كيف يمكن أن تهدد الهجمات السيبرانية استقرار السعودية؟

يعد المجال السيبراني أحد المجالات الحاضرة في جوانب التصعيد الأمريكي الإيراني الأخير. ويتيح نقل الصراع إلى الفضاء الإلكتروني الأطراف المختلفة من ارتكاب أعمال انتقامية، مع تقليل فرص الاستجابة والتصعيد من الجانب الآخر، وهكذا ينبغي فهم الهجوم الإلكتروني الذي قامت به الولايات المتحدة ردا على إسقاط إيران لطائرة أمريكية بدون طيار. ومع ذلك، بالنظر إلى التطور السريع للمعرفة والتكنولوجيا في كل ما يتعلق بالفضاء الإلكتروني، فإن دمج البعد السيبراني في مجال النزاعات الدولية يشكل خطرا حقيقيا على البلدان التي تتخلف عن السباق التكنولوجي. وفي هذا السياق، فإن المملكة العربية السعودية معرضة للخطر بشكل خاص.

وعلى الرغم من أن المملكة لا تشارك مباشرة في التصعيد الحالي في الخليج، تضعها الظروف الجيوسياسية في خط النار المباشر من منظور علم الفضاء الإلكتروني. ولا تخجل إيران من مهاجمة الأهداف المدنية أو المالية التي تحددها على أنها أقل حماية، وبالتالي أكثر ضعفا من الأهداف العسكرية. علاوة على ذلك، تعد السعودية من بين الدول التي تعاني من أكبر عدد من الهجمات الإلكترونية في العالم، ويعتقد أن معظم الهجمات ضدها تأتي من إيران. على سبيل المثال، تم توجيه 42% من الهجمات الإلكترونية، التي قامت بها منظمة تعرف باسم "إيه بي تي 33"، والتي يقول محللون إنها تتبع إيران، على مدى الأعوام الثلاثة الماضية، ضد أهداف سعودية، بينما تم توجيه 34% فقط من الهجمات ضد الأهداف الأمريكية.

وتواجه كل من الولايات المتحدة وإيران معضلة استراتيجية. فمن ناحية، لا يريد البلدان صراعا شاملا في الخليج، كما تشير التصريحات من أعلى المستويات في كلا البلدين. لذلك، لدى كلا الجانبين مصلحة في عدم اتخاذ تدابير من شأنها تصعيد الموقف. ومع ذلك، قد يحدث التصعيد في الخليج، ليس فقط نتيجة للهجمات الإيرانية، ولكن أيضا نتيجة الخطوات الأمريكية ضد البرنامج النووي الإيراني. وفي حين تعتقد طهران أنها يجب أن ترد على أحدث موجة من العقوبات التي فرضتها الإدارة الأمريكية، تخشى الولايات المتحدة أن تنظر إيران ودول الخليج إلى عدم الاستجابة للاستفزازات الإيرانية على أنه ضعف، وقد يقوض ذلك ثقة الخليج في الولايات المتحدة كحليف، الأمر الذي قد يشجع بدوره إيران على الاستمرار في أعمالها العدوانية.

وباعتبارها الحليف الرئيسي للولايات المتحدة في الخليج، تبقى المملكة العربية السعودية في خطر. ونظرا لأن قدرات الولايات المتحدة القوية فيما يتعلق بالحماية السيبرانية قد تجعل من الصعب على إيران القيام بهجوم كبير ضدها مباشرة، فقد تختار إيران ضرب المملكة، باعتبارها "القوة الناعمة" للولايات المتحدة في الخليج، من أجل الضغط على الإدارة لتخفيف سياسة العقوبات دون حاجة لوجود رد أمريكي على نطاق واسع. ومع قدرة المملكة المنخفضة نسبيا في عالم الإنترنت، يجعلها ذلك هدفا سهلا إلى حد ما. علاوة على ذلك، نظرا لأهميتها الاقتصادية والجيوسياسية للمجتمع الدولي، فقد تؤدي الهجمات الإلكترونية ضد الأهداف السعودية إلى أضرار جسيمة.

الأخطار المحتملة

وتوجد قناتان محتملتان رئيسيتان للنشاط السيبراني الإيراني ضد السعودية. الأولى هي القناة "المباشرة"، التي تشمل الهجمات على المنشآت والبنية التحتية السعودية، العسكرية والمدنية على حد سواء، والتي قد تلحق أضرارا مادية جسيمة، بل وقد تودي بحياة عدد كبير من الناس. وقد حدث مثال على هذا النوع من الأعمال المدمرة عام 2017، في هجوم إلكتروني ضد أحد مصانع البتروكيماويات في المملكة. ولم يكن الغرض من هذا الهجوم، الذي فشل بسبب خطأ في الكود أوقف نشاطه، لم يكن الغرض منه سرقة أو إتلاف قواعد البيانات السعودية، بل التسبب في أضرار حركية فعلية، وفي هذه الحالة، كان الهدف هو إحداث انفجار عن طريق التداخل بين أنظمة المصنع.

والقناة الأخرى قناة "غير مباشرة"، يتم فيها استخدام حسابات مزيفة على منصات شعبية على الإنترنت، مثل "فيسبوك" أو "تويتر"، لدعم خصوم النظام، ورعاية المعارضة الداخلية داخل المملكة. وتتمثل ميزة هذا النوع من الإجراءات في أنه قد يكون له وقع أقل من الهجمات الإلكترونية المباشرة، نظرا لقدرة البلد المهاجم على إخفاء نشاطه وتصويره على أنه احتجاج داخلي حقيقي. ولا يمكن استبعاد احتمال وقوع هجوم متعدد الجوانب يجمع بين النوعين. وفي هذا السيناريو، تتسبب الهجمات الإلكترونية في كارثة مدنية واسعة النطاق تهز المجتمع السعودي. وفي الوقت نفسه، يستغل التخريب السيبراني المتزايد الوضع الداخلي الحساس لتشجيع الانتفاضة النشطة ضد العائلة المالكة. ولدى إيران مصلحة في تعزيز المخاوف في المملكة من قدرتها على تحفيز التمرد الشيعي ضد أسرة آل سعود، وهو الخوف الذي "ساعد" في الماضي في منع السعودية من التحرك ضد إيران.

عقبات كبرى

وإدراكا منه لمخاطر الهجوم الإلكتروني، يعمل النظام الملكي السعودي على وضع استراتيجية إلكترونية مناسبة، لكن طبيعة النظام السعودي تعيق التقدم في هذا الصدد. فمن ناحية، يوزع الانقسام الإداري الهيكلي في النظام السعودي السلطات ذات الصلة بين العديد من مراكز القوى في مختلف الوزارات

والوكالات. ويجعل هذا الموقف من الصعب إنشاء وتفعيل سياسة إلكترونية موحدة تلبي الاحتياجات الأمنية المتنوعة في المملكة.

وتبقى العقبة الرئيسية الأخرى أن المجتمع السعودي متخلف من الناحية التكنولوجية، وهي مشكلة تهم المملكة ككل. وقد جعلت عقود من الثروة النفطية تطوير القطاعات الاقتصادية الأخرى أمرا غير ضروري. وبالإضافة إلى ذلك، تم شراء الهدوء على الجبهة المدنية من خلال الإعانات السخية، إلى جانب عدد كبير من الوظائف الحكومية، وهو ما لم يمنح السكان أي حافز للعمل بجد أو متابعة تعليم متقدم. نتيجة لذلك، تفتقر المملكة إلى البنية التحتية البشرية والتكنولوجية اللازمة للقدرات المتقدمة في المجال السيبراني أيضا. وتشكل صناعة تكنولوجيا المعلومات نحو 0.4% فقط من الناتج القومي الإجمالي للمملكة، وتعتمد المملكة بشكل أساسي على المساعدة الخارجية لتلبية الاحتياجات المدنية المتعلقة بالإنترنت.

وللتغلب على هذه الصعوبات، اتخذت المملكة تدابير في الأعوام الأخيرة أدت إلى تحسين الوضع بشكل طفيف. حيث أنشأت 3 فروع رئيسية مرتبطة بالمجال السيبراني تعمل بشكل متزامن. الأول هو الهيئة الوطنية للأمن السيبراني. وتم تأسيس الهيئة عام 2017، وهي تابعة للملك "سلمان" وولي العهد "محمد بن سلمان" بشكل مباشر، وهي مسؤولة عن تنسيق السياسات والتنظيم والتدريب في مجال الدفاع الإلكتروني لجميع المنظمات الحكومية والخاصة. وتعد الهيئة هي الوكالة الرئيسية المسؤولة عن تكنولوجيا الأمن نفسها في المملكة.

وينضم إليها هيئة ثانية هي "الاتحاد السعودي للأمن والبرمجة الإلكترونية"، التابع للجنة الأوليمبية السعودية، وهو مسؤول بشكل أساسي عن إعداد الموظفين والبنية التحتية التكنولوجية اللازمة لقطاع الإنترنت والبرمجة. وكجزء من عمله المستمر، ينظم "الاتحاد" مؤتمرات ومسابقات من أجل زيادة الوعي بقضايا الأمن السيبراني، وتشجيع الشباب السعودي على التخصص في هذا المجال. وانضم إلى هاتين الوكالتين كيان ثالث سري وأكثر عدوانية، تم إدارته، على الأقل حتى اغتيال الصحفي السعودي "جمال خاشقجي"، من قبل "سعود القحطاني"، الذراع الأيمن لولي العهد. وتوظف هذه الوكالة المئات من السعوديين، الذين يعملون "كجيش صغير" على قنوات التواصل الاجتماعي، لمراقبة معارضي النظام، وحذف التعليقات الساخطة حول مواضيع حساسة، ونشر التعليقات التي تدعم سياسة النظام الملكي.

وعلى الرغم من التدابير التي اتخذها الديوان الملكي، إلا أن المملكة لا تزال معرضة للخطر إلى حد ما. فقد وجدت دراسة حديثة أن 4 فقط من بين كل 10 مدراء تنفيذيين سعوديين أفادوا بأن منظماتهم مستعدة للتعامل مع الهجمات الإلكترونية، وذلك على الرغم من محاولات السعوديين لتشجيع التعليم في هذا المجال، مثل المؤتمر الدولي حول الأمن السيبراني الذي استضافته المملكة في فبراير/شباط الماضي. ولم تقم المملكة بعد بتطوير أي تكنولوجيات عدوانية حقيقية، وتعتمد على التكنولوجيا الأجنبية في هذا المجال.

وكما تشير التطورات الأخيرة في الخليج، من المحتمل جدا أن يمتد التصعيد بين الولايات المتحدة وإيران بشكل متزايد إلى الفضاء الإلكتروني. ويشكل مثل هذا التطور خطرا خاصا على السعودية، بسبب احتمال أن تكون المملكة وسيلة إيران لإلحاق الضرر بالمصالح الأمريكية في المنطقة. ويظهر فحص الوضع الحالي للمملكة في عالم الإنترنت أنها غير مستعدة لمثل هذا السيناريو، وأن التدابير التي اتخذتها المملكة في الأعوام الأخيرة لن تؤتي ثمارها إلا على المدى الطويل. لذلك، من أجل أمنها، يتعين على السعودية إيجاد حلول قصيرة الأجل، مثل الحصول على التقنيات والمساعدة من الشركات الأجنبية، للخروج من الأزمة بأقل قدر ممكن من الضرر. ومع ضعف مستوى أنظمة حماية صناعة النفط في المملكة، مع أهميتها بالنسبة لاقتصاد الطاقة العالمي، قد تكون هناك حاجة لتدخل الولايات المتحدة وربما (إسرائيل)، لأجل تحسين قدرة المملكة العربية السعودية على حماية نفسها في عالم الإنترنت.

المصدر | معهد دراسات الأمن القومي الإسرائيلي