الأزمة الإيرانية تنتقل إلى الفضاء السيبراني

بواسطة ميكا لوديرميلك (/ar/experts/myka-lwdyrmylk)

يوليو
متوفر أيضًا باللغات:
English **(/policy-analysis/iran-crisis-moves-cyberspace)** /
Farsi **(/fa/policy-analysis/gstrsh-bhran-ayran-bh-fday-saybry)**

عن المؤلفين

ميكا لوديرميلك **(/ar/experts/myka-lwdyrmylk)**

ميكا لوديرميلك هو مستشار للأمن السيبراني ومحلل جيوسياسي مقره في الشرق الأوسط. الآراء المُعرب عنها هنا خاصة بالكاتب فقط.

تحليل موجز

اتخذت مؤخراً التوترات المتزايدة في الخليج العربي بُعداً إلكترونياً من خلال قيام الولايات المتحدة بشن هجوم سيبراني على أنظمة الحواسيب العسكرية الإيرانية ردّاً على إسقاط إحدى طائراتها بدون طيار بينما أفادت بعض التقارير أن قراصنة الحكومة الإيرانية في المجال الألكتروني قاموا بتصعيد عمليات التجسس عبر الإنترنت باستهدافهم المنظمات الأمريكية. والواقع أنه سبق لطهران أن انتقمت من الولايات المتحدة في مجال العالم السيبراني حيث تقلّ العوائق فتسمح بمنافسة تتكافأ فيها الفرص بصورة أكثر - بينما تقل حظوظ أمريكا لأن فسحتها المعرّضة للاعتداء أكبر بكثير من نظيرتها الإيرانية. وبما أن الدلائل تشير إلى نية إيران مواصلة هذا النهج ينبغي على الحكومة الأمريكية والقطاع الخاص اتخاذ الخطوات المناسبة لتعزيز دفاعاتهما السيبرانية.

مراجعة الهجمات الألكترونية الانتقامية الإيرانية

كلما نفذت إيران عمليات سيبرانية ردّاً على نزاعات أو توترات أو تحركات اعتبرتها هجومية سابقاً كانت تصمم تلك العمليات بشكل يُلحق تكاليف ملموسة ويُظهر قدرة استهداف استراتيجية مع الحفاظ على إمكانية الإنكار بشكل معقول وتجنب التصعيد. ومن أبرز هذه الهجمات السيبرانية "عملية أبابيل" التي استهدفت المؤسسات المالية الأمريكية بين عامَي 2012 و2013 و"هجوم شامون" عام 2012 ضد شركة النفط السعودية العملاقة "أرامكو" والضربة التي تعرضت لها مؤسسة "لاس فيغاس ساندز" عام 2014.

وحدثت "عملية أبابيل" في وقت كانت تفرض فيه واشنطن عقوبات إضافية على "البنك المركزي الإيراني" وكيانات أخرى واستُخدمت فيها هجمات موزّعة لـ "الحرمان من الخدمات" لعرقلة برامج الخدمات المصرفية عبر الإنترنت. ومع أن هذه الهجمات كانت بدائية إلا أن "أبابيل" كانت حملة فعالة في استهدافها إذ عرقلت مؤقتاً بعض الوظائف التجارية لدى إحدى الركائز الجوهرية الحساسة في الاقتصاد الأمريكي وتسببت بأضرار بلغت عشرات ملايين الدولارات. وعلى الرغم من أن مجموعة قراصنة في المجال الألكتروني تطلق على نفسها اسم "المقاتلين الإلكترونيين في كتائب عز الدين القسام" قد تبنّت المسؤولية عن عملية "أبابيل" إلّا أنه من شبه المؤكد أن الحكومة الإيرانية هي التي أوعزت بها.

وقد اتّبعت الهجمات الإلكترونية على "أرامكو" ومؤسسة "لاس فيغاس ساندز" الخطة نفسها. وعلى الرغم من تبنّي جماعات القرصنة الإلكترونية ذات الدوافع السياسية مسؤولية هاتين العمليتين إلا أن كلتيهما رُبطتا بإيران وبتطورات محددة اعتبرتها طهران بمثابة تهديد لها. فقد وقع "هجوم شامون" بعد تشديد عقوبات النفط الأمريكية واكتشاف عمليات سيبرانية ضد البنية التحتية النووية الإيرانية بينما أعقب الهجوم على مؤسسة "ساندز" تأييد صاحب الشركة شيلدون أديلسون - من المتبرّعين السياسيين للحزب الجمهوري في الولايات المتحدة -توجيه ضربة نووية استباقية ضد إيران.

وعلى الرغم من وقوع الهجومين على الشركتين الأمريكية والسعودية في الوقت نفسه تقريباً إلّا أن آثارهما التدميرية اختلفت إلى حدٍّ كبير. فقد اعتُبر "هجوم شامون" من أكثر الهجمات السيبرانية ضرراً التي تم الإبلاغ عنها على الإطلاق حيث أتلف أكثر من 30 ألف جهاز حاسوب ومحى نسبة ضخمة من البنية التحتية لتكنولوجيا المعلومات لدى "أرامكو" وشلّ عملياتها التجارية. وربما تم تسهيل الهجوم

من قبل شخص من داخل الشركة الذي وفر معلومات عن الشبكة وتجاوز الصلاحيات بما يفسّر ربما سبب الاعتداء على جهة سعودية انتقاماً على الخطوات الأمريكية.

وفي المقابل خلّفت "عملية أبابيل" تأثيرات أقل بكثير كونها قطعت اتصال بعض المصارف الأمريكية بالإنترنت وعرقلت إمكانية وصول العملاء إلى خدماتها. ولا يُخفى أن "هجمات الحرمان من الخدمات" كانت كبيرة - إذ بلغت في ذروتها 70 جيجابايت (غيغابايت) في الثانية وهذا مستوىً عالٍ بمقاييس عام 2012 - إلا أنها لم ترقَ إلى مستوى "هجوم شامون" ما قد يشير إلى أن إيران اتخذت قراراً مدروساً بتكبيد الولايات المتحدة تكاليف خاطفة مع تجنب إلحاق أضرار جسيمة قد تدفعها إلى الانتقام.

تقييم خيارات إيران الإلكترونية

من المرجح أن تتخذ العمليات السيبرانية المستقبلية التي قد تشنّها إيران على الولايات المتحدة شكل هجمات مستهدفة ومعايرة ضد مؤسسات تجارية أو ركائز اقتصادية مهمة بهدف إلحاق ضرر وتكبيد خسائر مالية وعرقلة حياة الأمريكيين أو عملياتهم التجارية. ومن شأن خبرة إيران المتنامية في الهجمات بواسطة برمجيات المحو الخبيثة **(https://www.dhs.gov/cisa/news/2019/06/22/cisa-statement-iranian-cybersecurity-threats)** - مقرونةً بالمعلومات الاستخباراتية التي استخلصتها من عمليات التجسس السيبراني المتواصلة - أن تُعرّض مجموعة كبيرة من الجهات الأمريكية للخطر وتتحدّى قدرة واشنطن على تحديد الأهداف المحتملة.

لقد سبق أن شهدت الأزمة الراهنة أدلة على حدوث عمليات سيبرانية من كلا الجانبين. ففي الشهر الماضي شنّت الولايات المتحدة هجمات إلكترونية على أنظمة الأسلحة الإيرانية بعد أن قام النظام بإسقاط طائرة بدون طيار من نوع "آر كيو-4". وكشفت شركات الأمن السيبراني أيضاً استعدادات لساحة المعركة تقوم بها جهات فاعلة سيبرانية إيرانية وقد يكون في ذلك دلالةٌ على ما سيحدث فالإمكانيات الإيرانية الآخذة في التطور وعمليات التجسس المستمرة تشير إلى احتمال تعّرض الجهات الأمريكية لخطر كبير.

والجدير بالذكر أن إمكانيات إيران السيبرانية كانت أقل تطوراً بين عامَي 2012 و2014 واقتصرت هجمات الجمهورية الإسلامية عموماً على أحداث فردية بدلاً من حملات متواصلة. ومع ذلك تحذو طهران اليوم حذو الصين وروسيا والولايات المتحدة فتنفّذ عمليات استطلاع وتجسس طويلة المدى تمنحها إمكانية النفاذ والاستخبارات (على سبيل المثال البيانات والوثائق الشخصية خرائط مواطن الضعف والشبكات). وخلال العامين الماضيين كشفت شركات الأمن والحكومة الأمريكية عن عمليات تجسس سيبراني إيرانية تستهدف الجهات الحكومية الأمريكية والبنى التحتية الحيوية والملاحة العسكرية/التجارية وقطاعَي التصنيع والهندسة من بين قطاعات أمريكية أخرى. ووفقاً لبعض التقارير استهدف القراصنة الإيرانيين في المجال الألكتروني نظام أسماء النطاقات على الإنترنت وسحبوا من مزوّدي خدمات الشبكات الألكترونية وشركات الاتصالات بياناتٍ يمكن أن تسهل عملياتهم المستقبلية.

وإذا صعّدت إيران أعمالها إلى حد شنّ هجمات سيبرانية معطِّلة فبإمكان هذه الهجمات استهداف شبكة الكهرباء في الولايات المتحدة (التي سبق أن سبرت أغوارها) أو شبكات المياه (التي تسللت إليها) أو أنظمة الاتصالات السلكية واللاسلكية (التي استَخرجت منها البيانات) أو حتى الحكومات المحلية. وفي العام الماضي أدانت وزارة العدل الأمريكية شخصين إيرانيين بتهمة تنفيذ هجومٍ إلكتروني بواسطة ما يُعرف ببرنامج الفدية الخبيث ضد مدينة أتلانتا. وعلى الرغم من عدم ارتباط هذين الشخصين بالحكومة الإيرانية إلا أن الهجمات المدمّرة أو التضليلية تبقى ضمن إمكانيات طهران. وبالمثل فإن حلفاء الولايات المتحدة في الخليج قد يجدون أنفسهم أهدافاً مؤاتية للقراصنة الإيرانيين وخاصة السعودية التي تتعرّض للهجمات أو الاختراقات بشكل منتظم منذ عام 2013 على أقل تقدير.

وبما أن الولايات المتحدة لجأت إلى الأساليب السيبرانية للرد على أي هجومٍ حركي فقد لا تجد القيادات الإيرانية سبباً وجيهاً لأي تحفّظ استراتيجي في الفضاء السيبراني. وبالفعل فإن الرد الأمريكي المتحفظ قد يشجّع طهران على التحرك بقوة في هذا المجال اعتقاداً منها أن واشنطن ملتزمة بترددها في اتخاذ إجراء في المجالات العسكرية الأخرى. فالرئيس ترامب الذي غالباً ما يكرر شكوكه في الجهة التي تُسند إليها الهجمات السيبرانية الخارجية ضد أمريكا قد يعطي إيران حافزاً إضافياً شأنه شأن البيان الذي أشار فيه إلى أن إسقاط الطائرة بدون طيار ربما كان خطأ.

التخفيف من المخاطر السيبرانية الأمريكية

تمتلك مؤسسات القطاع الخاص وتُدير أيضاً معظم شبكات البنى التحتية الرئيسية في أمريكا مما يجعلها خارج نطاق الجهود المباشرة التي تبذلها الحكومة للدفاع عن شبكاتها. ومع ذلك يمكن لصانعي السياسات اتخاذ عدة تدابير لتعزيز الدفاعات السيبرانية الأمريكية وربما أيضاً إثناء إيران عن شن هجمات عبر استعراض القوة في الفضاء الإلكتروني.

فمن جهة يمكن أن تساعد مشاركة المزيد من المعلومات مع الأهداف المحتملة في القطاع الخاص في تعزيز البنى التحية الأساسية ودعم الأصول المهمة. وفي الوقت الحالي تقوم وكالات الاستخبارات بالمحافظة بشراسة على سرية المعلومات المتعلقة بالتهديدات السيبرانية مجادلةً بأن هذا الإجراء ضروري لحماية المصادر والأساليب والأدوات المعنية. ومع ذلك تمنع هذه السياسات الجهات الضعيفة من الحصول على معلومات حيوية تحتاجها للوقاية من الهجمات السيبرانية أو التخفيف من حدة عواقبها. صحيحٌ أن إدارة

الرئيس أوباما اتخذت خطوات أولية (**https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari**) لمعالجة هذه المشكلة في عام 2015 ولكن يجب بذل المزيد من الجهود إما لرفع السرية عن المعلومات ذات الصلة أو تزويد شركات البنى التحتية الرئيسية الموجودة خارج قطاع الدفاع بالمعلومات السرية المتعلقة بالتهديدات ومع امتلاك الجهات الخاصة للمعلومات الاستخباراتية المناسبة فقد تمكّنت من الدفاع عن نفسها ضد الهجمات - كما حدث في "عملية أبابيل" حيث أصبحت جهود القراصنة الإيرانيين في المجال الألكتروني غير فعالة بشكل متزايد مع قيام المصارف بتكييف أنظمتها الدفاعية

ومن جهة أخرى من الصعب ردع الهجمات السيبرانية عندما تكون الأطراف المعنية عديمة المعرفة تماماً بالقدرات الأمريكية وهذا لا يعني أنه ينبغي على الولايات المتحدة الكشف عن إمكانياتها السيبرانية بصورة كاملة ولكن بوسع وكالات الاستخبارات أن تتخذ خطوات محدودة لإظهار مدى قوتها في الفضاء السيبراني وإعطاء إيران أدلة على أنها قادرة على تهديد الأصول الإيرانية المرتبطة بشبكة الإنترنت ووضعها في خطر وبالمثل بإمكان الولايات المتحدة التواصل مباشرةً مع القراصنة الإيرانيين في المجال الألكتروني عبر شبكاتهم الخاصة لتبيّن لهم أنها تتعقب تحركاتهم في وقت حدوثها وهناك سابقة لهذا التكتيك الأخير حين نفّذت القيادة السيبرانية الأمريكية العام الماضي عملية مماثلة ضد عملاء روس مكلفين بنشر المعلومات المضللة وفي الواقع لا تستدعي هذه الجهود أعمالاً علنية عالية المستوى فاستعراضات القوة التي تنفَّذ في الخفاء قد تكون أكثر فعالية من ناحية إظهار إمكانيات الولايات المتحدة واهتمام واشنطن الصادق بتخفيف التصعيد وعلى الرغم من أن الاستعراضات وحدها ليست حلًّا طويل الأجل إلا أنها قد تحث إيران على إعادة تقييم حساباتها في الهجمات السيبرانية من ناحية مقارنة تكاليفها بمنافعها

وأخيراً يجب على صانعي السياسات توخي الحذر عند تحديد الخطوط الحمراء فيما يتعلق بالرد على الهجمات السيبرانية فالولايات المتحدة لا تريد أن تظّن إيران أن هذه الهجمات لا يترتّب عليها أي تكاليف ومع ذلك فإن التصريح عن خط أحمر محدد قد يحدّ من خيارات الرد الأمريكي أو يُحدث ثغرةً في المصداقية إذا فشلت واشنطن في كشف التهديد بدقة أو اتخاذ خطوات المتابعة اللازمة في أعقاب أي استفزاز سيبراني إيراني

ميكا لوديرميلك هو مستشار للأمن السيبراني ومحلل جيوسياسي مقره في الشرق الأوسط الآراء المُعرب عنها هنا خاصة بالكاتب فقط ❖

موصى به

BRIEF ANALYSIS

Iran Takes Next Steps on Rocket Technology

/ /

◆

Farzin Nadimi

(/policy-analysis/iran-takes-next-steps-rocket-technology)

تحليل موجز

السعودية تُعدّل تاريخها وتقلّص من دور الوهابية

فبراير

◆

سايمون هندرسون

(ar/policy-analysis/alswdyt-tudwl-tarykhha-wtqlws-mn-dwr-alwhabyt/)

BRIEF ANALYSIS

Targeting the Islamic State: Jihadist Military Threats and the U.S. Response

February 16, 2022, starting at 12:00 p.m. EST (1700 GMT)

◆

Ido Levy ,
Craig Whiteside

(/policy-analysis/targeting-islamic-state-jihadist-military-threats-and-us-response)

TOPICS

الطاقة والاقتصاد **(ar/policy-analysis/altaqt-walaqtsad/)** الخليج وسياسة الطاقة **(ar/policy-analysis/alkhlyj-wsyast-altaqt/)**

الشؤون العسكرية والأمنية **(ar/policy-analysis/alshwwn-alskryt-walamnyt/)** الإرهاب **(ar/policy-analysis/alarhab/)**

المناطق والبلدان

إيران **(ar/policy-analysis/ayran/)** دول الخليج العربي **(ar/policy-analysis/dwl-alkhlyj-alrby/)**