإنترنت المستخدمة في الهجوم خاصة بدولة الإمارات، ما يعني أنها الدليل الرئيسي الذي سيُقدم في أية دعوى قضائية تُقام ضد الإمارات. هذا وقد ثبت أن الإمارات كانت تتعاون مع شركات مرتبطة بإسرائيل وعلى علاقة بأشخاص إسرائيليين. وعلى سبيل المثال نذكر الشركة المسماة "إن أس أو" (NSO) التي باعت الكثير من أجهزتها المتحركة الخاصة بالقرصنة الإلكترونية إلى عدد من الدول، من بينها دولة الإمارات، بهدف التجسس على شعوبها وعلى أطراف أخرى أيضًا(6). أسعار هذه الأجهزة باهظة جدًا وهي تختلف من جهاز متحرك لآخر. هذا بالإضافة إلى أن شركات أخرى، لها ارتباطات بإسرائيل، ثبت تعاونها مع الإمارات في تنمية قدراتها في القرصنة الإلكترونية، وهو ما تناقلته تقارير إعلامية مختلفة.

في الأصل، تصنف مثل هذه الهجمات السيبرانية غير قانونية، وهي في الواقع مُجرمة في القوانين الدولية. ومن الثابت أن البلدان المتورطة في مثل هذه الهجمات يجب تقديمها إلى المحكمة. لكن، وبالنظر إلى الإشكاليات المتعلقة بإثبات الحالة بشكل قطعي، هذا بالإضافة إلى نفي الحكومات المتكرر علاقتها المباشرة بالهجوم ودفعها بأن تلك الهجمات يمكن أن تكون من فعل جهة ثالثة أو مجموعات من الأفراد الذين يتعاطفون مع بعض الحكومات. وفي هذه الحالة فإن إثبات المسؤولية القانونية لتلك الحكومات قد تكون محل شك لكن مع إجراء بحث قضائي جنائي دقيق وجمع المعطيات التقنية، فإن إقامة دعوى قضائية ضد الإمارات بتهمة تنفيذ الهجوم ممكنة.

تؤكد الحقائق والتقارير الإعلامية المتضافرة، خاصة تلك الواردة في صحيفة محترمة مثل الواشنطن بوست، أن الحكومات ليست منزهة عن تنفيذ مثل تلك الهجمات الإلكترونية(7). ومع ذلك، فإن دولة الإمارات نفت علاقتها بالهجوم(8). ومؤخرًا نفت وزارة خارجية الإمارات وسفيرها في واشنطن، يوسف العتيبة، أي علاقة للإمارات بالهجوم.

كما استعملت الإمارات الهجمات السيبرانية، فإن خلافاتها مع عدد متزايد من الدول والجماعات جعلتها أيضًا عرضة لهجمات سيبرانية؛ حيث كان السفير الإماراتي، العتيبة، نفسه ضحية لهجوم إلكتروني وقع بعد الهجوم على وكالة قنا. وقد تبنت مجموعة قراصنة تسمى "غلوبل ليك" الهجوم الذي استهدف السفير العتيبة، حيث تمكن القراصنة من السيطرة على كمبيوتر العتيبة المحمول ونسخ كل الملفات والرسائل الإلكترونية، التي تم تسريب بعضها على المواقع الإلكترونية ونشرتها وسائل الإعلام العالمية، وهو ما عرَّض مساعي الإمارات للتأثير على مجريات الأحداث، ليس فقط في واشنطن بل وفي المنطقة وما حولها أيضًا، إلى الفشل. وكنتيجة للسيناريو المشار إليه أعلاه الذي تم من خلاله تنفيذ الهجوم السيبراني واختراق النظام الحاسوبي لوكالة قطر للأنباء، قام المهاجم وبشكل متزامن بنشر الشريط المفبرك لأمير قطر، وهو ما يُظهر إلى أي حد كان هذا السيناريو معدًّا سلفًا. وعلى إثر ذلك أعلنت البلدان الأربعة حصارًا شاملًا برًّا وبحرًا وجوًّا على قطر معتبرة إياها دولة إرهابية تدعم وتمول الجماعات الإرهابية وتزعزع استقرار بلدان الحصار.

دفاعات قطر واستراتيجيتها الأمنية السيبرانية

أصدرت قطر، في شهر مايو/أيار عام 2014، استراتيجيتها الأولى للأمن الوطني السيبراني، وحددت فيها بوضوح الأهداف التالية(9):

1. حماية البنية التحتية للمعلومات الحيوية الوطنية.

2. الاستجابة الفورية للحوادث والاعتداءات الإلكترونية وحلها والتعافي منها عبر مشاركة المعلومات في الوقت المناسب وتنسيق التعاون والعمل المشترك بين الجهات المعنية.
3. إنشاء إطار قانوني وتنظيمي لخلق فضاء سيبراني آمن ونشط.
4. التمكين لثقافة الأمن السيبراني ونشرها من أجل تعزيز الاستخدام الآمن والمناسب للفضاء السيبراني.
5. تطوير وتنمية قدرات الأمن الوطني السيبراني.

توفر هذه الأهداف مجتمعة تأسيس حماية ضد الهجمات والحوادث السيبرانية وتعزز من نظم الاستعداد لها وكشفها والرد عليها وتمكين فعالية التعافي منها. ويتم دعم كل هدف من هذه الأهداف عبر مبادرات تدفع نحو العمل على إنجازها.

أُسِّس فريق الاستجابة لحالات الطوارئ في قطر، المعروف تحت مسمى "Q-CERT" من أجل تنفيذ الاستراتيجية الوطنية وتحقيق الأهداف المفصلة أعلاه. وقد تمكن الفريق من إثبات مهاراته في تنبيه الجهات الحكومية إلى التهديدات الإلكترونية المحتملة وتحذيرها من مختلف الهجمات بواسطة الفيروسات والديدان الإلكترونية التي تستهدف مؤسسات البلد وبنيته الإلكترونية التحتية. وينظم فريق الاستجابة لحالات الطوارئ في قطر سنويًّا دورات تدريبية مشتركة لمنتسبي مختلف الجهات الحكومية، بمشاركة أهم مؤسسات القطاع الخاص أيضًا، من أجل تعريفهم بمختلف سيناريوهات الهجوم السيبراني ومن ثم إكسابهم مهارات إجهاض العديد من التهديدات السيبرانية. لكن، وبالرغم من كل تلك الاستعدادات والتدريبات فإن العديد من نقاط الضعف، التي ستواجهها النظم الحاسوبية في الكثير من البلدان، لا تزال موجودة. تتمثل إحدى تلك النقاط في الضعف البشري، حيث إنه مع إدمان أعداد متزايدة من المواطنين استخدام وسائط التواصل الاجتماعي والتطبيقات المختلفة بشكل يومي، فإن ذلك قد يجعلهم عرضة للهجمات السيبرانية ولتقنيات التصيد الإلكتروني على غرار ما حدث لوكالة الأنباء القطرية. هذا أمر لا مفر منه حتى مع حملة التوعية الواسعة التي يقوم بها فريق الاستجابة لحالات الطوارئ في قطر وتساعده فيها مختلف الجهات الحكومية. أما نقطة الضعف الثانية فهي وجود كيانات ترعاها الدول، التي تضمر تنفيذ هجمات سيبرانية، وتضع تحت تصرفها مواردها التكنولوجية والمالية الهائلة.

يمتلك العديد من المؤسسات الحكومية ونظم الحوسبة المختلفة التي تتحكم في البنى التحتية الإلكترونية القطرية برامج حماية متطورة من أجهزة وبرمجيات. وقد جُهزت تلك المؤسسات الحكومية بجدران حماية محدثة وبرمجيات مكافحة الفيروسات وبرمجيات منع الاختراقات وكشفها وغيرها من إجراءات الحماية المختلفة. لكن، وبالنظر إلى الحقائق المذكورة آنفًا، فسيكون من المستحيل تأمين المؤسسات الحكومية بالكامل من هجمات مستقبلية.

تعمل دولة قطر مع حلفائها ومختلف المنظمات الدولية للقضاء على خطر الهجمات السيبرانية وتُسهم بكل ما تملك من جهد في التعاون والتنسيق المشترك في هذا المجال. لذا، يجب أن يستمر هذا التعاون ويُعزَّز من أجل تأمين أقصى درجات الحماية.

سيناريو الحماية المفترض لقطر

لدى دولة قطر شبكة إنترنت عالية الجودة، وهو ما يساعد على انتشار استخدام الإنترنت ومختلف التطبيقات الاجتماعية على نطاق واسع سواء أكان في القطاع الحكومي أم الخاص. إن هذه الخدمة تعتبر نعمة في حد ذاتها، لكنها أيضًا نقمة ولعنة في ذات الوقت. فهي نعمة من حيث توفير إمكانات التواصل بين الأشخاص وإتاحة الوصول إلى المعلومات من على شبكة

الإنترنت العالمية، لكنها لعنة أيضًا لأنها تفتح الباب أمام هجمات إلكترونية محتملة؛ إذ تمثل الإنترنت مدخلًا لتنفيذ أغلب تلك الهجمات.

لا شك أنه ثمة متطلبات ومقاربات معينة لتوفير الحد الأقصى من الحماية الأمنية السيبرانية لدولة قطر، وهي تشمل، على سبيل المثال لا الحصر، ما يلي:

1. إنشاء مركز للسيطرة والتحكم السيبراني: يؤدي هذا المركز مهمة أساسية في قطر، فهو يؤمِّن الدفاع عن البنية الإلكترونية التحتية للبلاد من أية هجمات سيبرانية سواء أكانت قائمة حاليًا أم يُتوقع حدوثها مستقبلًا. وعادة ما يكون مثل هذا المركز، كما هي الحال في العديد من البلدان، تابعًا لمؤسسة الجيش الوطني أو إلى سلطة تنفيذية عليا تتمتع بصلاحيات تنفيذية مباشرة على جميع الكيانات الحاسوبية التي تؤمِّن البنى التحتية للبلد.
2. الإلغاء الكامل والفصل التام لخدمة الاتصال عن بُعد عبر شبكة الإنترنت العالمية الخاصة بالنظم الحاسوبية المرتبطة بالبنية التحتية الإلكترونية، وكذلك إلغاء خدمة الإنترنت التي تسمح بتحميل الملفات وتنزيلها بالنسبة لجميع الموظفين في منشآت البنية التحتية الإلكترونية للبلد. ويجب تنفيذ كل تلك الإجراءات والعمليات بكل صرامة داخل المنشآت التي هي على علاقة بخدمات البنى التحتية الإلكترونية الحيوية في البلد.
3. الاستفادة من المواطنين القطريين المؤهلين العاملين أصلًا في مجال الأمن السيبراني، مع الحرص على تعليم وتدريب المواطنين القطريين، من ذوي الكفاءة، على اكتساب مهارات الأمن السيبراني من أجل بناء فريق قطري قوي يكون قادرًا على تولي مسؤوليات حماية البنى التحتية الإلكترونية الوطنية من تهديدات الهجمات القائمة حاليًا وتلك المستقبلية(10).

حرب سيبرانية إقليمية

يُتوقع استمرار الحرب السيبرانية بين دول مجلس التعاون الخليجي، وخاصة من جانب دول الحصار، طالما بقيت الأوضاع تراوح مكانها وسيستمر ذلك إلى أن يحل الاستقرار. إلا أنه ثمة احتمال آخر قابل للتحقق يتمثل في إمكانية تعرض قطر لهجمات سيبرانية من دول أخرى هي على نزاع مع الدوحة ولديها ما يكفي من الموارد التكنولوجية والمالية لشن هجمات سيبرانية.

تتقدم قطر بسرعة في بناء وتجهيز عدد من البنى التحتية المختلفة لاستيعاب فعاليات أكبر حدث في العالم ألا وهو تنظيم كأس العالم لكرة القدم 2022، أي بعد حوالي أربع سنوات من الآن. وقد ضخت قطر أكثر من 200 مليار دولار لإقامة تلك المشاريع. أما اليوم فالحاجة ملحَّة للاستثمار بكثافة في تقنيات الأمن السيبراني والبنى التحتية من أجل تنظيم آمن وناجح لبطولة كأس العالم القادمة.

وفي كل الحالات، فإن الهجمات السيبرانية لن تتوقف، وعلى كل دولة، بما فيها قطر، الاستعداد لمواجهة الخطر المحتمل مع التمسك بأمل ألا تحدث أي هجمات على البنى الإلكترونية التحتية الأساسية ذات التأثير المباشر على حياة الناس اليومية. وإذا ما كان لهذا السيناريو أن يتحقق، فإن نفس البلدان التي تخطط لشن هجمات سيبرانية على البنى التحتية الحيوية هي ذاتها التي تخطط أيضًا لغزو فعلي وشن حروب مادية. وقد سجل التاريخ تنفيذ مثل هذا السيناريو فعليًّا في عدد من البلدان عبر العالم.

---

* *د. محمد الدوراني، خبير في الأمن السيبراني الخليجي*

*** ملاحظة: أُعد النص في الأصل باللغة الإنجليزية لمركز الجزيرة للدراسات، ترجمه د. كريم الماجري إلى اللغة العربية.*

مراجع

1. Jones, Mac, "Hacking, bots and information wars in the Qatar Spat, The Washington Post, 7 June 2017, (Visited on 13 May 2018): https://wapo.st/2jSkOKf
2. "Wag the Dog", Wikipedia, the page last edited on 20 April 2018".
3. Coats Ulrichson, Kristian, "What's going on with Qatar?", washingtonpost.com, 1 June 2017, (Visited on 13 May 2018): https://wapo.st/2KVXI1z
4. "US intelligence confirms UAE planned Qatar fake news hack", Washington Post, 17 July 2017, (Visited on 13 May 2018): https://wapo.st/2jSq2Wd
5. Schickert, Peter, "Not 'Russian hackers'? Wapo report accuses UAE of orchestrating Qatar media hack, /Global Look Press, Russia Today, July 17, 2017, (Visited on 13 May 2018): https://on.rt.com/8hy1
6. Ngo, Amanda, "Behind the &1B NSO Hacking Business", nocamels, Nocamels, 27 July 2017.
7. DeYoung, Karen and Nakashima, Ellen, "UAE orchestrated hacking of Qatari government sites, sparking regional upheaval, according to U.S. intelligence official", Washington Post, July 16, 2017, (Visited on 13 May 2018): https://wapo.st/2ICbtUM
8. "UAE foreign minister denies hacking Qatari government media sties", The Financial Times, 2018, (Visited on 13 May 2018): https://www.ft.com/content/47c3464e-6ada-11e7-b9c7-15af748b60d0
9. "Qatar National Cyber Security Strategy", motc.gov, May 2014, (Visited on 13 May 2018): http://www.motc.gov.qa/sites/default/files/national_cyber_security_strategy.pdf
10. Al-Dorani, Mohammed, "Cyber Challenge & GCC Countries", November 2015.

انتهى