مركز حمورابي

الصراع القادم بين إسرائيل وإيران قد يكون في الفضاء السيبراني

الصراع القادم بين إسرائيل وإيران قد يكون في الفضاء السيبراني

ريشي إينجار، مراسل في مجلة فورين بوليسي
ترجمة : صفا مهدي

مركز حمورابي للبحوث و الدراسات الاستراتيجية

4 آيار **2024**

للبلدين تاريخ طويل من الهجمات عبر الإنترنت ضد بعضهما البعض، والتي قد تلعب دورًا في الوقت الذي تفكر فيه إسرائيل في الانتقام من هجوم إيران.

كان هجوم إيران على إسرائيل خلال عطلة نهاية الأسبوع - بأكثر من 300 ذخيرة، بما في ذلك الصواريخ الباليستية والطائرات بدون طيار، التي تم إطلاقها مباشرة من الأراضي الإيرانية - غير مسبوق من نواح كثيرة. ما لم يكن غير مسبوق هو تهديد الهجمات الإلكترونية التي رافقته.

زعمت مجموعة قرصنة مرتبطة بإيران أنها عرضت أنظمة الرادار الإسرائيلية للخطر في الأسابيع التي سبقت الهجوم، على الرغم من أن أكبر وكالة إلكترونية إسرائيلية قالت إنها لم تشهد أي «نشاط غير طبيعي على الإنترنت» خلال الهجوم الصاروخي يوم السبت. ارتفع استهداف إيران لإسرائيل في عالم الإنترنت بشكل كبير منذ الصراع الإقليمي الأوسع الذي أشعله هجوم حماس في 7 أكتوبر 2023، حيث قال رئيس المديرية الإلكترونية الوطنية الإسرائيلية (INCD)، غابي بورتنوي، الأسبوع الماضي إن شدة الهجمات الإلكترونية التي تواجهها إسرائيل تضاعفت ثلاث مرات في تلك الفترة.

ومع ذلك، فإن الصراع الحالي بين البلدين يسبقه تاريخ طويل من الصفقات عبر الإنترنت بأكثر من عقد. في وقت مبكر من عام 2006 - وربما قبل ذلك - تقول التقارير إن الولايات المتحدة وإسرائيل بدأتا في تطوير ثم نشر سلاح إلكتروني، يعرف الآن باسم Stuxnet، للتسلل وتخريب نظام الكمبيوتر في منشأة نطنز النووية الإيرانية، وهي محطة تحت الأرض تستخدم لتخصيب اليورانيوم. تنكر كل من إسرائيل والولايات المتحدة أنهما أنشأتا Stuxnet، على الرغم من أن المؤسسات الإخبارية المستقلة تتفق على نطاق واسع على أن البلدين يقفان وراء البرامج الخبيثة. يعتبر هذا السلاح، الذي تم اكتشافه في عام 2010،

على نطاق واسع نقطة انطلاق لبرنامج إلكتروني إيراني متطور تعتبره واشنطن الآن من بين أكبر تهديداتها، بالإضافة إلى تلك التي يشكلها خصوم آخرون - مثل روسيا والصين وكوريا الشمالية.

إن الهدف الرئيسي لإيران كان دائما إسرائيل.

"إنها واحدة من أقدم الخلافات السيبرانية التي لدينا بالحقيقة" ،قال محمد سليمان، مدير برنامج التكنولوجيا الاستراتيجية والأمن السيبراني في معهد الشرق الأوسط في واشنطن، العاصمة الأمريكية. "أعاد الإيرانيون هندسة عكسية لـ Stuxnet لبناء برامج ضارة خاصة بهم هاجموا بها دول الخليج العربي."
كانت إسرائيل دائماً الأكثر تقدماً بين الطرفين، ويساعدها في ذلك التعاون الوثيق مع الولايات المتحدة وحلفاء آخرين في الغرب. بالإضافة إلى الوكالة السيبرانية الوطنية، تشكل وحدة جمع المعلومات الاستخبارية في جيش الدفاع الإسرائيلي، المعروفة باسم الوحدة 8200، القوة الرئيسية في العمليات السيبرانية الهجومية في البلاد، ويُعتقد أنها تعاونت مع الولايات المتحدة في تطوير هجوم Stuxnet.

أضاف سليمان: «أود أن أسمي إسرائيل قوة عظمى إلكترونية وإيران قوة إلكترونية صاعدة». «إيران لا تعادل إسرائيل حقًا في الفضاء الإلكتروني، لكنها دولة ذو منهجيات سريعة للغاية من حيث بناء قدراتها الخاصة، وقد تعلموا أيضًا من الإسرائيليين طوال هذه السنوات» .
تعهدت إسرائيل بالانتقام من هجوم إيران بطائرات مسيرة وصواريخ يوم السبت، لكن الرئيس الأمريكي جو بايدن وآخرين يحثون القادة الإسرائيليين على ممارسة ضبط النفس من أجل تجنب تصعيد الصراع بشكل كبير. يمكن أن تكون العمليات الإلكترونية إحدى السبل التي يمكن أن تنفذ من خلالها تلك الاستجابة.
"سواء كانوا على صواب أم لا، [إيران وإسرائيل] يبدو أنهم يعتقدون أن العمليات السيبرانية أقل تصعيداً من العمليات الحربية، وبالتالي يمكنهم القيام بها بتوقع رد أقل من الجانب الآخر"، قال تشارلز فرايليخ، الذي كان مستشاراً سابقاً للأمن القومي الإسرائيلي وشريك في تأليف كتاب "إسرائيل وتهديد السيبران: كيف أصبحت الأمة الناشئة قوة سيبرانية عالمية".

على الرغم من هذه الفكرة، فمن المرجح أن تتعامل إسرائيل مع أي هجوم إلكتروني ضد إيران على قدم المساواة مع أي عملية عسكرية أخرى. "لدى جيش الدفاع الإسرائيلي عقيدة عملياتية – بمعنى آخر، يعرفون كيف يريدون استخدامها أو كيفية استخدامها"، قال فرايليتش، وهو حاليًا زميل بارز في معهد دراسات الأمن القومي في تل أبيب. "لم يقوموا بصياغة استراتيجية إلكترونية شاملة". "تتطلب العمليات السيبرانية الهجومية عملية موافقة مشابهة جدًا للعمليات الحركية؛ مع أي شيء مهم، سوف يصعد إلى أعلى السلسلة ويصل إلى رئيس الوزراء نفسه".

تتنوع أشكال العمليات الإسرائيلية ضد إيران بشكل واسع، بدءًا من الهجمات التي تستهدف التأثير على المنشآت النووية إلى التلفيات في البنية التحتية العسكرية أو حتى البنية التحتية المدنية. "هناك عدد من مراكز الجاذبية المحتملة داخل إيران التي قد تختار إسرائيل إعاقتها أو التخفيف من تأثيرها دون استخدام ضربات حركية أو عمليات عسكرية تقليدية"، قال أندرو بورين، الذي كان مسؤولاً استخباراتياً أمريكياً سابقًا والآن هو المدير التنفيذي للأمن العالمي في شركة تقدير المخاطرالاستخباراتية Flashpoint.

إن من أبرز الأمثلة في الماضي القريب هي مجموعة مرتبطة بإسرائيل تُعرف باسم Predatory Sparrow، والتي هاجمت مجموعة متنوعة من الأهداف في إيران بين عامي 2021 و2023، بما في ذلك شبكات القطارات ومصانع الصلب ومحطات الوقود. قال بن ريد، مدير تحليل التجسس الإلكتروني في شركة مانديانت للأمن السيبراني المملوكة لشركة Google، إنه في حين أن إسرائيل لم تُعلن رسميًا مسؤوليتها عن أفعال المجموعة، إلا أنها تتوافق تمامًا مع أهداف البلاد. وأضاف حول الجماعة التي تقف وراء الهجمات: "إنها ممثلة تتمتع بقدرات عالية وليس لديها دافع مالي، ولم يتم ربح أي أموال من ذلك، ولقد أثرت على إيران عدة مرات على مدى بضع سنوات". "لذا هذا نوع من التضييق".
إن هذه الأساليب الخاصة بالجماعة تتناسب مع ما قد ترغب إسرائيل في القيام به في المستقبل، بمعنى القدرة على إحداث اضطراب عام كبير دون تصعيد كبير أو خسائر في الأرواح - على عكس إطلاق الصواريخ الإيرانية التي تم إرسالها بشكل مكثف، والتي كانت بارزة جدًا. لكنها غير فعالة في النهاية.

قال: "تم تصميم هذا ليلاحظ"، "إنها لافتات إعلانية براقة."
قالت إدارة بايدن مرارًا وتكرارًا إن دعمها لإسرائيل لا يزال «صارمًا» لكنها أشارت إلى أن الولايات المتحدة لا تدعم هجومًا إسرائيليًا مضادًا ضد إيران ولن تشارك في مثل هذا الهجوم. ولم تحدد ما إذا كان ذلك يمتد إلى جميع أشكال الهجوم، بما في ذلك العمليات الإلكترونية، أو مجرد العمليات العسكرية الحركية. (لم يرد البيت الأبيض على الفور على طلب للتعليق، ورفضت وزارتا الدفاع والخارجية الأمريكية التعليق). لكن من غير المرجح أن يحتاج الإسرائيليون إلى مساعدة من الولايات المتحدة لتنفيذ هجوم إلكتروني ضد إيران، على الأقل من وجهة نظر القدرات الفنية.

قال بورين: "لدى إسرائيل قوات عسكرية متقدمة للغاية، ولا تطلب جثًا أو قواتًا أمريكية للمشاركة في حروبها... في الواقع، يتشابه الأمر إلى حد كبير في مجال السيبراني". "إسرائيل تمتلك بعضًا من أكثر قدرات الدفاع والهجوم على مستوى الدولة تطورًا في الفضاء السيبراني"، أضاف. "إنهم حلفاء، لكن أعتقد أن النشاط التشغيلي السيبراني لإسرائيل يتم من قبل الإسرائيليين، بتقنية وبرمجة إسرائيلية، ولذلك أعتقد أن إسرائيل من المرجح أن تستمر بما يلي في الحرب".

مركز حمورابي للبحوث و الدراسات الاستراتيجية

أسس مركز حمورابي للبحوث والدراسات الاستراتيجية في،18-11-2006 بمدينة بابل(الحلة)، كمركز علمي بحثي يمتد الى دراسة الموضوعات السياسية و المجتمعية بصورة علمية و استراتيجية، فضلاً عن التركيز على القضايا والظواهر الحادثة والمحتملة قي الشأن المحلي والأقليمي والدولي ، ويتعامل مع باحثين من مختلف التخصصات داخل العراق وخارجه، وتحتضن بغداد المقر الرئيسي للمركز.

www.hcrsiraq.net

07810234002

hcrsiraq@yahoo.com

t.me/hammurabicrss

مركز حمورابي للبحوث والدراسات الاستراتيجية

العراق - بغداد- الكرادة - العرصات الهندية-قربالسفارةالصينية