فراس إلياس | نشر في ١٤ أغسطس ٢٠١٩,

عقيدة الأمن السيبراني في إيران ومعادلات المواجهة مع أمريكا

إن تطور عقيدة الأمن السيبراني في إيران، أخذت تفرض نفسها في إطار إستراتيجية الأمن القومي الإيراني، ولا بد من القول إن الركيزتين الرئيسيتين لهذه العقيدة هما: الأولى تتمثل بحماية الأمن الوطني الإيراني عن طريق بناء بنية تحتية علمية، تكنولوجية واستخبارية، تعتمد على إستراتيجية وقائية في أثناء الدفاع وإستراتيجية استباقية في أثناء الهجوم، أما الركيزة الثانية فتتمحور حول تطوير العديد من المفاهيم والتقاليد القتالية الخاصة بها، وذلك عن طريق تشكيل شبكة معقدة من الجيوش الإلكترونية القادرة على شن هجمات سيبرانية متعددة على أهداف محددة في آن واحد، هذا إلى جانب تفعيل قدراتها الاستخبارية في نشر المعلومات المضللة وإجهاض المسيرات المناهضة للحكومة الإيرانية.

ولتحقيق هذه الأهداف، أنشأت إيران مؤخرًا شبكة متطورة من المؤسسات التعليمية والبحثية، فضلًا عن الدور الذي تؤديه وزارة الاتصالات وتكنولوجيا المعلومات، ومركز أبحاث الاتصالات الإيراني، في مختلف مجالات التكنولوجيا المتقدمة، بما في ذلك أمن المعلومات، علاوة على ذلك، تم إنشاء منصب مسؤول التعاون التكنولوجي المرتبط بمكتب رئيس الجمهورية، إذ تم تأسيس الرقابة على مشاريع البحوث في مجال تكنولوجيا المعلومات على أعلى مستوى في الحكومة الإيرانية، ولضمان تنفيذ هذا الغرض، أوجدت إيران منظومة الإنترنت الحلال (وهو مشروع إنترنت وطني تديره وزارة الاستخبارات والأمن الوطني الإيراني)، كما أن هناك مركزًا مختصًا بأمن المعلومات يعمل تحت إشراف وزارة الاتصالات وتكنولوجيا المعلومات الإيرانية.

في مايو 2009، أدخلت شركة Security American اسم إيران بين الدول الخمسة التي تتمتع بأقوى قدرات إنترنت في العالم، فضلًا عن ذلك تستخدم إيران وحدات تكميلية أقل كفاءة إلى حد ما من وحدات

الإنترنت المركزية الإيرانية

إن الجزء الأكثر نشاطًا في العمليات السيبرانية الإيرانية اليوم، تقوم به قيادة الدفاع السيبراني الإيراني التي تأسست في نوفمبر 2010، وتعمل تحت إشراف منظمة الدفاع الوقائي، وهي وحدة مستقلة ضمن هيئة الأركان الإيرانية المشتركة، إذ يتم تنفيذ الجزء الأفضل من العمليات السيبرانية من الجيوش الإلكترونية الإيرانية التي توظف اختصاصيين مؤهلين تأهيلًا عاليًا في مجال تكنولوجيا المعلومات، ومن الوحدات الأكثر نشاطًا في هذا الجيش فريق الأمن الرقمي الذي أصبح معروفًا بالتزامه الأيديولوجي تجاه الحكومة الإيرانية.

في حين أصبحت القدرات الفنية للقوات السيبرانية الإيرانية واضحة جدًا، فتمكنت من التسلل مرارًا إلى الحكومات الغربية وشبكات الاستخبارات الإقليمية، فعلى الرغم من كل الإجراءات الأمنية التي تم اتخاذها في ديسمبر 2011، أشار المدير التنفيذي لشركة Google إريك شميدت، في مقابلة مع شبكة CNN الأمريكية، إلى أن الإيرانيين موهوبين على نحو غير معتاد في الحروب السيبرانية الحديثة، وذلك لأسباب لا تفهمها الولايات المتحدة.

في مايو 2009، أدخلت شركة Security American اسم إيران بين الدول الخمسة التي تتمتع بأقوى قدرات إنترنت في العالم، فضلًا عن ذلك تستخدم إيران وحدات تكميلية أقل كفاءة إلى حد ما من وحدات الإنترنت المركزية الإيرانية، فإلى جانب جيش الباسيج الإلكتروني للعمليات الداخلية، أوجد مجلس الأمن القومي الإيراني العديد من الوكالات الإلكترونية، التي تعمل ضمن إطار المجلس الأعلى للفضاء السيبراني، ومن أبرزها:

1- قيادة الدفاع السيبراني.

2- الجيش السيبراني الإيراني.

3- مركز تنسيق المعلومات.

4- جيش قوة القدس السيبراني (العمليات الخارجية).

5- الجيش السوري السيبراني .SEA

6- مجموعة مقاتلي القسّام الإلكترونية.

7- مجموعة سيف العدل.

8- كتائب حزب االله الإلكترونية.

9- مجموعة بارستوا الإلكترونية.

10- جهاز الشرطة (الأمن السيبراني الداخلي).

11- لجنة تحديد ومتابعة المواقع غير المصرح بها.

وفي هذا الإطار أيضًا، أشار راندون فاليريانو، وهو باحث في جامعة كارديف ومؤلف كتاب "حرب الإنترنت مقابل الحقائق السيبرانية" الذي نشرته مطبعة جامعة أكسفورد عام 2015، أمام لجنة الأمن الداخلي والشؤون الحكومية بمجلس الشيوخ الأمريكي في 10 من مايو 2017، أن قدرات إيران في الحرب السيبرانية والتجسس أقل شأنًا مقارنة بقدرات دول مثل الولايات المتحدة و"إسرائيل" وروسيا والصين، وتلك الخاصة بعدد من الدول الأوروبية.

لكن بالنسبة للدكتور لفاليريانو، فإن الخطر الحقيقي في العمليات السيبرانية الإيرانية لا يكمن في قدراتها وإجراءاتها المباشرة، بل في استخدامها السائد للوكالات السيبرانية، ففي شهادته أمام أعضاء مجلس

الشيوخ الأمريكي، قال إن"الخطر الرئيسي من إيران، تمامًا كما هو الحال في مداخل التهديدات الإرهابية، بأن تستخدم إيران الجهات الفاعلة بالوكالة لمهاجمة أهداف غربية، إن تمكين هؤلاء الفاعلين، أي الجيوش الإلكترونية المرتبطة بها، قد يكون خطيرًا إذا كانت إيران ستنقل التكنولوجيا إلى هذه الجماعات التي يمكنها عندئذ استخدام نقاط ضعف معروفة في عملياتها".

وتأكيدًا لهذه المخاوف الأمريكية، فبعد تمكن الولايات المتحدة الأمريكية من شن هجمات سيبرانية على العديد من المواقع الإلكترونية في إيران يوم 7 من أبريل 2018، تمكنت إيران في اليوم التالي من شن هجمات داخل الولايات المتحدة الأمريكية، عبر كتائب القسام الإلكترونية والجيش السوري الإلكتروني.

ترى إيران في الإنترنت وسيلة للتحكم بسكانها والدفاع ضد الحرب الناعمة وشنّها وجمع المعلومات الاستخبارية وردع الهجمات في المجال السيبراني والمجال المادي وضرب الأعداء من أجل تحقيق آثار نفسية وجسدية

تبرز الحرب السيبرانية باعتبارها السلاح المفضل لإيران للتعامل مع الخصوم المحليين والأجانب، ولأكثر من عقد من الزمان، شنت إيران حملة قهرية ضد المعارضين للنظام، علاوة على ذلك، في أعقاب اكتشاف الهجمات الإلكترونية على برنامجها النووي عام 2010، وفرض عقوبات جديدة على قطاعيها النفطي والمالي عام 2011 وما بعده، نفذت هجمات إلكترونية انتقامية ضد أهداف قطاع النفط في المملكة العربية السعودية، وضد القطاع المالي الأمريكي، في الوقت نفسه، وزادت بشكل كبير جهود الاستطلاع الإلكتروني ضد المسؤولين الأجانب المشاركين في السياسات العدائية ضد إيران، وخاصة في الولايات المتحدة، إذ تؤكد هذه الأحداث الأهمية المتزايدة التي تعلقها إيران على قدراتها الإلكترونية، التي من المحتمل أن تضطلع بدور أكبر في السنوات القادمة.

ترى إيران في الإنترنت وسيلة للتحكم بسكانها والدفاع ضد الحرب الناعمة وشنّها وجمع المعلومات الاستخبارية وردع الهجمات في المجال السيبراني والمجال المادي وضرب الأعداء من أجل تحقيق آثار نفسية وجسدية، فالاعتماد المتفشي للاقتصادات المتقدمة على تكنولوجيا المعلومات والاتصالات، يضمن أن إيران ستكون دائمًا لديها أهداف ضعيفة للهجوم عليها، ومن أجل أن تكون مصدر إزعاج أو فرض تكاليف على الأعداء، قد تسمح لها الحرب السيبرانية بأن تضرب بقوة، وعلى الفور، وعلى أساس مستمر، بطرق غير ممكنة في المجال المادي.

يمكن القول إنه في ضوء النسق التصاعدي لصراع الإرادات بين إيران والولايات المتحدة الأمريكية في منطقة الخليج العربي ومضيق هرمز، فإن الحرب السيبرانية أكثر ميدان مرشح للتصاعد خلال الفترة القادمة

تحتاج الولايات المتحدة إلى مواصلة الجهود لوضع معايير تحظر الهجمات السيبرانية على البنية التحتية الحيوية، وتضمن استخدام الإنترنت وفقًا لقانون النزاع المسلح (على سبيل المثال، تسترشد بمبادئ التمييز والضرورة العسكرية والتناسب)، في حين من المؤكد أن إيران ستنتهك بالتأكيد أي مدونة سلوك إلكترونية توافق عليها، تمامًا كما انتهكت بشكل متكرر التزاماتها بموجب القانون الدولي، عن طريق مهاجمة السفارات والمشاركة في دعم الإرهاب وكسر التزاماتها بعدم الانتشار النووي، فوجود مثل هذه المعايير سيوفر للولايات المتحدة قوة للضغط، من أجل فرض عقوبات إذا فعلت إيران ذلك.

هذا إلى جانب مواقف أقوى للردع عبر الفضاء السيبراني والقوة العسكرية تجاه إيران، التي يمكن أن تساعد على الأقل في تقييد سلوك إيران في المجال السيبراني، ومن ثم يقلل من فائدة هذه الإمكانية التي قد تؤدي إلى تغيير قواعد اللعبة بين إيران من جهة، والولايات المتحدة الأمريكية من جهة أخرى.

كما يمكن القول إنه في ضوء النسق التصاعدي لصراع الإرادات بين إيران والولايات المتحدة الأمريكية

في منطقة الخليج العربي ومضيق هرمز، فإن الحرب السيبرانية أكثر ميدان مرشح للتصاعد خلال الفترة القادمة، فكلا الطرفين يفضلان خوض الصراع في هذا الميدان، لانخفاض الكلف الإستراتيجية المتوقعة من هذه المواجهة، كما أن إيران لديها خبرة كبيرة في هذا الميدان، وذلك بشنها هجمات سيبرانية على منظومات القيادة والسيطرة أو البنية التحتية الأمريكية، بالمستوى الذي لا يدفع الولايات المتحدة الأمريكية إلى التطرف بالرد أو على الأقل مراعاة النسبة والتناسب في حالات الرد المستجابة.

رابط المقال: https://www.noonpost.com/28950/