النشاط السيبراني الإيراني ، ما بين السرية والعلن

د. محمد فريد عزي

باحث رئيسي - إدارة البارومیتر

د. هدى النعيمي

مستشار الإسلام السياسي

عبدالله خليفة مترف

باحث رئيسي - رئيس وحدة الدراسات الإيرانية والتركية

/https://trendsresearch.org/ar/insights

مقدمة

تعتبر إيران من أولى الدول الإقليمية التي دشنت حضورها في الفضاء الإلكتروني منذ عام 1993، وسبقت غيرها في الوصول إلى شبكة الإنترنت والتكنولوجيا الإلكترونية، لكنها سرعان ما بدأت في البحث عن الوسائل الكفيلة للحد من التدفق الحر للمعلومات لكبح حرية التعبير. وهكذا تبلور عمل حكومي إلكتروني، ظهرت بوادره الأولية في شبكة من الفاعلين على الإنترنت، في محاولات لفرض الرقابة والتدخل فيما يكتبه، أو يتحدث به، أو ما يتصرفه المعارضون للنظام أو الناشطون على وسائل التواصل الاجتماعي.

على أن إيران ما بعد الشاه تبنّت نهجاً من السيطرة المركزية على المعلومات، وأوجدت وزارات حكومية مخصصة للإشراف على وسائل الإعلام المختلفة، كما تبنّت ضوابط صارمة تحظر توجيه انتقادات للمرشد الأعلى وحكومته. وغالباً ما يأتي تصنيف منظمة

"مراسلون بلا حدود" لإيران على أنها واحدة من أكثر الدول قمعية في العالم فيما يتعلق بحريات الصحافة.[1]

وستحاول هذه الورقة تبيان أهداف البرنامج السيبراني الإيراني، والجهود التي بذلت لتطويره، والتعرف على قدرات هذا البرنامج مع عرض نماذج لهجمات إلكترونية إيرانية طالت مؤسسات غربية وعربية، بالإضافة إلى تسليط الضوء على الجهات الفاعلة التي تشن الحملات السيبرانية داخل إيران وخارجها.

-أهداف البرنامج السيبراني الإيراني

للبرنامج السيبراني الإيراني أهداف عدة؛ يرتكز أغلبها على منع حدوث هجوم آخر مماثل لما حدث في هجوم ستوكسنت Stuxnet في عام 2010 الذي تسبّب في إحداث أضرار جسيمة في المفاعلات النووية الإيرانية؛ ليس في إبطاء شبكة نظامها فحسب، وما نتج عنه من خسائر وإصابات مادية حقيقية، وكأن أجهزة الطرد المركزي قد تعرَّضت للقصف مع انخفاض بنسبة 30٪ في كفاءة التخصيب[2]. بل في تجنب حدوث اختراق لأجهزة الكمبيوتر الإيرانية بواسطة فيروسات أيضاً، مثل التي أوقعها فايروس Flame في عام 2012، الذي عمل على محو البيانات فيها. وقد كشفت شركة "كاسبر سكاي لاب" أن هذا الفيروس يمكنه سرقة معلومات مهمة محفوظة في الحواسيب إلى جانب معلومات في أنظمة مستهدفة بعينها[3].

وبالاتجاه نفسه، تسعى إيران لكبح جماح الأنشطة الإلكترونية وإحباطها لأحزاب المعارضة المحلية ومعارضي النظام، الذين يمثل الفضاء الإلكتروني بالنسبة إليهم منصة اتصالات مهمة لنشر المعلومات وتنظيم الأنشطة المضادة. بالإضافة إلى ذلك، يأمل النظام في منع اختراق الفضاء الإلكتروني الداخلي بالأفكار والمعلومات الغربية التي تتعارض مع الرؤية الإيرانية.

ويقف انعدام الثقة والمواجهة المستمرة بين إيران والولايات المتحدة، متغيراً رئيسياً خلف المسعى الإيراني في تطوير أنظمة ذكية، تعزز من القوة غير المتماثلة، وتحول دون تحرك المجتمع الدولي باتجاه تغيير النظام. فهي تعتقد أن الحرب الناعمة التي تشنها الولايات المتحدة – أي الجهود الرامية إلى غرس الأفكار والقيم والأيديولوجيات الأجنبية لتقويض نظامها، والتي غالباً ما تتم عبر وسائل سيبرانية كمواقع التواصل الاجتماعي والإنترنت – تشكّل خطراً على صمود النظام، ولها تأثير أعمق من خطر العمل العسكري.

ولهذا، فإن الاعتماد على الذات سيحرر طهران من محددات دولية تمنعها من اكتساب التقنيات المتطورة، ويمكّنها في الوقت نفسه من تطوير تقنيات عسكرية محلية غير مكلفة، تُحدث تأثيرات عملياتية كبيرة في مشهد التنافسين الإقليمي والدولي في المنطقة. خصوصاً أن موقع إيران الجيوسياسي يتموضع في منطقة تشهد حضوراً كثيفاً لمصالح دولية وإقليمية متنافسة وأحياناً متضاربة.

وعلاوة على ما تقدم، تهدف استراتيجية إيران إلى توسيع قوتها وتعزيز حضورها الإقليمي، وتجنب القيود الشديدة على قدراتها العسكرية التقليدية. وبحسب ما جاء في تقرير صدر عام 2019 عن المعهد الدولي للدراسات الاستراتيجية، فإن العقوبات والقيود الدولية على واردات الأسلحة جعلت من الصعب على إيران تطوير أو شراء أسلحة تواكب التطورات العسكرية والتقنية.[4]

ولهذا، تُعدّ الحرب الإلكترونية أداة مهمة لتضخيم قوة إيران وتقوية مكانتها وممارسة نفوذها على الصعيدين الإقليمي والدولي، لذلك انخرط عدد من قادة الجيش والبحرية والقوات الجوية والدفاع الجوي والحرس الثوري الإيراني، وقوات الشرطة في سبتمبر 2013 في برنامج الأمن السيبراني في جامعة القيادة والسيطرة التابعة للجيش الإيراني للتدريب على الأجهزة والبرامج، ومواجهة وتحليل وإعداد رد فعل مناسب ضد التهديدات السيبرانية"[5].

وبالسياق نفسه، طوّرت إيران ردود أفعال غير متماثلة كالصواريخ الباليستية والطائرات من دون طيار، بالإضافة إلى الميليشيات الموالية لها في العراق وسوريا ولبنان واليمن، وبناء شبكة قرصنة إلكترونية، بهدف التمكن من إيقاع الخسائر بالعدو، وتجنب المواجهة في ساحة المعركة التقليدية.

ومن هنا، تشكل الهجمات الإلكترونية جزءاً من سلسلة متصلة من الصراع، وبهذا الصدد قال قائد الحرس الثوري الإيراني حسين سلامي؛ "نحن في جو حرب استخباراتية شاملة مع الولايات المتحدة، وجبهة أعداء الثورة والنظام الإسلامي.. هذا الجو هو مزيج من الحرب النفسية والعمليات الإلكترونية والاستفزازات العسكرية والدبلوماسية العامة، وتكتيكات التخويف"[6].

وغالباً ما يصعب تحديد المسؤول عن الهجمات السيبرانية، وبحسب مايكل آيزنشتات[7]، فإن الغموض والفتور والمراوغة عند تنفيذ أنشطة قد تكون عالية المخاطر، يتوافق مع بعض عناصر الثقافة الاستراتيجية الإيرانية القائمة على التقية والمواربة، وهو ما يخولها إدارة هذه المخاطر بشكلٍ أفضل.

وعلى هذا الأساس، فإن من الصعوبة بمكان تحميل المسؤولية بسرعة وبشكلٍ مقنع عن هجوم سيبراني – حيث لا تعتمد التحاليل الجنائية السيبرانية على الأدلة الحسية بالمعنى التقليدي – وبالتالي تستطيع طهران وإلى حدٍّ ما أن تنكر قيامها بهذا العمل. ويشير النمو في الحجم والتعقيد الذي أظهره المشغلون السيبرانيون الإيرانيون إلى أن التهديد من هذه المجموعات مستمر في التسارع، وأن مواجهته تتطلب أشكالاً جديدة ومبتكرة من أساليب الدفاع الرقمي.

ويسمح النشاط السيبراني بمعاقبة الخصوم الأيديولوجيين وتشويه سمعتهم، وقد اعتمدته طهران في شن هجمات "انتقامية" ضد أعدائها، ولا سيما المملكة العربية السعودية والولايات المتحدة الأمريكية. ويُعتقد أن القراصنة الإيرانيين كانوا وراء الحملات المصممة

لتعطيل مجموعة متنوعة من كيانات الحكومة والقطاع الخاص الأمريكية أيضاً، لتشمل البنوك والفنادق، والانتخابات الرئاسية الأمريكية. ومن المحتمل أن تكون مثل هذه العمليات السيبرانية مصممة لإظهار القوة وتقديم تحذيرات للدول أو الشركات الأخرى التي تمارس ضغوطاً في التعامل على إيران[8].

- **الجهود الإيرانية السيبرانية**

تعبر الجهود السيبرانية الإيرانية عن مجموعة من الأنشطة التي يديرها أفراد عبر الإنترنت لتحقيق هدف معين: يراد منه تعزيز التحكم الأيديولوجي في المجتمع، أو شل قدرة الخصم وتحييده عن تحقيق أهدافه من خلال الاضطراب والتدمير والارتباك والخداع وعدم الثقة[9]. ناهيك عن كونه في أحد وجوهه استعراضاً للقوة، وتفاخراً إيرانياً بما تتوافر عليه من قدرات وقوة.

وتسمح العمليات الإلكترونية بسرقة الملكية الفكرية لتعزيز ميزتها التنافسية، من خلال التركيز على تقنيات الدفاع والمعلومات. وبحسب تقرير عام 2018 الصادر عن مركز مكافحة التجسس والأمن القومي الأمريكي الذي أكد "أن إيران ستواصل العمل على اختراق شبكات الولايات المتحدة لأغراض التجسس الاقتصادية أو الصناعية، إذ سيعتمد الاقتصاد الإيراني – الذي لا يزال مدفوعاً بشكل كبير بالعائدات النفطية – على النمو في الصناعات غير النفطية ومن المتوقع أن تستمر إيران في استغلال الفضاء الإلكتروني لاكتساب مزايا في هذه الصناعات بعد أن أصبحت محاولات القرصنة الإيرانية الآن تهديداً إلكترونياً مستمراً[10].

وتمتلك إيران شبكة ضخمة من الأشخاص عبر الإنترنت، التي بدأت بالتشكل منذ عام 2008، وقد استهدفت عملياتها عشرات الدول، تفاوتت في رسائلها ومقاصدها. ويمكن للمتتبع أن يستنتج الكثير عن الجهات الفاعلة المتنوعة التي تنشر الدعاية نيابة عن

الحكومة الإيرانية، بالإضافة إلى الأهداف المختلفة التي تنوي إيران تحقيقها في عدد من الدول.

وتأسيساً على ما تقدم، صرح المرشد الأعلى علي خامنئي في عام 2009، أن "ترويج المحتوى" يعد "السلاح الدولي الأكثر فاعلية" ضد الأعداء الأجانب. وفي عام 2011، تفاخر رئيس الإذاعة الإيرانية بأنه طوّر سبع كتائب إلكترونية من "خبراء الإعلام والمتخصصين"، تتكون من 8400 عضو. بالإضافة إلى قيام الحرس الثوري الإيراني بتدريب الآلاف من المجندين على "إنتاج المحتوى"، وتعليمهم استراتيجية وسائل التواصل الاجتماعي والتصميم الجرافيكي[11].

وينشط على منصات التواصل الاجتماعي الآلاف من وكلاء النظام الإيراني ففي يناير 2020، حدد موقع Facebook 766 صفحة يتابعها 5.4 مليون مستخدم؛ و344 حساباً على إنستغرام يتابعه 439 ألف مستخدم، كما أشار Facebook إلى 43 حدثاً حصل من خلاله المؤثرين الإيرانيين على 57 ألف دولار من الإعلانات، وكشف موقع Twitter عن 7.896 حساباً يدعم طهران وسياساتها، فيه ما يقرب من 8.5 مليون تغريدة [12] .

وتعد الحملة الانتخابية الرئاسية في عام 2009، لحظة فارقة على صعيد العمل السيبراني، مع انبثاق "الحركة الخضراء" التي قادت احتجاجات شعبية حاشدة ضد فوز الرئيس الإيراني الأسبق محمود أحمدي نجاد بولاية حكم ثانية، لتتصاعد الحملة الحكومية الإلكترونية ضد المعارضة من حيث النطاق والشدة، بعد أن تشكلت قوة إلكترونية، اتخذت عدداً من التكتيكات تراوحت ما بين إنتاج المحتوى والقرصنة، واتخذت وجوهاً متعددة من الأنشطة التي يتم القيام بها على الإنترنت، بهدف تعزيز قوة الدولة وزيادة سيطرتها على الخطاب الإلكتروني والحد من الفضاء المعارض.

وعليه، تستخدم إيران العمليات الإلكترونية لجمع المعلومات الاستخباراتية وإجراء عمليات التجسس، إذ يستخدم النظام الإنترنت لـ"إسكات" معارضيه و"إضعافهم" في الداخل، ووفقاً لتقرير وزارة الخارجية الأمريكية لعام 2018، فإن معظم ضحايا العمليات الإلكترونية للنظام هم مواطنون إيرانيون يعيشون داخل إيران أو خارجها[13].

تنشط الشبكات السيبرانية الإيرانية من خلال استخدام الوكلاء، من خبراء تكنولوجيا المعلومات من الشباب البارعين، والمدربين على القرصنة والمراقبة، كما أنها تتمتع بالسرية بشأن هيكلها وروابطها المباشرة مع المؤسسات الأمنية والعسكرية الإيرانية، فضلاً عما تلقاه من الدعم والحصانة القانونية.

ويبدو أن هذه الأنشطة والأولويات تتماشى بشكل مباشر مع خطاب خامنئي للحرب الناعمة، الداعي إلى خوض حرب أيديولوجية ناعمة سيبرانية. ففي خطابه الموجه للأكاديميين في 30 أغسطس 2009، تحدّث المرشد عن الحاجة الملحّة لخوض حرب أيديولوجية ناعمة في عالم الإنترنت، وهو موقف يُنظر إليه بمنزلة الدعوة لحمل السلاح ولا سيما من قِبل الحرس الثوري الإيراني[14].

وبالمعنى نفسه، شرعت إيران خلال العقد الماضي في توسيع منظومتها الإلكترونية الوطنية مع إنشاء وكالات ومنظمات الفضاء الإلكتروني للإدارات الحكومية كلها، بهدف تأسيس تنظيم هرمي سيبراني متنوع مع خطة عمل واضحة وتخصيصات مدروسة للموارد وتوزيع المسؤولية والقدرة على حفظ المعلومات ونشرها وإدارة المعرفة والبيانات.

ولهذا، يدير الحرس الثوري الإيراني برنامجاً موسعاً للأنشطة السيبرانية منذ ولاية أحمدي نجاد الثانية، وبدأ في تجنيد محترفين لقوته الإلكترونية. كما يقوم معهد رانا للحوسبة الذكية، وهي منظمة تعمل تحت إشراف وزارة الداخلية الإيرانية، بأعمال التجسس، وتطوير الأدوات السيبرانية لمساعدتها على الوصول إلى مجموعة متنوعة من البنى التحتية للدول الأجنبية، ناهيك عن مراقبة ما يطرحه المواطنون من محتوى داخل إيران وخارجها[15].

وبالاتجاه نفسه يعتبر قائد المقر الافتراضي لهيئة أركان القوات المسلحة الإيرانية العميد بهروز إثباتي، المجال السيبراني منطلقاً لجبهة جديدة في الحرب بين النظام الإيراني والغرب، وخاصة مع الولايات المتحدة[16].

وتأسيساً على ما تقدم، تأتي اتفاقيات التعاون السيبراني الروسية الإيرانية لتوسيع الجهود المشتركة لمواجهة الأعداء المشتركين، وتعزيز التعاون واسع النطاق في مجال الأمن السيبراني، بما في ذلك تنسيق الإجراءات، وتبادل التقنيات، وتدريب المتخصصين، والتنسيق في الأمم المتحدة والمنظمات الدولية الأخرى[17].

- **علاقات إيران.. فرص لتطوير برنامجها السيبراني**

كما هو معروف تمت أول صفقة إلكترونية روسية – إيرانية في عام 2015، التي قال رئيس منظمة الدفاع المدني الإيرانية؛ إنها ضرورية لأن البلدين يواجهان أعداء مشتركين في الفضاء الإلكتروني. وفي عام 2017، وقّعت موسكو وطهران مذكرة تفاهم للتعاون بشأن القضايا المتعلقة بتكنولوجيا المعلومات والاتصالات، بما في ذلك "حوكمة الإنترنت، وأمن الشبكة" والاتصال الدولي بالإنترنت"[18].

وفي عام 2018، وبمبادرة من طهران، أنشأ الجانبان لجنة ثنائية للتعاون الإعلامي، تهدف إلى مكافحة ما وصفه رئيس وفد طهران بـ" الإرهاب الإعلامي" الغربي. وتعمل اللجنة على قضايا مثل تبادل الصحفيين، وتوفير التغطية الإعلامية المتبادلة، والقيام بإنتاج محتويات مشتركة، ومواجهة روايات وسائل الإعلام الغربية، كما قدمت روسيا للإيرانيين تدريبات على منصات وتقنيات إعلامية جديدة[19].

ومن المرجح، أن تقوم روسيا بتزويد طهران بأنظمة الدفاع الإلكتروني وتدريب كوادرها على معالجة أوجه القصور الدفاعية لديها، الأمر الذي سيجعل الهجمات الإلكترونية المحتملة ضد الأهداف الإيرانية أكثر تكلفة وصعوبة في المستقبل. علاوة على ذلك،

يمكن لإيران بدورها توفير التقنيات الروسية لوكلائها في المنطقة، مثل: "حزب الله"، وميليشيا الحوثي، والميليشيات الطائفية في العراق، التي يمكن استخدامها ضد أهداف خليجية، كما بالإمكان إرسال فرق إلكترونية روسية إلى إيران لمراقبة الشبكات الإيرانية وفحص البرامج الضارة الأمريكية أو الإسرائيلية المستخدمة ضدها، ما يساعد كلا البلدين على تعزيز قدراتهما الدفاعية ضد الهجمات السيبرانية المستقبلية.[20]

ونستنتج مما تقدم، أن طهران تواصل سعيها لتكون لاعباً إلكترونياً عالمياً، عبر تعزيز قدراتها على مستوى الهجوم السيبراني وتوسيع وصولها إلى البنية التحتية والأنظمة الإلكترونية الأجنبية، كما أكد العميد غلام رضا جلالي، رئيس منظمة الدفاع المدني الإيرانية، مؤخراً، إمكانية جعل الدفاع الإلكتروني بمنزلة ضمان لاستقلال البلاد وأمنها. وصرح جلالي أنه "في الفضاء الإلكتروني، نواجه مجموعة من الفرص والتهديدات. لا يمكننا التركيز على الفرص فقط ولكن يجب علينا تبنّي نظرة أكثر شمولاً في هذا المجال من خلال تحديد التهديدات. من ناحية أخرى، يجب أن نركز على توطين البنى التحتية في مجال التكنولوجيا"[21].

وليس من المستبعد أن يضم اتفاق التعاون الاستراتيجي بين الصين وإيران في بعض بنوده ما يتعلق بالسيطرة على الفضاء الإلكتروني أيضاً، وبهذا الصدد أكد محمود نابافيان، نائب رئيس اللجنة البرلمانية للمادة 90، في مقابلة نُشرت في وكالة "مهر" للأنباء في 11 إبريل 2021 أن إيران فقدت السيطرة على الإنترنت داخل البلاد، وأنه من المهم إعادة تأكيد سيطرتها بمساعدة الصينيين. كما أشار نابافيان، إلى ضرورة إعادة ممارسة السيطرة على "محركات البحث ووسائل التواصل الاجتماعي والبريد الإلكتروني" كأهداف رئيسية لإيران في التعاون الأمني الرقمي مع الصين.[22]

- **نماذج من هجمات إلكترونية إيرانية**

يعد فايروس ستوكسنت **Stuxnet** أول سلاح رقمي في العالم استهدف على وجه التحديد منشآت التخصيب النووي الإيرانية، ونجح في شلها منذ نحو عقد من الزمان[23]، وحفز طهران على التعاطي مع الأنشطة الإلكترونية لتتجه بدورها إلى الاستثمار في البنية التحتية السيبرانية العسكرية، مدعومة بتصورات التفوق التي تتحلى بها الشخصية الإيرانية، والتأكيد على ما تتمتع به من قدرات تضعها في خانة المساواة التكنولوجية مع الدول المتقدمة.

ومنذ ذلك الحين، اتُهمت إيران بارتكاب عدد من الهجمات الإلكترونية. من أشهرها ما تعرضت له شركة نفط أرامكو السعودية في أغسطس عام 2012 عندما أدى الفيروس "شمعون" إلى تدمير بيانات نحو 30 ألف جهاز كمبيوتر[24].

لتعقبها "عملية أبابيل" التي تزامنت مع قيام الإدارة الأمريكية بفرض 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، فإن "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[25]. ومع أن مجموعة من القراصنة تطلق على نفسها اسم "المقاتلين الإلكترونيين في كتائب عز الدين القسام" قد تبنّت المسؤولية عن عملية "أبابيل"، وبحسب ما أوردته ميكا لوديرميلك فإن الحكومة الإيرانية قد أوعزت بهذا الهجوم[26]. وفي إطار الكشف عن هذه العملية وجهت الولايات المتحدة تهماً ضد سبعة متسللين إيرانيين، متهمين بشن هجمات على مجموعة من البنوك الأمريكية، أوقعت خسائر مالية تقدر بعشرات الملايين من الدولارات[27].

وكان من المتوقع، أن تزيد طهران من أنشطتها الإلكترونية بشكل كبير بعد مقتل الجنرال قاسم سليماني، إذ حذر خبراء الأمن السيبراني الأمريكي من رد فعلها على مقتله، وشدد خبراء على ضرورة استعداد الولايات المتحدة لاحتمال هجمات إلكترونية إيرانية جريئة، تهدف إلى إلحاق أضرار مالية كبيرة أو تهديد أرواح الأمريكيين كرد انتقامي.

وبرغم ذلك، لم تستهدف الهجمات السيبرانية التي قامت بها طهران أياً من المنشآت ذات الأهمية الكبرى كالمؤسسات النفطية، أو شبكات النقل، أو القيادة العسكرية، لأن القيام بهذا النوع من الهجمات سيتم مرة واحدة، نظراً إلى صعوبة تكرار أسلوب الهجمة نفسها[28].

ومن الواضح أن إيران لن تذهب باتجاه خيار القيام بهجوم إلكتروني مباشر يمكن أن يؤدي إلى رد فعل مسلح، وهو أمر تتجنبه طهران التي تميل إلى اعتماد البراغماتية في أغلب مواقفها. ولهذا فمن المحتمل أن نرى المزيد من الهجمات الخفية التي يصعب إسنادها مباشرة إلى إيران.

وتعتقد يانا بوبكوستوفا، مديرة المركز الأوروبي للطاقة والتحليل الجيوسياسي، أن إيران تبذل قصارى جهدها لمنع مواجهة عسكرية مباشرة مع الولايات المتحدة الأمريكية، وعوضاً عن ذلك تحاول إضعاف أعدائها بهجمات إلكترونية[29]. وبالاتجاه نفسه يقول فيليب إنغرام، الكولونيل السابق في المخابرات العسكرية البريطانية؛ "تمتلك إيران نطاقاً واسعاً ومتطوراً للغاية من القدرات لاستهداف البنية التحتية الوطنية المهمة، والمؤسسات المالية، والمؤسسات التعليمية، والمصنعين، وأكثر من ذلك". ويحذر من أن إيران لديها "القدرة على شن الهجوم الإلكتروني الأول"[30].

وتأكيداً على ما تقدم، نفذ قراصنة إيرانيون أطلقوا على أنفسهم اسم "القطة الساحرة" من خلال انتحال شخصية أستاذ وباحث جامعي بريطاني، خرقاً لموقع إلكتروني تابع لكلية الدراسات الشرقية والأفريقية في جامعة لندن؛ بهدف قرصنة بعض المعلومات الشخصية عن باحثين وأساتذة معظمهم من الولايات المتحدة وبريطانيا.

كما استهدفوا ما لا يقل عن 13 بريداً إلكترونياً شخصياً لموظفي وزارة الخزانة الأمريكية، واحداً يخص مديراً في شبكة إنفاذ الجرائم المالية، التي تحارب غسل الأموال وتمويل الإرهاب، وآخر يستخدمه رئيس التراخيص في مكتب مراقبة الأصول الأجنبية، المسؤول عن تطبيق العقوبات الأمريكية[31].

- **الهيكل السيبراني الإيراني**

يعتبر العديد من الباحثين أن الاختراق الإيراني الإلكتروني كان سريعاً، وقد مكّنها من بناء قدرة إلكترونية تنافس الولايات المتحدة والصين وروسيا والمملكة المتحدة وإسرائيل، وهي الدول الفاعلة الأكثر هيمنة في الفضاء الإلكتروني. ووفقاً لوثائق وكالة المخابرات الأمريكية التي نشرها إدوارد سنودن في عام 2013، كثفت إيران من مراقبتها لحكومة الولايات المتحدة. وتصف إحدى هذه الوثائق، التي كتبها الجنرال كيث ألكسندر، المدير السابق لوكالة الأمن القومي، التهديد بأنه خطير بما يكفي لأن تطلب الولايات المتحدة المساعدة من بريطانيا في احتواء الضرر الناجم عن "اكتشاف إيران لأدوات استغلال شبكات الكمبيوتر"– وهو مصطلح يعبر عن الأسلحة السيبرانية[32].

ويرجع التطور السريع في قدرات إيران السيبرانية، إلى فايروس Stuxnet الذي ضرب البرنامج النووي الإيراني، وأوقع فيه ضرراً كبيراً، ففي وثيقة أخرى سربها سنودن، ذكرت وكالة الأمن القومي الأمريكية أن إيران "أظهرت قدرة واضحة على التعلم من قدرات الآخرين وتصرفاتهم"[33].

وتبدو إيران بارعة في بناء الشبكات الإلكترونية في جميع أنحاء العالم، وتستخدم طريقة غير مكلفة للتدريب والتعاون مع الوكلاء، كما تدعم القدرات الإلكترونية لأذرعها العسكرية في لبنان واليمن وسوريا والعراق. ففي يوليو 2012، خصص النظام الإيراني مليار دولار لتعزيز القدرات السيبرانية للبلاد، والاستثمار في التقنيات الهجومية والدفاعية الجديدة

وتوظيف كادر من القراصنة السيبرانيين وتدريبهم. بالتوازي مع ذلك، قامت إيران بتشكيل مجموعة متنوعة من الوكالات المحلية المكلفة بإدارة شؤون الفضاء الإلكتروني[34].

وفي أدناه بعض الجهات التي تُصدر قرار تنظيم الحملات السيبرانية في إيران أو ممن تشرف على تنفيذه:

– **المرشد الأعلى علي خامنئي** – صانع القرار النهائي في جميع قضايا الأمن الداخلي والوطني؛ يمارس سيطرة مباشرة على الحرس الثوري الإيراني والقوات المسلحة والأجهزة الأمنية.

– **المجلس الأعلى للأمن القومي:** أعلى هيئة لصنع سياسات الأمن القومي. يتلقى توجيهات من المرشد الأعلى؛ ويضم في عضويته رئيس الجمهورية، ورئيس البرلمان، ورئيس القضاء، والوزراء، وقادة الجيش[35].

– **المجلس الأعلى للفضاء الإلكتروني:** يشرف على سياسة الإنترنت والفضاء الإلكتروني؛ ويقدم تقاريره إلى المرشد الأعلى علي خامنئي، ويضم في عضويته الرئيس والوزراء وقائد الحرس الثوري الإيراني وغيرهم من كبار المسؤولين من أجهزة المخابرات والأمن، ترتكز مسؤوليته في حماية البلاد من المحتوى السلبي للفضاء السيبراني[36].

– الحرس الثوري الإيراني

بالإضافة إلى وحدات الحرب الإلكترونية التابعة له، يستعين الحرس الثوري بمجموعات من المتسللين الإيرانيين الناشطين في الداخل والخارج، للتمويه عن أنشطته السيبرانية، ودحض أي مزاعم بتورط إيران في الحرب الفضائية وجرائم الإنترنت.

ويتعاون مع الحرس الثوري فريق Ashiyane Digital Security، لتدريب المتسللين على العمل في الأنشطة السياسية والدعائية الموالية لإيران في مواقع التواصل الاجتماعي

والمنتديات الغربية والإسرائيلية، والتسبب بأعطالها، بالإضافة إلى القيام بالاحتيال الائتماني، والتسلل إلى قواعد البيانات والمؤسسات المالية[37].

– وحدات الباسيج

تشارك وحدات الباسيج غير العسكرية بنشر التعليقات على الكثير من المواقع، وهم مشغلون غير محترفين وعديمي الخبرة، يقومون بعمليات اختراق أو تسلل بسيطة ضد أعداء النظام في الداخل[38].

- **الشرطة الإلكترونية (FETA)**

تعمل على "التحكم" في مستخدمي الإنترنت، من خلال ممارسة الضغط على مزودي خدمة الإنترنت، وإجبارهم على تقديم معلومات عن مستخدمي الشبكة. وهي مسؤولة كذلك عن مكافحة ما يسمى "بالجرائم السياسية والأمنية"، من خلال استخدام مجموعة من المتسللين لاختراق المواقع وحسابات البريد الإلكتروني للمعارضين[39].

- **لجنة تحديد المواقع غير المصرح بها**

تشكلت في يوليو 2009 من قِبل المجلس الأعلى للثورة الثقافية الذي يخضع لسيطرة المرشد الأعلى، وتعمل على تحديد المواقع التي لم يوافق النظام على عملياتها لأسباب مختلفة، تتألف هذه اللجنة من أعضاء، مثل: النائب العام، والقائد العام للشرطة، ورئيس جهاز الإذاعة والتلفزيون الحكومي، ووزراء الثقافة، والاستخبارات، والاتصالات، والعلوم[40].

وخلال المفاوضات النووية، انخرطت إيران بين الأعوام 2013 و2017 في حملة تجسس إلكتروني، بتوجيه من الحرس الثوري الإيراني، حيث تسلل قراصنة إيرانيون إلى مئات الجامعات والشركات الخاصة والوكالات الحكومية في الولايات المتحدة وحول العالم،

وسرقوا أكثر من 30 تيرابايت من البيانات الأكاديمية والملكية الفكرية[41]. وقد أنفقت الجامعات المتضررة نحو 3.4 مليار دولار على خدمات الاشتراك وحدها للوصول إلى البيانات المعنية[42].

وفي ضوء ما تقدم تشير التطورات إلى ظهور حقبة جديدة من السيبرانية قد لا تصل تفاعلاتها إلى مستوى استخدام القوة أو الحرب، ولكنها تسعى إلى تحقيق تأثيرات استراتيجية أو تكتيكية محددة تؤثر في سلوك الدول المعادية.

وأخيراً، تعد التهديدات السيبرانية ظاهرة عالمية تتطور باستمرار من خلال شبكات جيدة التنظيم تتمتع بقدرات متقدمة وأقسام متخصصة للعمل، بقصد الوصول إلى بيانات أو إتلاف أو تعطيل أو سرقة أحد أصول تكنولوجيا المعلومات أو شبكة الكمبيوتر أو الملكية الفكرية أو أي شكل آخر من أشكال البيانات الحساسة . يمكن أن تأتي التهديدات السيبرانية من داخل المؤسسة بواسطة مستخدمين موثوق بهم أو من مواقع بعيدة من قِبل أطراف مجهولة. وتتراوح هذه التهديدات ما بين الدعاية والتشويش على صفحات الويب المزعجة منخفضة المستوى إلى التجسس والاضطراب الخطير وتعطيل البنية التحتية على نطاق واسع.

وليس من المبالغة القول إن إيران تعكف على تطوير قوتها الإلكترونية، التي أضحت تتطور وتنضج على نحو كبير ، الأمر الذي يتطلب جهوداً عربية نظيرة، لإيجاد استراتيجية إلكترونية، توازي في قدراتها ما توصلت له طهران من قدرات، وتطوير أجندة بحث مشتركة مع الحلفاء لمواجهة التهديدات الإيرانية وغيرها من الجهات الفاعلة في الفضاء السيبراني. وبالتالي فهناك حاجة إلى نهج استراتيجي للأمن السيبراني يتبع إطار عمل شامل، يعتمد على التركيز على بناء قدرات الأمن السيبراني الوقائية والتفاعلية، وعلى تطوير المواهب والقدرات الوطنية.

المصادر

[1] . هشام رشاد، "مراسلون بلا حدود: إيران ضمن الأسوأ عالمياً في حرية الصحافة"، العين الإخبارية، 22/4/2019. https://bit.ly/2W4uurF

.[2]Michael Holloway, "Stuxnet Worm Attack on Iranian Nuclear Facilities", July 16, 2015, https://stanford.io/3EMbjV0

.[3]Jim Finkle, "Powerful "Flame" cyber weapon found in Iran", Reuters, MAY 28, 2012, https://reut.rs/3hZaAGb

" .[4]Outgunned Iran takes on U.S. with 'asymmetric' strategy of missiles, drones and militia allies", The Japan Times, Jan 8, 2020, https://bit.ly/3CDnsdb

. [5]Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran, 2017, https://bit.ly/3zzPUdW

. [6]James Andrew Lewis, "Iran and Cyber Power", CSIS, June 25, 2019, https://bit.ly/2XGOZeu

[7] . مايكل آيزنشتات، "الوسائل السيبرانية: سلاح إيران المختار"، معهد واشنطن، 29 يناير 2017. https://bit.ly/3EMkxAH

. [8]Adam Hlavek, Strategic goals behind Iranian cyber-attacks, Security Boulevard, October 26, 2020, https://bit.ly/3orkYcw

.[9]James P. Farwell and Darby Arakelian, “What Does Iran’s Cyber Capability Mean for Future Conflict?”, https://ciaotest.cc.columbia.edu/journals/shjdir/v14i1/f_0028742_23336.pdf, p,50.

.[10]Adam Hlavek, op.cit.

. [11]Emerson T. Brooking, Suzanne Kianpour, “IRANIAN DIGITAL INFLUENCE EFFORTS: GUERRILLA BROADCASTING FOR THE TWENTY-FIRST CENTURY”, Atlantic Council, 2020, https://bit.ly/3kCVJmH, p. 15.

.[12]Ibid.

.[13]ANNIE FIXLER, “The Cyber Threat from Iran after the Death of Soleimani”, COMBATING TERRORISM CENTER, CTCSENTINEL, FEBRUARY 2020, VOLUME 13, ISSUE 2, https://bit.ly/3u48ppP

. [14]Tightening the Net Part 2: The Soft War and Cyber Tactics in Iran, op.cit.

“ .[15]Iran’s domestic espionage: Lessons from recent data leaks”, intel 471, https://bit.ly/3CBCn7B

.[16]Paul Bucala and Caitlin Shayda Pendleton, “Iranian Cyber Strategy: A View from the Iranian Military”, Critical Threats, November 24, 2015, https://bit.ly/3lRuC6L

.[17]John Hardie, Annie Fixler, “Russia-Iran cooperation poses challenges for US cyber strategy”, Global Norms, c4isrnet, https://bit.ly/39AJZea

.[18]Ibid.

.[19]Ibid.

.[20]Ahmed El-Masry, The Abraham Accords and their cyber implications: How Iran is unifying the region’s cyberspace, mei.edu, June 9, 2021, https://bit.ly/2ZNO5hL

.[21]Farhad Rezaei, “Iran’s Military Capability: The Structure and Strength of Forces”, Insight Turkey, Winter 2019 / Volume 21 Number 4, https://bit.ly/2Y0eCHN

.[22]Iranian MP: China will Help Us Conquer Cyber Space, Iran wire, 12 April 2021, https://bit.ly/39HoyYI

.[23]KIM ZETTER, “An Unprecedented Look at Stuxnet, the World’s First Digital Weapon”, 11.03.2014, https://bit.ly/3EMVU6Q

[24] . هجمات إلكترونية "متزايدة" تستهدف أرامكو، الحرة، 6 فبراير 2020، https://arbne.ws/3lVXrzb

.[25]Denial of service attacks against U.S. banks in 2012–2013, September 2012, cfr, https://on.cfr.org/3nfKBgU

[26] . ميكا لوديرميلك، "الأزمة الإيرانية تنتقل إلى الفضاء السيبراني"، معهد واشنطن، 9 يوليو 2019. https://bit.ly/3u4bK8l

.[27]Thomas Brewster, U.S. Accuses 7 Iranians of Cyberattacks on Banks and Dam, forbes, https://bit.ly/3qGtpmR

[28] . ياسمين أيمن، "هل تشتعل الحرب السيبرانية بين إيران وأمريكا بعد مقتل سليماني؟"، العين الإخبارية، 16/1/2020. https://bit.ly/3zAvFwW

[29] . إبعاد احتمالی جنگ سایبری میان ایران وآمریکا، دویجه وله فارسی، 09.01.2020. https://bit.ly/2XXYiHk

.[30]Kate O'Flaherty, "The Iran Cyber Warfare Threat: Everything You Need to Know", Forbes, Jan 6, 2020, https://bit.ly/3zyo3eb

.[31]Hacking group "Charming Kitten" targets nuclear experts and Treasury officials, cbs news, DECEMBER 13, 2018, https://cbsn.ws/3CKrocf

.[32]Jordan Brunner, "Iran Has Built an Army of Cyber-Proxies", The Tower, August 2015, https://bit.ly/3kAKQ4N

.[33]Ibid.

.[34]Ilan Berman, “Cyberwar and Iranian Strategy”, ilanberman, August 2012, https://bit.ly/3kEurw5

.[35]Kenneth Katzman, “Iran: Internal Politics and U.S. Policy and Options,” Congressional Research Service, October 17, 2018, page 4, https://bit.ly/3zFdC8H

.[36]Michael Connell, “Deterring Iran’s Use of Offensive Cyber: A Case Study,” CNA, October 2014, page 4, https://bit.ly/2WcRYLr

.[37]Gabi Siboni and Sami Kronenfeld, “Iran and Cyberspace Warfare”, https://bit.ly/3kDcePM, p.86.

.[38]Dorothy Denning, “Following the developing Iranian cyber threat,” The Conversation, December 11, 2017, https://bit.ly/3lRU38k

.[39]U.S. Department of the Treasury, Press Release, “Treasury Announces Sanctions Against Iran,” February 6, 2013, https://bit.ly/3i9Ufyy

.[40]Hossein Bastani, “Structure of Iran’s Cyber Warfare”, INSTITUT FRANCAIS D’ANALYSE STRATEGIQUE, https://bit.ly/3i7jC3Y

.[41]U.S. Department of Justice, Press Release, “Nine Iranians Charged with Conducting Massive Cyber Theft Campaign on Behalf of The Islamic Revolutionary Guard Corps,” March 23, 2018, https://bit.ly/3AHiR93

.[42]Ibid.