الوسائل السيبرانية: سلاح إيران المختار

بواسطة مايكل آيزنشتات (/ar/experts/maykl-ayznshtat-0)

يناير
متوفر أيضًا باللغات:
English (**/policy-analysis/cyber-irans-weapon-choice**)

عن المؤلفين

مايكل آيزنشتات (/ar/experts/maykl-ayznshtat-0)

مايكل آيزنشتات هو زميل أقدم ومدير برنامج الدراسات العسكرية والأمنية في معهد واشنطن

مقالات وشهادة

لأكثر من عقدٍ من الزمن تشنّ الجمهورية الإسلامية حملة مستمرة من التجسس الألكتروني تستهدف المعارضين الإيرانيين فبعد اكتشافها هجمات "ستكسنت" السيبرانية على برنامجها النووي في عام 2010 وفرضها عقوبات جديدة على النفط والقطاعات المالية الإيرانية ابتداءً من عام 2011 ردّت إيران على ذلك بشنها هجمات سيبرانية ضد أهداف من القطاع النفطي في المملكة العربية السعودية والقطاع المالي الأمريكي وفي غضون ذلك ضاعفت إلى حد كبير جهود التجسس الإلكتروني ضد المسؤولين الأجانب المنخرطين في السياسة الإيرانية خاصةً في الولايات المتحدة وأنشطة الاستطلاع السيبراني ضد بنى تحتية هامة في الولايات المتحدة وغيرها

وتسلط هذه الأحداث الضوء على الأهمية المتنامية التي تمنحها إيران لقدراتها السيبرانية التي من المرجح أن تضطلع بدور أكبر في السنوات المقبلة والسؤال الذي يطرح نفسه هنا ما الذي يفسّر اهتمام إيران بالوسائل السيبرانية أولاً يناسب هذا الاهتمام جيداً بعض عناصر الثقافة الاستراتيجية الايرانية أي تفضيل الغموض والفتور والمراوغة عند تنفيذ أنشطة قد تكون عالية المخاطر مما يخولها إدارة هذه المخاطر بشكلٍ أفضل وثانياً بسبب صعوبة تحميل المسؤولية لهجوم سيبراني بسرعة وبشكلٍ مقنع - حيث لا تعتمد التحاليل الجنائية السيبرانية على الأدلة الحسية بالمعنى التقليدي - فقد تستطيع طهران أن تنكر ذلك إلى حد ما

ثالثاً ما زالت القواعد السيبرانية الدولية غير مكتملة وتأمل إيران صياغتها لكي تبقى عمليات هجومها وتجسسها السيبرانية سلوكاً مسموحاً به تماماً كما يتقبل الكثيرون استخدامها للإرهاب ورابعاً تدعم أنشطة إيران السيبرانية مزاعم النظام في كون البلاد قوة علمية وتكنولوجية صاعدة وبالفعل تتمتع إيران بموارد بشرية من بين الأفضل عالمياً في هذا المجال فطالما تصدّر طلابها السباقات الأولمبية الأخيرة في العلم والتكنولوجيا والهندسة والرياضيات على الرغم من أن الظروف السياسية والاقتصادية في الداخل والفرص المغرية في الخارج غالباً ما تدفع الكثيرين إلى البحث عن العمل خارج البلاد

وأخيراً إن الوسائل السيبرانية تسمح لإيران بمهاجمة خصومها عالمياً وبشكل آني وعلى أساس مستدام كما تمكّنها من تحقيق آثار استراتيجية بأشكالٍ لا تستطيع اتباعها في المجال الحسي

غير أن خطر الهجمات السيبرانية ضد إيران له علاقة بمخاوف طهران الأعمق فبما أن الجمهورية الإسلامية تبوأت السلطة من خلال الثورة يُعتبَر الصمود هاجسها الرئيسي وتُعتبر الثورة المضادة كابوسها الأساسي فهي تعتقد أن الحرب الناعمة التي تشنها الولايات المتحدة - أي الجهود الرامية إلى غرس الأفكار والقيم والإيديولوجيات الأجنبية لتقويض الجمهورية الإسلامية التي غالباً ما تتم عبر وسائل سيبرانية كمواقع التواصل الاجتماعي والإنترنت - تشكّل خطراً على صمود النظام أكبر من خطر الهجوم أو الاجتياح العسكري

لذلك تعتقد طهران أن الوسيلة السيبرانية تُمكّن تنظيم خصومها المحليين وتهيئ أعداءها الأجانب لإضعاف النظام عبر حرب ناعمة لكنها توفّر أيضاً وسائل غير مسبوقة للنظام لمراقبة سكان البلاد وحماية نفسه من التهديدات المحلية والأجنبية ومهاجمة أعدائه

في العقد الماضي تطوّرت عدّة إيران السيبرانية من وسائل ضعيفة التقنية تمثلت في التهجم على أعدائها عبر تشويه المواقع وشن هجمات بهدف الحرمان من الخدمات إلى ركيزة أساسية لأمنها الوطني. وفي الواقع قد تكون الوسيلة السيبرانية هي الجزء الرابع الذي يُضاف إلى ثالوث القتال والردع الحالي في إيران. وحالياً يتشكل هذا الثالوث من قدرة تعطيل حركة النقل البحري في مضيق هرمز وممارسة إرهاب أحادي الطرف وبالوكالة على عدة قارات وإطلاق قذائف وصواريخ طويلة المدى ضد أهدافٍ في جميع أنحاء المنطقة.

إلا أن إيران لا تستطيع إغلاق مضيق هرمز دون الإضرار بمصالحها الخاصة إلى حد كبير لأن جميع صادراتها تقريباً من النفط والغاز وكل وارداتها تقريباً تعبر هذه النقطة الضيقة. بالإضافة إلى ذلك ضعفت قدرتها على ممارسة الإرهاب في السنوات الأخيرة فيما عزز خصومها قدرتهم على إعاقة أنشطتها الإرهابية إلى حد كبير منذ حوادث 9/11. وعلى الرغم من أن ترسانتها الصاروخية - وهي العمود الفقري لقوة ردعها الاستراتيجية - توفّر قدرات هامة فقد يعرّض استخدامها إيران إلى الرد المماثل لأنه يمكن التحقق بسهولة من مصادر الصواريخ.

وتنطوي العمليات السيبرانية على مخاطر أقل وتوفّر لطهران خيارات لا توفّرها الأجزاء الأخرى من ثالوثها الحالي. وبالتالي تنظر إيران بشكلٍ مؤكد تقريباً نحو استخدام الوسيلة السيبرانية على أرض المعركة لتعطيل الدفاعات الصاروخية للعدو وقدرته الخاصة بالقيادة والتحكم وأنظمته الجوية والبحرية غير المأهولة وخدماته اللوجستية - التي تُخزَّن في الولايات المتحدة على شبكات حاسوبية غير سرية. ويبدو أن أنشطة استطلاعها الشبكية تشير إلى أنها تُطور خطط طوارئ لمهاجمة البنى التحتية الحيوية الخاصة بأعدائها. كما قد تستهدف كيانات تعتقد أنها تُمكّن أنشطة الولايات المتحدة الخاصة بـ "الحرب الناعمة": كوسائل الإعلام وناشري الثقافة الشعبية ومراكز التفكير التي تُعتبَر معادية لإيران والجامعات والوكالات الحكومية الأمريكية التي تُعتبَر أنها تقود هذه الجهود. ويمكن أن تلجأ أيضاً إلى استهداف الثقافة ووسائل الإعلام التي تعتقد أنها سَخرت من حساسية قيادة البلاد أو أهانتها.

وتُظهر أنشطة إيران السيبرانية أن قوةً سيبرانية من الدرجة الثالثة قد تسبب إزعاج كبير وتستطيع أن تنفذ هجمات مكلفة مع أنها لم تُثبت بعد قدرةً على شن هجمات استراتيجية على بنى تحتية هامة. وعلاوةً على ذلك تُظهر تجربة الولايات المتحدة مع "ستكسنت" أنه حتى القوى السيبرانية المتقدمة قد تواجه تحديات في تحقيق آثار استراتيجية نظراً لتعقيد الهدف والقيود - المفروضة ذاتياً أو غير ذلك - على سير العمليات السيبرانية الهجومية. ومع ذلك قد لا ينطبق هذا التقييم على جميع أنواع أهداف البنى التحتية ويمكن أن يتغيّر في الوقت الذي تصبح فيه أدوات الهجوم والاستطلاع السيبرانية أكثر تطوراً.

لقد أظهرت إيران أنها تفضّل الرد المشابه على الهجمات السيبرانية على الرغم من أنه إذا تم إحباطه فليس من الواضح ما إذا كانت سترد في المجال الحسي. ومع ذلك فبما أن أداء الاقتصاد والبنية التحتية الأساسية والقوات العسكرية في الولايات المتحدة يعتمد على شبكات حاسوبية هشة نسبياً من المرجح أن تجد إيران دائماً طريقةً للرد المماثل وإن كان ذلك رمزياً. وبما أن أمريكا تعيش في "بيتٍ سيبراني من زجاج" فقد تكون الطريقة الأكثر فعالية لردع أعداءٍ في المجال السيبراني كإيران هي من خلال التهديد بعمل عسكري في المجال الحسي.

بيد ما زالت الولايات المتحدة تعاني منذ وقتٍ طويل من ثغرة في المصداقية قد تعقّد مثل هذه الجهود. فردة فعلها الصامتة على تفجيري "ثكنات المارينز في بيروت" في عام 1983 و"أبراج الخبر" في عام 1996 وعلى دعم إيران لجماعات شيعية متطرفة هاجمت القوات الأمريكية في العراق بعد اجتياحها البلاد في عام 2003 علّمت إيران أنها تستطيع شن حرب بالوكالة ضد الولايات المتحدة من دون خطر تلقي رد عسكري أو دفع ثمن غير مقبول. وربما أدى تبني واشنطن لـ "ستكسنت" من أجل تفادي ضربة عسكرية إسرائيلية على البرنامج النووي الإيراني إلى تعزيز التصور المتمثل في كونها غير مستعدة لمواجهة طهران في المجال الحسي. وما يتناقض مع ما سبق هو أن الاستخدام الأساسي للهجوم السيبراني ربما قد أضعف قوة الردع السيبرانية من دون قصد. وسيكون ردم هوة المصداقية مفتاح الجهود المستقبلية لردع إيران في المجالين السيبراني والحسي.

مايكل آيزنشتات هو زميل "كاهن" ومدير برنامج الدراسات العسكرية والأمنية في معهد واشنطن. ❖

"سايفر بريف"

موصى به

BRIEF ANALYSIS

Unpacking the UAE F-35 Negotiations

/ /

◆

Grant Rumley

(/policy-analysis/unpacking-uae-f-35-negotiations)

ARTICLES & TESTIMONY

How to Make Russia Pay in Ukraine: Study Syria

/ /

◆

Anna Borshchevskaya

(/policy-analysis/how-make-russia-pay-ukraine-study-syria)

تحليل موجز

مواجهة أزمة الغذاء في سوريا

فبراير

◆

عشتار الشامي

(ar/policy-analysis/mwajht-azmt-alghdha-fy-swrya/)

TOPICS

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

المناطق والبلدان

إيران **(ar/policy-analysis/ayran/)**