القدرات السيبرانية الإيرانية (الحرب الأخرى بين إيران وخصومها)

الكاتب: ضياء قدور

شارك في إعداد البحث ومراجعته: أحمد الرمح

التصنيف: دراسات استراتيجية

مدخل

في الوقت الذي تعتبر فيه تقارير غربية أن التهديد السيبراني الإيراني للمنشآت والبنى التحتية الوطنية الحيوية كبير للغاية، أصبحت إيران تمتلك نطاقاً واسعاً ومتطوراً للغاية من القدرات "السيبرانية" التي تمكّنها من شن هجمات إلكترونية تستهدف بها البنى التحتية الوطنية المهمة، والمؤسسات المالية، والخدمية، والتعليمية، والصناعية، لهذه البلدان، دون أن تفضي هذه الهجمات الإلكترونية إلى حدوث رد فعل مسلح أو اندلاع حرب شاملة لا ترغب فيها طهران.

في ظل التقدم العلمي والتكنولوجي (ثورة المعلومات)، الذي يشهده العالم، وفّر هذا النوع من الحروب غير التقليدية أرضية مناسبة لطهران لشن هجمات انتقامية فعالة وأقل تكلفة ضد خصومها، سواء في الداخل أم في الخارج، وساهم بتطوير القدرات السيبرانية الإيرانية في رفع مستوى الرقابة الصارمة التي تفرضها طهران على المستوى الداخلي في خضمّ ما تواجهه من انتفاضات شعبية عارمة تستخدم المجال السيبراني ساحة لنقل أخبارها وتطوراتها الميدانية.

يناقش هذا البحث، القدرات السيبرانية الإيرانية التي مكّنت طهران من تنفيذ هجمات سيبرانية ضارة ضد خصومها من حكومات ومنظمات وأفراد، بدءاً من إلقاء نظرة موجزة على تعريف الحرب السيبرانية وأساليبها، من ثم يسلط الضوء على الدوافع التي حفزت إيران لتطوير قدراتها السيبرانية، وأهم الأهداف الداخلية والخارجية التي استهدفتها الهجمات السيبرانية الإيرانية خلال العقود الماضية، واضعاً قراءة نقدية للقدرات السيبرانية الإيرانية في مرآة الواقع الدولي، ومنتهياً بمجموعة من الاستنتاجات والخلاصات.

محاور البحث:

- **تعريف موجز بالحرب السيبرانية:**
- **تطور القدرات السيبرانية الإيرانية، الدوافع والأهداف:**
- **القدرات السيبرانية الإيرانية في مرآة الواقع الدولي (قراءة نقدية)**
- **خلاصة واستنتاجات**

تعريف موجز بالحرب السيبرانية

وفقاً للتعريف الكلاسيكي، فإن أي محاولة للوصول إلى المعلومات الخاصة والسرية أو إيجاد خلل في شبكات الكمبيوتر تسمى هجوماً إلكترونياً. وببساطة أكثر، فإن أي نوع من الهجمات المنطلقة من جهاز كمبيوتر أو شبكة من أجهزة الكمبيوتر إلى جهاز أو شبكة من أجهزة الكمبيوتر الأخرى هو هجوم إلكتروني أو سيبراني.

هناك العديد من الطرق المختلفة لشن هجوم إلكتروني، لكن معظم الهجمات الإلكترونية قد تنقسم إلى سبع فئات([1]):

أولاً: البرامج الخبيثة أو الضارة Malware

البرامج الضارة هي جزء من التعليمات البرمجية، مثل أي برنامج آخر تمّ تطويره بواسطة مبرمِج واحد أو أكثر، والغرض من هذه الشيفرة الخبيثة التخريب، والتجسس على المعلومات، وسرقتها، والتحكم عن بعد بجهاز كمبيوتر الضحية.

باختصار تهدف البرامج الضارة إلى إتلاف جهاز كمبيوتر أو شبكة من أجهزة الكمبيوتر، ويعدّ هذه النوع

من أكثر أساليب الحروب السيبرانية خطورةً، وقد استخدمت إيران هذا النوع من الهجمات السيبرانية لمهاجمة الأقليات العرقية والدينية، وتشير تقارير إلى أن قراصنة الحكومة الإيرانية استخدموا برمجيات خبيثة لمهاجمة أكثر من مئة شخص، بمن فيهم نشطاء حقوقيون أتراك والدراويش الغنابادیین".

ثانياً: التصيد الاحتيالي Phishing

تعتمد هذه الطريقة على الحصول على كلمة مرور موقع ويب عن طريق إنشاء موقع ويب أو صفحة مزيفة، ولكنها تبدو تماماً مثل الموقع الأصلي.

في أسلوب التصيد الاحتيالي، تم استبدال الحرف ph بالحرف f للإشارة لمفهوم "الغش أو الاحتيال"، تماماً مثل الصياد الذي يخدع السمكة التي يصطادها بالطعم. وفي الحقيقة يعتمد قراصنة الحكومة الإيرانية منذ سنوات على أسلوب التصيد الاحتيالي، الذي يعدّ أحد أكثر أساليبهم استخداماً، في اصطياد ضحاياهم، وأصبح لديهم خبرة كبيرة في هذا المجال.

ثالثاً: برامج الفدية Ransomware

تشبه برامج الفدية البرامج الضارة من نواحٍ عديدة، باستثناء أنها أنشئت بغرض الابتزاز. في هذا النوع من الهجوم، عادةً ما يقوم المهاجم بتشفير معلومات كمبيوتر الضحية بطريقة غير قابلة للاستخدام ويطلب من الضحية المال لفك تشفيرها. ببساطة، يأخذون معلومات الكمبيوتر كرهينة للمطالبة بالإفراج عنها.

كان برنامج Wannacry من أشهر برامج الفدية وأكثرها تدميراً، ففي عام ٢٠١٧، أصابت البرامج الضارة حوالي ٢٠٠٠٠٠ جهاز كمبيوتر في جميع أنحاء العالم، بما في ذلك إيران، وطالب المهاجمون الضحايا بدفع ثلاثمئة دولار بعملة (البيتكوين) العملة الرقمية لفتح أجهزة الكمبيوتر.

رابعاً: الحرمان من الخدمة DDOS

يقول المثل العربي "إن يداً واحدة لا تصفق"، وهذا المثل ينطبق تماماً على أسلوب الحرمان من الخدمة.

يمكن لكل موقع ويب أو خدمة عبر الإنترنت الاستجابة لعدد محدود فقط من الطلبات. فعندما تدخل إلى موقع مركز أبحاث ودراسات مينا https://mena-studies.org/ar/، يستطيع هذا الموقع الاستجابة فقط لعدد معين من الطلبات لزيارته، وعندما يقع هذا الموقع أو الخدمة تحت ضغط كبير، سيفقد وعيه كأي

إنسان مُجهَد من العمل الشديد، ولن يكون قادرًا على الاستجابة للطلبات. الغرض من مثل هذا الهجوم هو جعل موقع ويب أو أي خدمة متصلة بشبكة كمبيوتر غير متاحة، أو لا يمكن الوصول إليها، وذلك بشكل أساسي لتعطيل الخدمة.

خامساً: الرجل في المنتصف Man in the middle

هجوم الرجل في المنتصف هو في الواقع وسيلة للتنصت. تخيّل أنك على اتصال بصديقك من خلال وسيط نجح في كسب ثقتك. يتمكن هذا الشخص الوسيط من إقناع كلاكما بأن لديكما علاقة خاصة، ومباشرة، لكنه يستمع عملياً إلى جميع محادثاتك، وقد يغيرها في بعض الحالات. مثل هذا الإجراء يسمى الرجل في المنتصف. في أغسطس ٢٠١١، أعلنت غوغل أنها نجحت في تحديد هجوم من قبل قراصنة الحكومة الإيرانية ومنعه استخدام هذه الطريقة لمهاجمة المعارضين السياسيين ونشطاء حقوق الإنسان.([٢])

سادساً: حقن SQL

يعدّ هذا الأسلوب هجوماً مباشراً على قواعد البيانات أو وهي لغة لاستخراج البيانات من قواعد البيانات. وباستخدام هذا الأسلوب، يحاول المهاجم التسلل إلى قاعدة البيانات من خلال العثور على ثغرات أمنية، والغرض من ذلك سرقة المعلومات بما في ذلك كلمة المرور، أو إتلاف المعلومات المخزنة في قواعد البيانات.

سابعاً: ثغرات يوم الصفر Zero-day exploits

هو استغلال الثغرات الأمنية في برامج الكمبيوتر التي لم تكتشفها الشركة المصنعة أو إذا اكتشفت ولم تصلّح بعد. كان فيروس ستوكسنت من أكثر هذه الهجمات شهرة، وهو الذي استهدف منشأة تخصيب اليورانيوم في إيران، إذ اكتشف صانعو ستوكسنت أربع ثغرات أمنية في نظام التشغيل Windows لم يعرفها أحد، لذلك وضعوا خططًا لاستخدام هذه الثغرات الأربع لتعطيل أو تدمير عملية تخصيب اليورانيوم في إيران.([٣])

تطور القدرات السيبرانية الإيرانية، الدوافع والأهداف:

كان هجوم فيروس ستوكسنت على المنشآت النووية الإيرانية عام ٢٠١٠، –الذي اتهمت الولايات المتحدة

وإسرائيل بالتخطيط له– واحداً من أكثر الهجمات السيبرنية تطوراً في التاريخ الحديث، إذ تسبب بأضرار مادية للمعدات التي تتحكم فيها أجهزة الكمبيوتر المستهدفة، وأعاد برنامج تخصيب اليورانيوم الإيراني عدة سنوات إلى الوراء، ما مثّل نمطاً جديداً من الهجمات السيبرانية.([٤])

وفي الحقيقة كان هجوم ستوكسنت بمثابة محفز قوي لتطوير القدرات السيبرانية الإيرانية، كما أنه أطلق يد إيران في عالم التأثيرات السيبرانية، لدرجة أن إيران استثمرته بكثافة في بناء دفاعات وقدرات هجوم سيبرانية في الوقت ذاته. منذ ذلك الحين، اتُهمت إيران بارتكاب عدد من الهجمات السيبرانية، باستخدام الطرق، والأساليب المتعددة المذكورة أعلاه، والتي توفرها طبيعة الحرب السيبرانية المفتوحة وظروفها، لكن هناك عدداً من الدوافع التي أجبرت النظام الإيراني على تطوير قدراته السيبرانية في ظل المتغيرات المحلية والإقليمية والدولية التي واجهها خلال العقود الماضية.

الدوافع:

أولاً: حماية النظام الحاكم من خلال القمع السيبراني للمعارضين والانتفاضات

لطالما اعتقد المرشد الأعلى الإيراني علي خامنئي أن واشنطن تسعى للإطاحة بالنظام الحاكم من خلال تحريض الجماهير على غرار الثورة المخملية، التي أطاحت بالنظام الشيوعي التشيكوسلوفاكي عام ١٩٨٩، وقد خلق معارضو النظام ومنتقدوه باستخدامهم المبكر والفعال للإنترنت وشبكات التواصل الاجتماعي انطباعاً لدى المتطرفين والمتشددين في طهران بأن القوات الأجنبية تخطط للإطاحة بالنظام الحاكم باستخدام تقنيات الإنترنت الجديدة.

بناءً على هذه الحجة، انطلقت أول عملية سيبرانية لإيران (خلال عام ٢٠٠٩ الثورة الخضراء) بسبب المخاوف التي كانت تدور حول تعرض استقرار النظام لتهديدات خارجية، وأن فضاء الإنترنت، الذي دعمت الحكومات الغربية الوصول غير المقيد إليه([٥])، سيسهل ذلك.

وفي ظل طرد السلطات لوسائل الإعلام الأجنبية من إيران، وتجسسها على شبكات المحمول، واعتقالها لأبرز المعارضين البارزين، أصبح الإنترنت القناة الرئيسة للتواصل والتنسيق خلال الثورة الخضراء التي اندلعت عام ٢٠٠٩ وقد شكل ظهور مواقع التواصل الاجتماعي، مثل فيس بوك وتويتر، وتطبيقات المراسلة، مثل تلغرام، تهديداً كبيراً لأنها تحدت احتكار الحكومة الإيرانية طويل الأمد لوسائل الإعلام

ومعدات الاتصال. خلال الحركة الخضراء، استخدمت مجموعات الهكر الموالية للنظام الإيراني استراتيجية متعددة الجوانب شملت اختراق المواقع ومراقبة الشبكات، ومن ديسمبر ٢٠٠٩ حتى يونيو ٢٠١٣، أقدم ما يسمى بالجيش السيبراني الإيراني على إرسال رسائل داعمة للحكومة على مواقع المعارضة، والشركات التجارية الإسرائيلية، ووسائل الإعلام الفارسية المستقلة، وشبكات التواصل الاجتماعي.([٦])

وفي الوقت الذي كان يدعو فيه المدافعون عن حقوق الإنسان، وقادة المعارضة لتنظيم احتجاجات شعبية عارمة، تعرضت المواقع المهمة، كتويتر([٧])، لأسلوب الحرب السيبرانية (الحرمان من الخدمة)، ما حرم المستخدمين من الوصول لهذه المواقع بشكل مؤقت. بالإضافة لذلك، سعت الحكومة الإيرانية للتجسس على معارضيها، من خلال إرسالها برامج ضارة ادّعت أنها تحتوي على معلومات تتعلق ببرامج المظاهرات القادمة. وفي ذلك الوقت قام أحد خبراء الهكر الإيرانيين باختراق الشركة الأمنية الهولندية DigiNotar، ما سهل إصدار شهادات تشفير مزيفة (التصيد الاحتيالي) سمحت لطهران بالتجسس على جميع مستخدمي Gmail داخل البلاد، في اختراق يعد أحد أكبر الخروقات الأمنية في تاريخ الإنترنت.([٨])

إن معظم ضحايا العمليات السيبرانية الإيرانية هم إما إيرانيون أو أعداد كبيرة من المهاجرين الإيرانيين، الذين يصنفهم قادة البلاد كأعداء ويخشونهم، لكن أهداف المراقبة السيبرانية في طهران لم تقتصر على أولئك الذين يعتبرهم النظام معارضين ساعين للإطاحة بالنظام فحسب، بل شملت أيضاً المؤسسات الثقافية غير السياسية وحتى المنظمات الحكومية الإيرانية وشخصيات سياسة إصلاحية([٩])، وبالتالي أظهر التجسس السيبراني والهجمات التخريبية على منتقدي الحكومة للإيرانيين أن أنشطتهم على الإنترنت ليست بعيدة عن متناول الحكومة.

ثانياً: استعراض القوة:

خلال العقود الماضية، تحوّل الفضاء الافتراضي إلى ساحة صراع جديدة فيما يمكن تسميته بالحرب الباردة بين الولايات المتحدة وحلفائها من جانب وإيران من جانب آخر.

قد تكون إيران أكثر الحكومات التي غدت هدفاً للهجمات السيبرانية المخربة للولايات المتحدة وحلفائها، لكن المجموعات الأمنية التابعة للحرس الثوري ووزارة المخابرات الإيرانية تمكنت من تطوير مهاراتها في تنفيذ الهجمات السيبرانية التي استهدفت المعارضين الإيرانيين في الداخل والخارج، والشركات والمنظمات غير الحكومية، وكذلك المؤسسات الاقتصادية والدفاعية والمالية للدول المختلفة، بما في

ذلك ألمانيا، وإسرائيل، والمملكة العربية السعودية، والولايات المتحدة.([١٠])

غالباً ما تنكر طهران، التي استخدمت ميليشياتها باستمرار لإثبات قوتها في المنطقة، مشاركتها في مثل هذه الهجمات، متخفية وراء وكلاء أو وسطاء سيبرانيين أيضاً لمنع انتساب هذه الهجمات لها، لكن رغم هذا الإنكار، استثمرت إيران بشكل علني في القدرات السيبرانية المحلية للأغراض الهجومية والدفاعية على حد سواء، وهي على استعداد لاستخدامها للانتقام من أعدائها، أو في حالة نشوب حرب مسلحة.

ثالثاً: التكلفة المنخفضة (الهجوم السيبراني فعّال وأقلّ تكلفة من الحرب الحقيقة)

صحيح أن منحى الهجمات السيبرانية الإيرانية أخذ بداية متأخرة نسبياً (بعد عام ٢٠١٠ تقريباً)، حيث بدأت إيران باختراق بعض المواقع الإلكترونية، وكان هذا المنحى منخفض رأس المال، الأمر الذي يرجع جزئياً إلى قدرات الدولة المحدودة في هذا الصدد، لكن تأثير موسكو على المؤسسات الديمقراطية والقادة السياسيين خلال الانتخابات الأمريكية لعام ٢٠١٦([١١]) أظهر أن حرب المعلومات يمكن شنها باستخدام حلول بدائية ذات تكاليف منخفضة وتأثير وفعالية كبيرين في ذات الوقت. ومن هذا المنطلق، استغلت إيران أوجه القصور أو عدم الاستعداد للأهداف المعرضة للخطر داخل البلاد وخارجها، بما في ذلك شركات النفط السعودية، ودول الشرق الأوسط، والبنوك الأمريكية.

النقطة المهمة هي أن هذه العمليات غالباً ما كانت تؤدي إلى خسائر مالية كبيرة، إلا أن الأساليب المستخدمة لتدمير البيانات أو تعطيل الوصول إلى المواقع كانت بسيطة نسبياً، وذات تكلفة منخفضة، ناهيك بأن هجمات طهران ضد المصالح الخارجية كانت هجمات تجسسية وتخريبية ضد الأهداف غير المحصنة في الدول المنافسة.

وفي الحقيقة، أظهرت إيران أن الدول الأضعف عسكرياً يمكنها استخدام العمليات العدوانية السيبرانية لمحاربة أعدائها المتقدمين، الذين فرضت عليهم طهران تكاليف انتقامية لإثبات قدرتها.

الأهداف:

أولاً: الأهداف الخارجية

بما أن إيران غير قادرة على خوض صراع مثمر أو رادع ضد خصوم أكثر استعداداً منها، فإنها تشن هجمات

سيبرانية مدمرة وانتهازية لإثبات قدرتها على الانتقام، وضمنياً يمكن أن تهدد العمليات السيبرانية الإيرانية البنية التحتية والموارد الاقتصادية لخصومها الذين ليس لديهم الدعم والاستعداد الكافي في هذا المجال. بالإضافة إلى المملكة العربية السعودية، تُعدّ الدنمارك وألمانيا وإسرائيل والولايات المتحدة من بين الدول التي كشفت علانية عن جهود التجسس للجماعات الإيرانية ضد مؤسساتها الحكومية أو العسكرية أو العلمية.

وتستهدف طهران أيضاً الدول المجاورة في جميع أنحاء الشرق الأوسط، لكن على الرغم من تنوع التهديدات السيبرانية التي تشكلها الحكومة الإيرانية إلا أن أنماط سلوكها بما في ذلك أهدافها، ظلت ثابتة عموماً بمرور الوقت.

الولايات المتحدة وأوروبا

في سبتمبر/أيلول ٢٠١٢، أطلقت مجموعة تطلق على نفسها اسم "مقاتلو عز الدين القسام السيبرانيين" حملة سيبرانية (الحرمان من الخدمة) ضد القطاع المالي الأمريكي. قبل الحملة، كان المهاجمون يستغلون نقاط الضعف في برمجيات آلاف المواقع لإنشاء منصة هجوم تحت سيطرتهم. مع هذا الجيش من الخوادم في الشركات المضيفة، تمكّن المهاجمون من تعريض أهدافهم لعاصفة من حركة المرور الكثيفة والمدمرة على الإنترنت. وفي المرحلة الأولى من عملية أبابيل، استهدفت هذه المجموعة البنية التحتية المصرفية الأمريكية، حيث تعرضت البنوك الأمريكية لحركة مرور تعادل ثلاثة أضعاف سعتها الأساسية ما تسبب بتوقف أنظمتها وقواعد بياناتها عن العمل.([١٢])

على الرغم من أن المراحل التالية من عملية أبابيل (حتى المرحلة الرابعة في يوليو٢٠١٣) لم تكن مثمرة للغاية، حيث كان القطاع المالي يعمل باستمرار على تحسين نظامه الدفاعي، لكن وفقاً لمكتب التحقيقات الفيدرالي، منعت عملية أبابيل مئات الآلاف من عملاء البنوك من الوصول إلى حساباتهم لفترات طويلة من الزمن، ما أدى إلى خسائر تقدر بعشرات الملايين من الدولارات.([١٣])

بالإضافة إلى ذلك، يشرح تقرير صادر عن وكالة الأمن القومي الأمريكية الدافع وراء عملية أبابيل، قائلاً: "تظهر إشارات استخباراتية أن هذه الهجمات كانت انتقاماً للأنشطة الغربية ضد القطاع النووي الإيراني، وكان مسؤولون حكوميون إيرانيون رفيعو المستوى على علم بالهجمات".([١٤])

لم تتوقف الهجمات السيبرانية بعد عملية أبابيل التي تعدّ أكثر الهجمات السيبرانية تدميراً على الولايات

المتحدة، ولاحقاً زُعم أن إيران تمكنت من الوصول إلى شبكة الإنترنت غير السرية لقوات مشاة البحرية الأمريكية لعدة أشهر منذ أغسطس ٢٠١٣ .([١٥])

وفي إصدار عام ٢٠١٦ من التقييم الأمني السنوي لوزارة الداخلية الألمانية، صنفت الحكومة الألمانية إيران كمصدر جديد للتجسس السيبراني ضد هذا البلد. ويتماشى هذا التقييم مع التقارير التي تفيد بأن البرلمان الألماني تأثر بعملية برمجيات خبيثة استهدفت قراء صحيفة جيروزاليم بوست الإسرائيلية.([١٦])

وفي ١٤ فبراير/شباط ٢٠٢٠، خلصت شركة الأمن السيبراني فاير اي في بحثها إلى أن ألمانيا تعد هدفاً جذاباً للهجمات السيبرانية التي تدعمها حكومات مثل روسيا والصين وإيران، نظراً لأهميتها السياسية والاقتصادية في أوروبا والعالم.([١٧])

على نحو عام نادراً ما نجحت إيران بالتسلل إلى البنية التحتية للحكومات الأمريكية والأوروبية، خاصة الشبكات السرية شديدة الأمان، لأن الوكالات الحكومية في هذه الدول عادة ما تخضع لحراسة مشددة، بحيث لا يتمكن عملاء التهديد الإيراني([١٨]) من التسلل إليها. نتيجة لذلك، اتبعت إيران أهدافًا أبسط، في محاولة لاستهداف رسائل البريد الإلكتروني الشخصية وحسابات وسائل التواصل الاجتماعي لموظفي الحكومة الأمريكية باستخدام أسلوب (التصيد الاحتيالي الهادف). على سبيل المثال، حاول الإيرانيون اختراق حسابات البريد الإلكتروني الشخصية لأعضاء الفريق الأمريكي أثناء المفاوضات النووية.([١٩])

وبعد الانتخابات الرئاسية الأمريكية لعام ٢٠١٦، ركز عملاء التهديد الإيراني على موظفي أوباما السابقين، وأنصار حملة دونالد ترامب، والمؤسسات الإعلامية المحافظة، والمرشحين السياسيين للتعرف على الإدارة الأمريكية الجديدة.([٢٠])

وفيما بعد، استهدفت هجمات (التصيد الاحتيالي) الإيرانية النُّقاد الإيرانيين في الكونجرس الأمريكي حين كان ينظر في فرض عقوبات جديدة ضد إيران.([٢١])

على نحو عام، تسعى طهران إلى استهداف موظفي ومنظمات الحكومات الأجنبية الذين يركزون على إيران في الولايات المتحدة أو أوروبا، أي في مجال السياسة الإيرانية أو في وسائل الإعلام الناطقة باللغة الفارسية، مثل إذاعة صوت أمريكا أو راديو فردا.([٢٢])

وفي الحقيقة، إن المراقب للرسم البياني للهجمات السيبرانية الإيرانية يجد أن الأنشطة السرية والهجمات

الانتقامية قد تراجعت بين واشنطن وطهران منذ توقيع الاتفاق النووي عام ٢٠١٥، لتركز طهران بشكل أكبر على المعارضين السياسيين والأعداء الإقليميين، مثل إسرائيل والمملكة العربية السعودية، لكن هذه الأنشطة عادت مرة أخرى للواجهة خلال فترة حكم دونالد ترامب، خاصة بعد إسقاط إيران للطائرة الأمريكية المسيرة في ٢٠ يونيو ٢٠١٩، ومقتل قاسم سليماني بغارة أمريكية بالقرب من مطار بغداد في بدايات عام ٢٠٢٠ .

بعد يوم واحد فقط من مقتل قاسم سليماني، أصدرت وزارة الأمن الداخلي الأمريكية بيانًا تحذر فيه من هجوم إلكتروني من قبل إيران، قائلة: "لدى إيران برنامج إلكتروني قوي يمكن أن يشكل تهديداً للولايات المتحدة". وقال البيان "يمكن لإيران على الأقل تعطيل بعض من البنية التحتية الحيوية للولايات المتحدة لفترة محدودة".([٢٣])

المملكة العربية السعودية

بسبب توتّر العلاقات بين طهران والرياض منذ انتصار الثورة في إيران، احتلت المملكة العربية السعودية المرتبة الأولى بين الدول التي تعرضت لهجمات سيبرانية من قبل عملاء إيرانيين مدعومين من الحكومة. ومنذ بداية نشاط العمليات السيبرانية لإيران، تم اختراق المؤسسات السياسية والاقتصادية السعودية من قبل طهران بهدف التجسس والتخريب، إذ كانت المملكة العربية السعودية واحدة من أكثر مصادر الضحايا والأهداف شيوعاً في التقارير المختلفة التي تحدثت عن البرامج الضارة وحملات سرقة الحسابات وكلمات المرور من قبل عملاء التهديد الإيراني، ما يعكس الاختلافات الإيديولوجية والجيوسياسية العميقة بين البلدين، فضلاً عن ضعف المملكة العربية السعودية المستمر في الفضاء السيبراني.

كان الهجوم السيبراني الإيراني على منشآت أرامكو السعودية في ١٥ أغسطس ٢٠١٢ (والهجوم المماثل على شركة RasGasالقطرية بعد أسبوعين) مثالاً واضحاً على كيفية استخدام إيران للهجمات السيبرانية للانتقام من أعدائها الذين تعرضوا لخسائر مالية كبيرة في ظل استخدامها لوسطاء سيبرانيين مجهولين أبعدوا تهمة هذه الهجمات عن طهران.([٢٤])

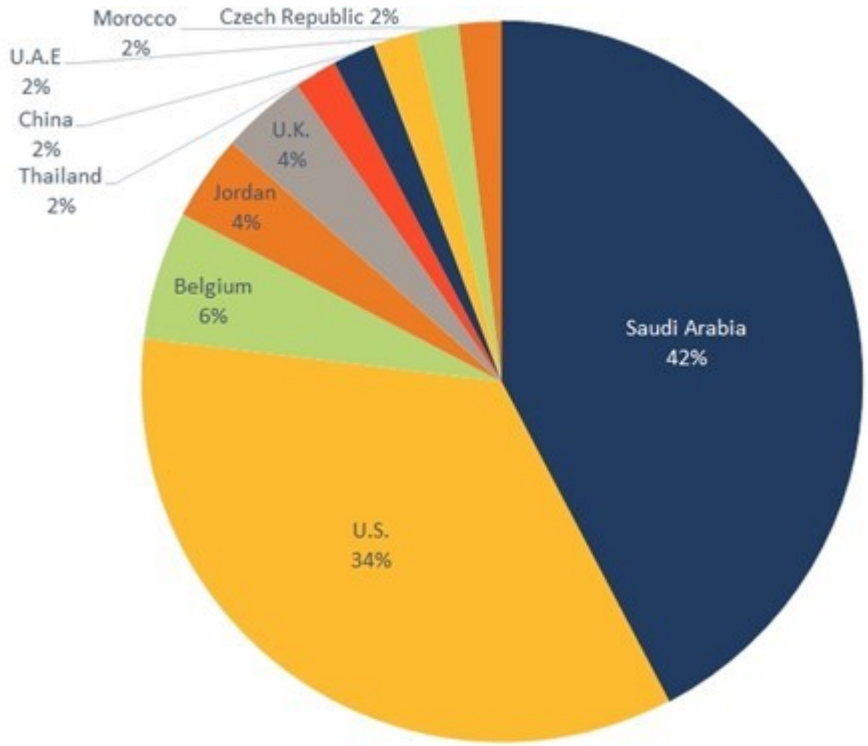
قد لا تكون إيران دائماً قادرة على الدفاع عن نفسها مقابل القدرات السيبرانية المتقدمة للولايات المتحدة، لكنها قد تفرض تكاليف باهظة على حلفائها، وهذه هي الرسالة التي أرادت إيران إيصالها من خلال هجوم "شامون" الذي تسبب بخسائر تقدر بمئات الملايين من الدولارات، إذ اخترق عشرات الآلاف من أجهزة

الكمبيوتر في شركة أرامكو السعودية. وفي ذات الوقت، عكست دورة الهجمات السرية الانتقامية المدمرة التي شوهدت في "شامون" و"أبابيل" التكتيكات الأمنية الإيرانية المتبعة داخل الفضاء الافتراضي.

وعلى سبيل المثال، بين عامي ٢٠١٠ و٢٠١٢، اغتيل العديد من العلماء النوويين الإيرانيين في ظروف غامضة، حيث نُسبت هذه الأعمال إلى الولايات المتحدة أو إسرائيل.([٢٥]) رداً على ذلك، حاولت طهران اغتيال مسؤولين إسرائيليين في أماكن غير متوقعة، مثل جورجيا والهند وتايلاند، لكنها فشلت في ذلك.

تُظهر هذه الدورة، أن إيران تتعلم من الهجمات وتسعى للانتقام بالطريقة نفسها، ويوفر هذا معايير محتملة لفهم إشارات إيران ودوافعها لتنفيذ عمليات سيبرانية خبيثة. من ناحية أخرى، بالمقارنة مع أعداء إيران الآخرين (وبالتحديد الولايات المتحدة وإسرائيل) لا يزال يتعين على الحكومة والمؤسسات الاقتصادية السعودية وضع أنظمة وبروتوكولات مناسبة لزيادة الأمن السيبراني الوطني، وذلك لوضع حد للهجمات السيبرانية الإيرانية التي اكتفت بإلحاق الضرر بالمؤسسات الاقتصادية السعودية، في الوقت الذي كانت تفشل فيه بإلحاق خسائر كبيرة بالولايات المتحدة.

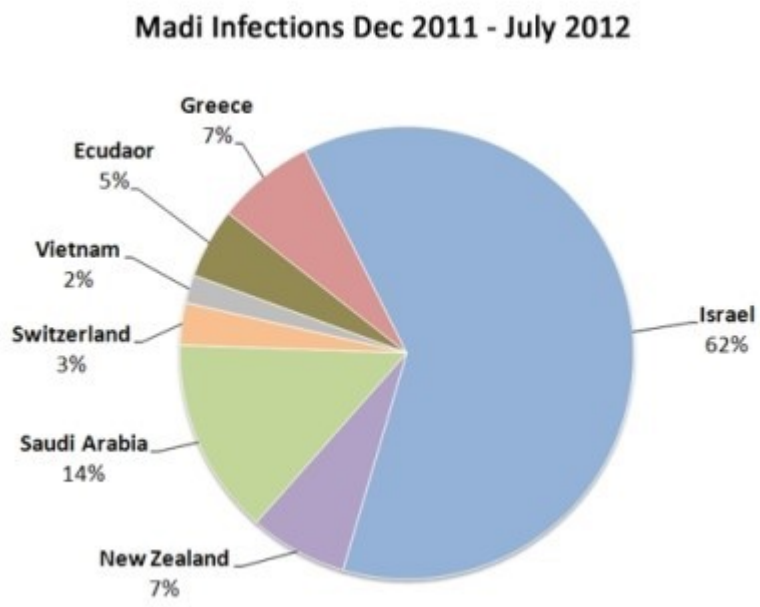
ما يؤكد ذلك، هجمات شامون ٢ التي أتلفت من نوفمبر ٢٠١٦ إلى يناير ٢٠١٧، قواعد البيانات والملفات المملوكة لكل من الحكومة السعودية والقطاع الخاص، بما في ذلك هيئة الطيران المدني، ووزارة العمل، والبنك المركزي السعودي، وشركات الموارد الطبيعية([٢٦])، وكذلك هجمات APT ٣٣ التي قامت بها مجموعة تعرف باسم (Elfin Group)، واستمرت من عام ٢٠١٦ حتى عام ٢٠١٩، لتضرب أكثر من خمسين منظمة (أغلبها يعمل في المجالات الحيوية والطاقة) تتوزع أغلبها في السعودية والولايات المتحدة وعدة دول أخرى، كما يُظهر المخطط البياني التالي([٢٧]):



إسرائيل:

على الرغم من كل شعارات العداء لإسرائيل التي تنتهجها السياسة الخارجية الإيرانية، لم تكن الكثير من الهجمات السيبرانية الإيرانية ضد المؤسسات الإسرائيلية بهدف التدمير والتجسس ناجحة، ويعود هذا بطبيعة الحال إلى مستوى مهارات الدفاع الإسرائيلية السيبرانية، الذي دفع طهران للاكتفاء بالهجوم على أهداف بسيطة (غير عسكرية على الأغلب) باستخدام أسلوب الحرمان من الخدمة أو التصيد الاحتيالي.

إحدى العمليات السيبرانية الإيرانية الناجحة ضد إسرائيل التي يمكن الإشارة لها هي عمليات مهدي (MalwareMadi)عام ٢٠١٢، التي تشير التحقيقات إلى أن خوادم قيادتها والتحكم بها كانت تدار من إيران، وأضرت بالمؤسسات الإسرائيلية بالدرجة الأولى، والسعودية بالدرجة الثانية، كما يشير المخطط البياني التالي([٢٨]):



بالإضافة لذلك، شنت إيران هجمات سيبرانية (الحرمان من الخدمة) ضد إسرائيل، وهي هجمات تشبه بتكتيكاتها الهجمات التي شنتها ضد الولايات المتحدة ومعارضي طهران، كما استهدفت إيران بأسلوب التصيد الاحتيالي المؤسسات الأكاديمية ومسؤولي الأمن القومي، والدبلوماسيين وأعضاء البرلمان الإسرائيلي (الكنيست)، وشركات الطيران الإسرائيلية، واللجنة العامة للعلاقات الأمريكية الإسرائيلية.([٢٩])

جدول بأهم الهجمات السيبرانية الإيرانية خلال العقدين الماضيين([٣٠]):

اسم العملية	الفترة التي امتدت خلالها	الضحايا
التأثير على وسائل التواصل الاجتماعي	2011- 2017	عملية سيبرانية تم تنفيذها من خلال حسابات وهمية و "روبوتات" في شبكات التواصل الاجتماعي لتوليد معلومات مضللة في المجتمع الأمريكي
أبابيل	ديسمبر 2011 - مايو 2013	هجمات سيبرانية على شركات في القطاع المالي تابعة للولايات المتحدة
Cleaver	2012 – 2014	التشغيل لأغراض التجسس الصناعي والحكومي
شامون	أغسطس 2012	تعرضت شركة الطاقة السعودية أرامكو لهجوم مدمر بواسطة البرمجيات الخبيثة
Bowman	أغسطس - سبتمبر 2013	تم اختراق شركة بومان النشطة في نيويورك
زهرة الزعفران	2013- 2014	استهدفت هذه الحملة أنظمة تكنولوجيا المعلومات في صناعة الدفاع الأمريكية والمنشقين عن النظام الإيراني الموجودين في الخارج
Sands Coorp	2014	هجوم إلكتروني ضد شركة لاس فيجاس ساندز
Thamar Reservoir	شباط 2014	استهدفت عملية التجسس السيبراني مراكز الأبحاث والصحفيين ونشطاء الشرق الأوسط
APT OilRig	2017 – 2018	سرقة المعلومات السرية من الشركات ذات المجالات النشطة والحكومية
شامون ٢	نوفمبر 2016 يناير 2017	عملية تجسس إلكتروني استهدفت عدة وزارات سعودية
Leafminer	2017- 2018	مجموعة التهديد التي استهدفت الحكومات والمنظمات المهمة الموجودة في الشرق الأوسط
APT 33	2016 - 2019	ركزت حملة التجسس السيبراني على المنظمات في مجالات الفضاء والطاقة والكيمياء

الأهداف الداخلية:

كانت إيران من أوائل الدول في الشرق الأوسط التي اتصلت بالإنترنت، ونتيجة لذلك، استخدم أكثر من نصف سكانها الإنترنت منذ ٧ مارس ٢٠١٧، ([٣١]) وهذا الأمر شكل تحدياً كبيراً للنظام الأمني في طهران في ظل ابتعاد أغلب الإيرانيين عن استخدام وسائل التواصل التقليدية التي كانت الأجهزة الأمنية الحكومية تخضعها لرقابة كاملة.

في الوقت ذاته، سمحت تكنولوجيا المعلومات لمستخدمي الإنترنت الإيرانيين استخدام الشبكات الاجتماعية وتطبيقات الدردشة الخاصة بسهولة، مستفيدين من منصات الإنترنت الموجودة خارج إيران،

وتقنيات التشفير لحماية اتصالاتهم من التنصت، ما وفر لهم مساحة أكبر من الحرية الاجتماعية.

لطالما حاولت الحكومة الإيرانية إجبار الشركات الأجنبية على قبول طلبات الحصول على معلومات المستخدمين، إلا أنها لم تنجح في هذا المسعى، في حين فشلت البدائل المحلية للخدمات الأجنبية كتلغرام وواتس آب([٣٢])، في جذب المستخدمين المهمين، بمن فيهم المسؤولون الإيرانيون، وملايين الإيرانيين الذين يعيشون داخل البلاد وخارجها، ما جعل أغلب اتصالات الإيرانيين وأنشطتهم الشخصية بعيدة على نحو متزايد عن متناول الحكومة خلال العقدين الأولين بعد انتصار الثورة في إيران.

شكلت حالة العمى شبه الكامل هذه هاجساً كبيراً لدى النظام الأمني البوليسي في طهران ما دفع عملياته السيبرانية لتكون أكثر مرونة بسبب تغير مجموعة الأدوات والبرامج الحديثة التي وضعها العالم الافتراضي في متناول جماهير الشعب الإيراني.

على سبيل المثال، بعد أن لجأ أغلب الإيرانيين إلى استخدام برنامج تلغرام، على اعتبار أنه برنامج آمن نسبياً مقارنة بغيره من برامج الدردشة، وجه عملاء التهديد الإيراني انتباههم إليه، ساعين إلى تنفيذ عمليات التصيد الاحتيالي لسرقة كلمات مرور وأسماء حسابات المستخدمين الإيرانيين لبرنامج التلغرام.

يعدّ برنامج تلغرام، أحد أكثر برامج المحادثة شعبية داخل إيران، ويستخدمه أكثر من عشرين مليون مستخدم داخل إيران، وعلى الرغم من كل الصراعات التي خاضتها الحكومة الإيرانية مع إدارة تلغرام، لا يزال هذا التطبيق متاحاً بسهولة داخل إيران خلافاً للعديد من تطبيقات المراسلة الأخرى، التي حُظرت. كان تساهل تعامل الحكومة الإيرانية مع تطبيق تلغرام ومستخدميه، والسماح لهم باستخدامه داخل إيران دليلاً على مدى حجم الاختراق الأمني الكبير الذي كانت تمارسه الحكومة الأمنية على مواطنيها.

ما يؤكد ذلك التقارير التي تتحدث عن أن عوامل التهديد المرتبطة بالحكومة الإيرانية تمكنت في عام ٢٠١٦ من الوصول إلى أكثر من ١٥ مليون رقم هاتف خاص بمستخدمي تلغرام داخل إيران([٣٣]). أي إن مستخدمي هذا التطبيق كانوا يخضعون بالكامل لرقابة حكومية صارمة، بما في ذلك التنصت ومراقبة تواصلهم كله، وهذا ما يفسر تساهل الحكومة الأمنية في طهران بالسماح للمستخدمين بالتواصل عبر هذا التطبيق دون أي عوائق.

على نحو عام، ركزت الهجمات السيبرانية المنسقة التي نفذتها مجموعات مختلفة من عملاء التهديد التابعين للحكومة الإيرانية على مدى فترات زمنية مختلفة، على مجموعة من الأهداف:

- المسؤولون الحكوميون والشخصيات الإصلاحية.
- الشخصيات الإعلامية.
- مجموعات المعارضة الإيرانية الكبرى (منظمة مجاهدي خلق الإيرانية نموذجاً).

ا- المسؤولون الحكوميون والشخصيات الإصلاحية

قد يقول قائل إن المسؤولين الإيرانيين قد يُعدّون خطأً أحمر بالنسبة لمجموعات الهكر المحسوبة على الحرس الثوري، ووزارة المخابرات الإيرانية، لكن الوثائق التي نشرها موقع بي بي سي فارسي عام ٢٠١٨([٣٤]) ، تظهر أن هذه المجموعات الأمنية لا ترى أي فرق بين وزير الخارجية الإيراني جواد ظريف وأي ناشط حقوقي يعمل خارج إيران، أو بين معارض إيراني منفي ومؤسسة عسكرية واقتصادية أمريكية أو سعودية أو إسرائيلية.

هذا الأمر يظهر حجم صلاحيات الدولة الأمنية العميقة التي تحكم إيران، إذ تُمكّن أيّ ضابط في الحرس الثوري، أو ربما عنصر مخابرات في وزارة المخابرات الإيرانية، أن يأمر بتوجيه هجمة سيبرانية (تجسسية) ضد المقربين من رئيس الجمهورية الإيراني حسن روحاني، بمن فيهم وزير خارجيته جواد ظريف، وشقيقه ومستشاره حسين فريدون، وماجد تخت روانجي، وعباس عراقجي، وحسام الدين آشنا، وعدة مسؤولين آخرين مقربين من حكومة روحاني ممن تعرضوا لهجمات سيبرانية يقودها عملاء التهديد الإيراني.

إن الحملات السيبرانية التي استهدفت أعضاء في حكومة روحاني، وشخصيات إصلاحية بارزة داخلها يظهر أهمية المراقبة الإلكترونية كأداة في أيدي الحكومة الأمنية المتطرفة تُمكّنها من السيطرة على المنافسين المحتملين للسلطة من خلال جمع معلومات حساسة عن حياتهم لابتزازهم أو إذلالهم، أو استخدام حساباتهم الإلكترونية كمنصة لمهاجمة شخصيات أخرى.

في الحقيقة، تقدم وزارة الخارجية الإيرانية المثال الأبرز والأكثر وضوحاً على التجسس داخل الحكومة، فمنذ بداية إدارة روحاني، غالباً ما كان الدبلوماسيون الإيرانيون هدفاً لحملات أسلوب (التصيد الاحتيالي)، خاصة أن هذه الأنشطة تماشت مع الاتهامات التي كانت تطلقها وسائل إعلام الحرس الثوري بخيانة مصالح إيران بعد توقيع الاتفاق النووي، وأحد الأمثلة على ذلك هو اعتقال عبد الرسول دوري أصفهاني، عضو فريق التفاوض النووي، بتهمة التجسس([٣٥]).

٢- الشخصيات الإعلامية

ينصبّ تركيز العمليات السيبرانية الإيرانية بانتظام على الصحفيين الذين يعملون مع وسائل الإعلام الإصلاحية والشبكات الفضائية الدولية الخارجة عن سيطرة الحكومة ومراقبتها الصارمة، وقد نفذ كثيرون من عملاء التهديد الإيراني عديد العمليات ضد الصحفيين الأجانب المقيمين في إيران، وكذلك الصحفيون الإيرانيون العاملون في منشورات بارزة مثل صحيفة شرق، باستخدام عمليات عديدة تهدف لسرقة الحسابات وكلمات المرور.

وبالمثل، يتعرض الصحفيون المستقلون داخل إيران للمضايقات على نحو منتظم تقوم بها شخصيات مزيفة ترسل لهم برامج ضارة لاختراق حساباتهم والتجسس عليهم. غالباً ما تستهدف هذه الحملات السيبرانية المطبوعات التي تغلق لاحقاً، أو الصحفيين الذين تحتجزهم قوات الأمن الإيرانية. فما حدث لجيسون رضائيان، مراسل صحيفة واشنطن بوست السابق في إيران، يظهر تركيز عملاء التهديد الموالين للحكومة على الصحافة الأجنبية العاملة في إيران. كان رضائيان هدفاً للحملات السيبرانية الإيرانية ([٣٦]) "flying kitten hackers"، فحاولت التسلل إلى حسابات Hotmailو Gmailالخاصة برضائيان عدة مرات بحسابات أمان مزيفة عن طريق سرقة أسماء المستخدمين وكلمات المرور، وذلك قبل اعتقاله في ٢٢ يوليو ٢٠١٤، وقد حكم عليه الحرس الثوري بالسجن مدة ثمانية عشر شهراً.

٣- مجموعات المعارضة الإيرانية الكبرى (منظمة مجاهدي خلق الإيرانية نموذجاً)

تعرضت مجموعات المعارضة الإيرانية، خاصة منظمة مجاهدي خلق، والمجلس الوطني للمقاومة الإيرانية لهجمات انتقامية تنوعت بين التصفية الجسدية لكوادرها في الخارج وحملات الاعتقال والإعدام الوحشية لأنصارها في الداخل الإيراني. وبصفتها أكبر مجموعة إيرانية معارضة، وتتمتع بشعبية واسعة قادرة على حشد وتنظيم مظاهرات واسعة في الداخل الإيراني، يعتبر النظام الإيراني منظمة مجاهدي خلق الإيرانية عدوه اللدود، ويسعى للتخلص من قياداتها بشتى السبل، وأحد أبرز الأمثلة على ذلك هي محاولة الاغتيال الأخيرة الفاشلة لرئيسة الجمهورية التي انتخبها المجلس الوطني للمقاومة الإيرانية، مريم رجوي، في مؤامرة فيلبنت الإرهابية عام ٢٠١٨ ([٣٧]).

ولهذا السبب، كانت منظمة مجاهدي خلق وكوادرها أبرز ضحايا الحملات السيبرانية التي ينظمها عملاء التهديد الإيراني الذين كان لهم هدف واحد: هو سرقة معلومات من جماعات المعارضة الإيرانية في أوروبا

والولايات المتحدة والتجسس على المعارضين الإيرانيين الذين غالباً ما يستخدمون تطبيقات الهاتف المحمول للتخطيط للاحتجاجات وتنظيمها.

في ١٨ ديسمبر ٢٠٢٠، ذكر تقرير نشرته صحيفة نيويورك تايمز الأمريكية أن عملاء التهديد الإيراني يستخدمون مجموعة متنوعة من تقنيات التسلل، بما في ذلك أسلوب التصيد الاحتيالي، ولكن الطريقة الأكثر انتشاراً هي إرسال ما يبدو أنه مستندات وتطبيقات مغرية إلى أهداف معارضة محددة بعناية([٣٨]).

على سبيل المثال، أرسل عملاء التهديد الإيراني وثيقة باللغة الفارسية بعنوان "النظام يخشى انتشار المدافع الثورية. "docx، في إشارة إلى الصراع بين النظام والمجلس الوطني للمقاومة الإيرانية، إلى أعضاء تلك الحركة، حيث احتوت هذه المستندات على برنامج ضار نشّط عدداً من أوامر برامج التجسس من خادم خارجي عندما فتحها المستلمون على أجهزة الكمبيوتر المكتبية أو الهواتف([٣٩]).

من ناحية أخرى، مكّن برنامج التجسس المهاجمين من الوصول إلى أي ملف تقريباً وتسجيل بيانات الحافظة والتقاط لقطات للشاشة وسرقة المعلومات، وتنزيل البيانات المخزنة على برنامج واتس آب أيضاً. بالإضافة إلى ذلك، اكتشف المهاجمون الإيرانيون ضعفاً في بروتوكولات التثبيت للعديد من التطبيقات المشفرة بما في ذلك تلغرام، التي كانت تُعدَّ دائماً آمنة نسبياً، ما مكّنهم من سرقة ملفات تثبيت التطبيقات، وإنشاء عمليات تسجيل دخول على تلغرام لتنشيط التطبيق في أسماء الضحايا على جهاز آخر ما أتاح للمهاجمين مراقبة جميع أنشطة تلغرام للضحايا سراً([٤٠]).

القدرات السيبرانية الإيرانية في مرآة الواقع الدولي (قراءة نقدية)

قبل أن تصبح تكنولوجيا المعلومات متاحة على نطاق واسع، ركزت الحكومة الإيرانية عملياتها الاستخباراتية في الخارج على تجنيد عملاء للتجسس واغتيال المعارضين السياسيين أو دبلوماسيي الخصوم، والتخطيط لمؤامرات إرهابية في الخارج، وعادة ما تسببت هذه العمليات المخابرتية في إحراج دولي لطهران، خاصة لدى اعتقال المهاجمين.

لكن مع اندلاع ثورة المعلومات وتطور القدرات السيبرانية الإيرانية، وفرت الهجمات السيبرانية فرصاً أقل خطورة لجمع المعلومات الاستخباراتية والانتقام مما تعدَّه طهران عدواً داخلياً أو خارجياً، مع قدرة كبيرة على الإنكار والنفي مقارنة بالعمليات الاستخباراتية السرية. وعلى مدى العقد الماضي، أصبحت العمليات

السيبرانية أداة رئيسة للسياسة الإيرانية لأغراض مثل التجسس، والانتقام، والقمع الداخلي، متبعةً في هجماتها نمطاً ثابتاً من التهديدات التي طالت مجموعة من الأهداف المحددة.

رغم ذلك، بدت الهجمات السيبرانية الإيرانية بدائية مقارنة بالهجمات التي ترعاها الحكومات في البلدان المتقدمة، ناهيك بأن حجم الخبرات واللوجستيات والاستثمار المطلوب لتنفيذ عمليات مثل الألعاب الأولمبية (فيروس ستوكس نت) لا يزال يتجاوز إلى حد كبير قدرات عملاء التهديد الإيراني. وعلى عكس العمليات السيبرانية الأمريكية والإسرائيلية، التي نفذتها أجهزة استخبارات محترفة مدعومة بمليارات الدولارات، لا تزال قدرات إيران الهجومية والدفاعية في المجال السيبراني فوضوية، وتفتقر إلى التمويل. وبالتالي، على الرغم من أن إيران غالباً ما تلجأ إلى تنفيذ الهجمات المدمرة لممارسة الضغط أو الانتقام، إلا أن قدراتها وفرصها تبقى محدودة، وضعيفة لتهديد خصومها المتقدمين، خاصة الولايات المتحدة وإسرائيل.

ما يؤكد ذلك هو الهجمات السيبرانية الإيرانية المستمرة والمتكررة ضد المصالح السعودية ذات الاستعداد والقدرات الدفاعية السيبرانية الأضعف مقارنة بنظيرتها الأمريكية والإسرائيلية. من ناحية أخرى، إنَّ ما يتحدث به المسؤولون الإيرانيون عن القوة العسكرية للبلاد، بما في ذلك القدرات السيبرانية، هو من باب التضخيم والمبالغة، ونادراً ما أعلنت طهران مسؤوليتها عن الهجمات السيبرانية، وأدلت بتصريحات متناقضة حول وضعها السيبراني.

وعلى الرغم من أن وسائل الإعلام الإيرانية تؤكد دائماً القدرات الدفاعية والهجومية للبلاد في المجال السيبراني، مستشهدةً بذلك بتقارير منشورة على وسائل الإعلام الغربية([٤١])، إلا أن طهران لا تعترف رسمياً بما تنفذه من هجمات سيبرانية ضد أعدائها، وتنفي دائماً تعرضها لأي خسائر ناجمة عن هجوم سيبراني مضاد.

وعلى ما يبدو، يسعى الخطاب الرسمي للنظام الإيراني إلى التضخيم والتهويل من القدرات السيبرانية الإيرانية، لكن في الوقت ذاته يقدم نفسه على أنه ضحية للعدوان الأجنبي (الأمريكي والإسرائيلي)، مستعيناً بتقارير الهجمات السيبرانية المدمرة التي وجهت ضد إيران خلال العقود الماضية.

وعلى سبيل المثال، عندما اتهمت الولايات المتحدة إيران بتنفيذ هجوم مدمر على البنوك الأمريكية (أبابيل)، رد نائب وزير الخارجية الإيراني حسين جابري أنصاري أن "الحكومة الأمريكية التي شنت هجمات

سيبرانية على منشآت إيران النووية السلمية، عرضت حياة الملايين من الأبرياء لخطر كارثة بيئية، وهي ليست في موضع يمكّنها من اتهام مواطني الدول الأخرى، بما في ذلك إيران، بدون وجود أدلة مبررة".([٤٢])

على الرغم من كل هذه الادعاءات، لم تنجح إيران في تطوير صناعة أمن سيبراني كامل وشامل، وفيما يتعلق بالاستثمار في الدفاع أو صياغة السياسات الوطنية لتأمين البنية التحتية الحيوية، فإنها لا تزال متخلفة عن الأنظمة الاقتصادية المتقدمة ومنافسيها الرئيسيين في المنطقة. صحيح أن الحكومة الإيرانية أنفقت عشرات الملايين من الدولارات على الأمن السيبراني في السنوات الأخيرة، لكن استثماراتها يبدو أنها تفشل أمام مليارات الدولارات التي تنفقها سنوياً الحكومة الأمريكية أو مئات الملايين من الدولارات التي تنفقها البنوك الأمريكية بشكل منفصل. وحتى لو ركزت إيران على تحسين قدراتها الدفاعية، فإنها ستظل تواجه قيوداً كبيرة بسبب العقوبات، ونقص المهارات المتخصصة. وبالنظر إلى خبرة أعداء إيران ومهاراتهم، يجب على المرء أن ينظر بعين الشك إلى تصريحات الحكومة الإيرانية المتعلقة بالتعقب السريع ومنع التسلل الأجنبي إلى الشبكات الإيرانية.

تعدّ إيران دولة من الدرجة الثالثة في قدراتها السيبرانية، فهي تفتقر إلى مؤسسات الأمن السيبراني المتقدمة القادرة على إجراء عمليات ماهرة، كما في دول مثل الصين وإسرائيل وروسيا والولايات المتحدة.

صحيح أن المهارات التقنية لإيران لا تمنعها من تنفيذ عمليات سيبرانية ناجحة، لكن هذه الإجراءات لا تزال تشير إلى وجود فوضى، ونقص خبرة في الهجمات التي تسبب أضراراً محدودة يمكن إصلاحها في وقت قصير. وفي الحقيقة، لقد حرمت العزلة السياسية والعقوبات الاقتصادية المفروضة على طهران الدولة من الحصول على التكنولوجيا والخبرة من الدول أو الشركات الأجنبية، وعلى ما يبدو فشلت إيران في زيادة قدراتها السيبرانية بسبب العقوبات الشديدة، إذ هي غير قادرة على الحصول على التقنيات اللازمة وتدريب الخبراء المهرة في المجال السيبراني. وعلى الرغم من أن المسؤولين الأمريكيين وبعض شركات الأمن السيبراني يعتقدون أن طهران تلقت مساعدة فنية من دول مثل روسيا وكوريا الشمالية والصين، إلا أنه لا يوجد دليل على وجود تعاون كبير بين إيران ودول أخرى في مجال تطوير قدرات الهجوم السيبراني الإيراني. صحيح أن إيران حصلت على أجهزة مراقبة الإنترنت من شركات الاتصالات الصينية([٤٣]) ودخلت في اتفاقيات تعاون في مجال الأمن السيبراني مع روسيا، لكن هذه العلاقات تختلف عن تزويد طهران بقدرات هجوم سيبراني. إضافة لذلك أظهر الإيرانيون موهبتهم في الهندسة الاجتماعية (خداع

الضحايا للوقوع بأفخاخ القرصنة)، وهذا لا يعني ببساطة أنهم حصلوا على هذه المواهب من التعليم الأجنبي أو نقل التكنولوجيا لهم. وفي الحقيقة، استخدم عملاء التهديد الإيراني مراراً وتكراراً أدوات القرصنة الاحترافية الجاهزة لتشغيل حملاتهم، ولكن لا توجد أدلة على أن طهران حصلت من حكومات أجنبية على برامج ضارة، في حين لا تشير أي من الهجمات، التي سجلت علنًا أو روقبت سراً، إلى استخدام أدوات أو موارد تتجاوز قدرة عملاء التهديد الإيراني.

خلاصة واستنتاجات

طوال العقود الأربعة الماضية، أخذت التوترات المتصاعدة بين إيران والولايات المتحدة منحىً جديداً داخل الفضاء السيبراني، إذ كانت طهران أحد أهداف الولايات المتحدة الرئيسة لعمليات السيبرانية الهجومية المدمرة والفريدة، وفي الوقت ذاته، كانت الهجمات السيبرانية التي نفذتها إيران واحدة من أكثر الهجمات تعقيداً وأهمية في تاريخ الإنترنت.

ما سبق يقودنا إلى مجموعة من الاستنتاجات والخلاصات التالية:

- أصبحت عمليات الهجوم السيبراني إحدى الأدوات الرئيسة للحكم في إيران، لأنها وفرت فرصاً أقل خطورة وتكلفة بالنسبة لطهران لجمع المعلومات والانتقام من الأعداء داخل البلاد وخارجها.
- أشارت مجموعة التكتيكات والأدوات وعملاء التهديد الإيراني خلال التحديات الداخلية الذي واجهها النظام في العقود الماضية إلى الوضع السيبراني لإيران في مواجهة مجموعة واسعة من التهديدات الداخلية والخارجية، لكن السمات الثابتة للعمليات السيبرانية الإيرانية منذ البداية أظهرت عدم وجود حدود واضحة بين العمليات ضد المعارضة المحلية والأعداء الأجانب، فقد استخدم عملاء التهديد الإيراني في الحملة ضد صناعة الدفاع الأمريكية البنية التحتية نفسها والأدوات المستخدمة في الحملات التي استهدفت برامج اللغة الفارسية المتعلقة بالنهوض بالمرأة مثلاً، كما أن البرمجيات الخبيثة نفسها المستخدمة في الهجمات المدمرة على المؤسسات الحكومية السعودية سبق استخدامها لمراقبة أعضاء الحركة الخضراء المعارضة.
- بينما تستخدم إيران ميليشياتها العميلة لإثبات قوتها الإقليمية في المنطقة، فإنها غالباً ما تستخدم وكلاءها السيبرانيين لإخفاء عملياتها الإلكترونية لإنكار مسؤوليتها رسمياً، وذلك رغم

وجود مؤشرات واضحة على أن مثل هذه العمليات نفذتها المجموعات السيبرانية التابعة للحرس الثوري، ولوزارة المخابرات الإيرانية.

- رغم أن إيران لا تمتلك القدرات السيبرانية المتطورة التي تملكها دول مثل الولايات المتحدة وإسرائيل وروسيا والصين، إلا أن عملياتها السيبرانية التخريبية أظهرت أوجه القصور وعدم الاستعداد للأهداف المعرضة للخطر داخل وخارج البلاد، خاصة المصالح السعودية، وأنه يمكن شن حرب المعلومات باستخدام أدوات وتكتيكات بدائية وبسيطة، وذلك لفرض تكاليف انتقامية باهظة على أعدائها.

هوامش:

[١] امير رشيدي – ما هو الهجوم السيبراني – بي بي سي فارسي - https://www.bbc.com/persian/science-54597932

[٢]المرجع رقم ١

[٣] ضياء قدور – كيف استطاع الموساد والـ CIAاختراق منشأة نووية في إيران؟ - https://bit.ly/2W8IiOv

[٤]المرجع رقم ٣

[٥] وزارة الخارجية الأمريكية تتحدث إلى تويتر بشأن إيران – رويترز – https://www.reuters.com/article/us-iran-election-twitter-usa-idUSWBT01137420090616

[٦]تاريخ الهجمات السيبرانية الإيرانية والحوادث – موقع متحدون ضد إيران النووية – https://www.unitedagainstnucleariran.com/history-of-iranian-cyber-attacks-and-incidents

[٧]تشارلز آرثر: اختراق موقع تويتر من قبل "الجيش السيبراني الإيراني" هو في الحقيقة مجرد توجيه خاطئ – الغارديان - https://www.theguardian.com/technology/blog/2009/dec/18/twitter-hack-iranian-cyber-army-dns-mowjcamp

[٨]كيفن جيه أوبراين: توسيع التحقيق الهولندي في قرصنة المواقع الرسمية – نيويورك تايمز - https://www.nytimes.com/2011/09/07/technology/dutch-widen-probe-into-hacking-of-official-sites.html

[9]قراصنة مرتبطون بالحرس الثوري الإيراني يستهدفون المقربين من روحاني- بي بي سي فارسي - https://www.bbc.com/persian/iran-42558658

[١٠]المرجع رقم ٦

[١١] القضاء الأمريكي يتهم عناصر بالمخابرات الروسية باختراق انتخابات ٢٠١٦ – موقع DWالعربي - https://bit.ly/3n6Aqc3

[١٢]انتشار الأزمة الإيرانية إلى الفضاء السيبراني – معهد واشنطن – https://www.washingtoninstitute.org/policy-analysis/view/iran-crisis-moves-into-cyberspace/fa

[١٣]الولايات المتحدة تتهم ٧ إيرانيين بارتكاب هجمات إلكترونية على البنوك والسدود – موقع forbes - https://www.forbes.com/sites/thomasbrewster/2016/03/24/iran-hackers-charged-bank-ddos-attacks-banks/

[١٤]استخدام إيران للحرب الاقتصادية عبر الإنترنت – مؤسسة الدفاع عن الديمقراطية – https://www.fdd.org/analysis/2018/11/06/evolving-menace/

[١٥]الولايات المتحدة تقول إيران اخترقت أجهزة الكمبيوتر الخاصة بمشاة البحرية – وال ستريت جورنال – https://www.wsj.com/amp/articles/us-says-iran-hacked-navy-computers-1380314771

[١٦]جيروساليم بوست ومواقع إسرائيلية أخرى تم اختراقها من قبل وكيل التهديد الإيراني - CopyKitten موقع clearskysec - https://www.clearskysec.com/copykitten-jpost/

[١٧]تحذير فاير آي من هجمات سيبرانية إيرانية محتملة على أهداف في ألمانيا - DWفارسي - https://m.dw.com/fa-ir/هشدار-فایرآی-نسبت-به-حملات-احتمالی-سایبری-ایران-به-اهدافی-در-آلمان/a-52381179

[١٨]عملاء التهديد الإيرانية تشير إلى مجموعات الهكرز الموالية للنظام الحاكم في إيران.

[١٩] سجلات تحقيق هيلاري ر. كلينتون، المستند ٣، مقابلة مع مكتب التحقيقات الفيدرالي من ٣ فبراير ٢٠١٦ - https://vault.fbi.gov/hillary-r.-clinton

[٢٠]الأنشطة السيبرانية الإيرانية في سياق المنافسات الإقليمية و التوترات الدولية - https://www.research-collection.ethz.ch/bitstream/id/5647001/20190507_MB_HS_IRNV1_rev.pdf?

sequence=1

[٢١]المرجع رقم ١٩

[٢٢] المرجع رقم ١٩

[٢٣] الأبعاد المحتملة للحرب السيبرانية بين إيران والولايات المتحدة – DWفارسي - https://m.dw.com/fa-ir/ابعاد-احتمالی-جنگ-سایبری-میان-ایران-و-آمریکا/a-51944656/

[٢٤]المرجع رقم ١٩

[٢٥] انفجار يقتل أستاذ الفيزياء في طهران - نيويورك تايمز – https://www.nytimes.com/2010/01/13/world/middleeast/13iran.html

[٢٦]المرجع رقم ١٩

[٢٧] الاستراتيجية الجيوسياسية لإيران والهجمات الإلكترونية لـ APT33 – lab52 - https://lab52.io/موقع blog/geopolitical-strategy-of-iran-and-the-cyberattacks-of-apt33/

[٢٨]هجمات مهدي: سلسلة حملات الهندسة الاجتماعية – https://www.globalsecuritymag.fr/The-Madi-Attacks-Series-of-Social,20120718,31449.html

[٢٩]"إيران تتجسس على إسرائيل والسعودية بهجمات إلكترونية كبيرة" – تايمز أوف اسرائيل – https://www.timesofisrael.com/iran-spied-on-israel-saudi-arabia-with-major-cyberattack/amp/

[٣٠]المرجع رقم ١٤

[٣١] اتصالات إيران، تقرير الإنترنت ٢٠١٦–٢٠١٧ – Financial Tribune - https://financialtribune.com/articles/economy-sci-tech/63062/iran-telecoms-internet-report-2016-17

[٣٢]"غوغل" يحذر من "تلغرام الذهبي" الإيراني لتلوثه ببرامج تجسس – إيران انترناشيونال – https://bit.ly/3oIRSDP

[٣٣]تمكن قراصنة إيرانيون من الوصول إلى أرقام هواتف ١٥ مليون مستخدم إيراني لبرنامج تلغرام – بي بي سي فارسي – https://www.bbc.com/persian/

iran/2016/08/160802_l12_iran_telegram_hack

[٣٤]المرجع رقم ٩

[٣٥] المرجع رقم ٩

[٣٦] المرجع رقم ١٩

[٣٧] فرنسا تطرد دبلوماسيا إيرانيا ردا على مؤامرة لشن هجوم على مؤتمر لمجاهدي خلق – إيران بلا أقنعة – https://bit.ly/3mbSD6S

[٣٨]قال باحثون إن قراصنة إيرانيين وجدوا طريقة في تطبيقات مشفرة – نيويورك تايمز – https://www.nytimes.com/2020/09/18/world/middleeast/iran-hacking-encryption.html

[٣٩]المرجع رقم ٣٧

[٤٠] المرجع رقم ٣٧

[٤١] إيران من بين القدرات السيبرانية العشرة في العالم/ هل اخترقت إيران البنوك الأمريكية ولعبة صراع العروش؟ – موقع اقتصاد نيوز الإيراني – https://bit.ly/2ILYn9I

[٤٢]جابري انصاري: امريكا ليست مؤهلة لتوجيه اتهام لايران بالهجمات السايبرية – وكالة أنباء مهر الإيرانية – https://bit.ly/2W6f0Qv

[٤٣]نائب إيراني: سننجز شبكة الإنترنت الوطنية بالتعاون مع الصين – العربية نت – https://bit.ly/3qNE5h7


MENA
RESEARCH
CENTER
مركز أبحاث ودراسات مينا