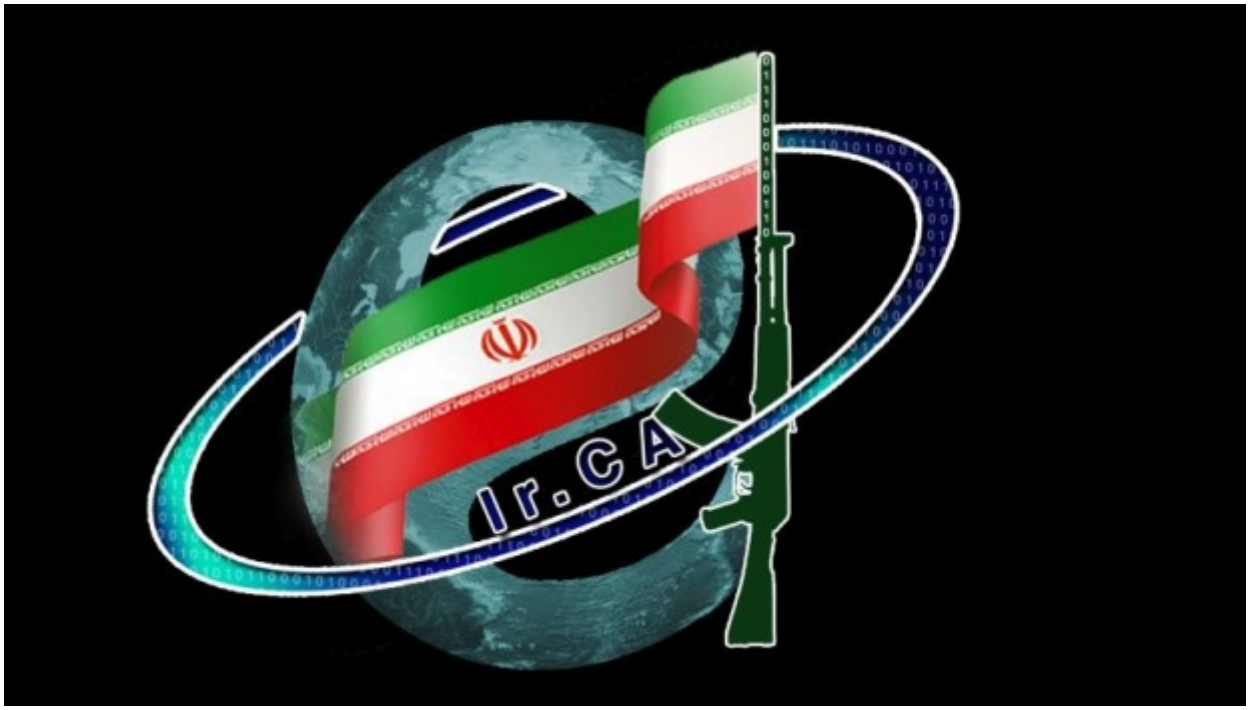
حروب الانترنت: الجيش الإلكتروني الإيراني



باستثناء إسرائيل، تعد إيران من أوائل دول المنطقة في تطوير جيش إلكتروني، وهي تمتلك الجيش الأكبر على صعيد المنطقة إن لم يكن الأوحد. وفقًا لنائب ممثل المرشد الأعلى في الحرس الثوري العميد محمد حسين سبيهر، فإن الحرس الثوري يمتلك رابع أكبر قوّة إلكترونيّة في العالم، علما أنّ البعض يشير إلى أنّه كان من حيث الحجم في وقت من الأوقات الجيش الثاني عالميًّا بعد الصين.

في العام 2009، بدأت مجموعة تسمي نفسها "الجيش الإلكتروني الإيراني" (ICA) بالظهور على الساحة رويدًا رويدا، وقد تزامن ذلك مع الانتخابات الرئاسيّة الإيرانيّة عام 2009، حيث يعدّ ذلك العام بداية تدشين العمل الحقيقي للقوات الإلكترونيّة الإيرانيّة. ركّزت السلطات الإيرانيّة آنذاك على عزل وتفكيك أنشطة المعارضة "الحركة الخضراء" داخليًّا إثر اعتمادها بشكل كبير –آنذاك- على التواصل بين أعضائها داخل إيران ومؤيديها خارج إيران من جهة، والتواصل مع العالم الخارجي من جهة أخرى على الإنترنت ووسائل التواصل الاجتماعي.

وتم على إثر ذلك إغلاق معظم مواقع الحركة الخضراء الإلكترونية، وقطع تواصلهم، ومراقبة حساباتهم في وسائل التواصل الاجتماعي، ونقلت بعض التقارير أنّ مجموعة إلكترونية واحدة استطاعت السيطرة على حوالي 300 ألف جهاز حاسوب داخل إيران تم اختراقها عبر تحويلها إلى صفحة حساب "جي ميل" (وهميّة) تم استغلالها لأعمال المراقبة والتجسس على الأغلب على مستخدميها.

وقد استخدمت تقنيات إلكترونية شديدة التعقيد ساهمت في ملاحقة وتعقب وإلقاء القبض على المعارضين الإيرانيين، ولإغلاق وتعطيل كل المنافذ الممكنة والمحتملة للثورة الخضراء على المستوى الإلكتروني في البلاد، ولقطع كل ما يتعلق بها من أخبار في الداخل إلى العالم الخارجي.

وعلى الرغم من أنّ الحرس الثوري لم يعلن امتلاكه لجيش إلكتروني آنذاك، إلا أنّ ذلك يتماشى مع منطق عمله في إنكار العمليات التي يقوم بها، كما أنّ البنية التحتية والقدرات الإلكترونية التي يتمتع بها هذا الجيش تؤكد صلته بالحرس الثوري.

لقد اقتصرت الأماكن المستهدفة آنذاك على المستوى الداخلي، أمّا الهجمات الخارجيّة للجيش الإلكتروني الإيراني فلم تستهدف مؤسسات أو مصالح خارجيّة عالية الخطورة، وإنما تمّ التركيز على شن سلسلة هجمات على مستوى عالٍ على مواقع مشهورة ليضع نفسه على ما يبدو تحت الأضواء على المستوى العالمي، ويرسل رسائل ذات طابع سياسي أكثر منها ذات طابع حربي خاصة عندما هاجم ونجح في قرصنة كل من موقع "تويتر" العالمي عام 2009، وموقع "بايدو" الذي يعد محرك البحث الأشهر في الصين عام 2010 وموقع صوت أمريكا الشهير.

الا أنّ عمله بدأ يتطور بعد ذلك، كما اتسعت رقعة الأماكن والمواقع والمؤسسات المستهدفة مما بدأ يطرح تساؤلاً حول الجهة الحقيقية المسئولة عن هذه المجموعة، وما هي قدرات إيران الحقيقيّة للقيام بحرب إلكترونيّة.

قدرات إيران في الحرب الإلكترونية

يضع تقرير صادر في العام 2008، لـ"ديفانس تيك" إيران في المرتبة الخامسة عالميًا من حيث الدول التي تمتلك قدرات حرب إلكترونيّة مهمة. أمّا "ريتشارد كلارك" -المسؤول السابق في مجلس الأمن القومي الأمريكي ومؤلّف كتاب "الحرب الإلكترونية"- فقد كان قد صنّف في كتابه هذا الصادر في عام 2010 إيران على أنّها تقع مباشرة بعد الصين من حيث امتلاك القدرات الهجوميّة في الحرب الإلكترونيّة.

لكن ووفقًا لعدد من الخبراء في مجال الإنترنت والشبكات الإلكترونية، فإن إيران تصنّف بالعموم على أنّها من دول الصف الثالث من حيث القدرات الإلكترونية فيما يتعلق بالحرب الإلكترونية، لكنّ هذا التصنيف لا يعني أنّها غير قادرة على إلحاق الأذى والدمار بدول الصف الثاني والأوّل، ولا يلغي أيضًا حجم التهديدات الصادرة عن جيشها الإلكتروني، أو ما يسمى محاربو الإنترنت.

وبخلاف قوى أخرى مثل روسيا والصين، فإن الاهتمام الإيراني بالحرب الإلكترونيّة إنما يدور حول نزاعها الدائم مع بعض الدول الغربية، فيركّز على قدرات الرد في إلحاق الأذى أكثر من التركيز على عمليات التجسس والسرقة، خاصّة بعد التجربة المريرة التي مرّت بها إثر تعرّضها لفايروس "ستاكسنت" الذي أصاب برنامجها النووي.

في العام 2011، لوحظ قيام السلطات الإيرانية بعملية تجنيد واسعة لتعزيز القدرات الإلكترونية في البلاد من خلال البحث عن قراصنة محترفين، وأيضًا عن شباب طموح يتقن تقنيات الكمبيوتر والالتفاف على أجهزة المراقبة الحكومية، والقيام بإغرائهم بمبالغ طائلة من أجل تجنيدهم وتحويلهم إلى قراصنة محترفين.

وفقًا لمحسن سازيغارا -وهو عضو سابق في الحرس الثوري- فإن النظام الإيراني يدفع حوالي 10 آلاف دولار شهريًا لهؤلاء. وعلى الرغم من أنّ هذا الرقم يعدّ رقمًا كبيرًا جدًا في إيران، إلا أنّه يعدّ صغيرًا مقارنة بالمهمّة التي يقوم بها هؤلاء، ومقارنة بالتكلفة التي من المفترض أن تتحملها الدولة في حال أرادت شنّ حرب تقليديّة.

بعض التقارير الإسرائيليّة تشير إلى أنّ إيران رصدت على الأقل مليار دولار للحصول على تقنيات وتكنولوجيا وتجنيد وتدريب وتوظيف خبراء في هذا المجال لتطوير قدراتها في الحرب الإلكترونيّة. وقد صرّح العميد "قولامريزا جلالي" أنّ بلاده ستقاتل العدو حتى في الفضاء الإلكتروني وعبر حروب الإنترنت.

وقد رصدت عدة تقارير استخباراتيّة –آنذاك- محاولات إيران استهداف عدد من المؤسسات الحكوميّة الأمريكيّة بهجمات إلكترونيّة من بينها مخططات لاستهداف منشآت نووية أمريكيّة كان قد تمّ الكشف عنها في نهاية عام 2011. كما نسب عدد من المتخصصين في مجال الأمن الإلكتروني في عام 2012 سلسلة من الهجمات الإلكترونية التي استهدفت مؤسسات اقتصاديّة وماليّة أمريكيّة شهيرة (منها جي

بي مورغان، ات اس بي سي، ستي جروب، سن ترست) إلى إيران رغم عدم تبني الأخيرة أو أي مجموعة فيها لهذه الهجمات التي أدتّ إلى انهيار المواقع الإلكترونية لبعض هذه المؤسسات، كما أدت إلى خسائر مالية اضطر بنك واحد منها على الأقل إلى إنفاق 10 ملايين دولار كحد أدنى لتحييد هذه الهجمات.

مجموعات مرتبطة بالجيش الإلكتروني الإيراني

بعد شهر يوليو/ تموز من العام 2012، بدأت الهجمات التي تحمل توقيع الجيش الإلكتروني الإيراني ولكن خطيرة عمليات تتبنى أخرى مجموعات صعود مع تزامنت الوقت من لفترة تقريب بالاختفاء (ICA) بأسماء وهميّة، ربط العديد من الخبراء بينها وبين الجيش الإلكتروني الإيراني، كان من بينها:

مجموعة محاربو القسّام الإلكترونية (QCF) : وتبنت في سبتمبر/ أيلول 2012، عمليات استهداف المواقع المالية والمصرفيّة الأمريكيّة.

مجموعة باراستو: وتبنّت في نوفمبر/ تشرين ثاني 2012، عمليات اختراق وتعطيل موقع الوكالة الدولية للطاقة الذريّة (IAEA) ونشر مخططات أوّلية لمفاعلات نووية أمريكية مزمع إنشاؤها على صفحة الموقع.

الجيش الإلكتروني السوري: وهي مجموعة إلكترونية موالية للنظام السوري، استهدفت عملياتها مواقع شهيرة أيضًا مثل "لينكد-إن" و"فايبر" و"تانغو"، بالإضافة إلى مؤسسات إخبارية كان منها "رويترز"، "واسوشياتد برس" في نيسان/إبريل 2013 حيث تم نشر خبر عن انفجار البيت الأبيض وإصابة أوباما، الأمر الذي أدى إلى خسارة مؤشر داو جونز الصناعي 150 نقطة على الفور حينها "تساوي 136 مليار دولار" قبل أن يتم تصحيح الأمر.

بالإضافة إلى مجموعة كانت استهدفت في آب/ أغسطس من العام 2012، شركة أرامكو عملاق الصناعة النفطيّة في السعودية، أكبر دولة منتجة للنفط في العالم.

وقد نسبت هذه الهجمات رغم اختلاف تسمياتها إلى إيران، وربط بعضهم على الأقل بشكل مباشر بينها وبين إيران؛ نظرًا لطبيعة الهجمات التي قامت بها هذه المجموعات، ونوع الأهداف التي جرى الهجوم عليها، والتي ترتبط بشكل أو بآخر بملفات إيرانية كالبنوك الأمريكية التي ترتبط برسالة العقوبات الغربية، وموقع وكالة الطاقة الدولية الذي يرتبط برسالة الملف النووي، ومواقع التواصل الاجتماعي التي ترتبط برسالة المعارضة الإيرانيّة.

البنية التحتية لقدرات إيران على خوض حرب إلكترونية

وتركز طهران بشكل عام في تطوير قدراتها الإلكترونيّة على الجانبين الدفاعي والهجومي. حيث تتجلى الأولويات على الجانبين كما يلي:

في الجانب الدفاعي: الحصول على القدرات اللازمة لحماية المنشآت المهمة والحساسة في البلاد، والبنية التحتية الإستراتيجية التي قد تتعرض لهجمات إلكترونية من قبل دول أو جماعات من خارج البلاد، كهجمات فايروس "ستكسنت" الذي ضرب برنامج تخصيب اليورانيوم المرتبط بالبرنامج النووي الإيراني.

أما في الجانب الهجومي: تجنيد المزيد من المحترفين القادرين على خوض حرب إلكترونيّة، وإلقاء الأذى والخسائر الفادحة في بنية الخصوم التحتيّة، والحصول على التكنولوجيا اللازمة في مجال الحرب الإلكترونية بما يمكّن من التقدّم على هذا الصعيد.

ويستطيع المتابع لجهود إيران في وضع أسس، تطوير، وتحديث البنية التحتيّة اللازمة لخوض حرب

إلكترونيّة أن يصل إلى استنتاج مفاده أنّ برنامج بناء وتطوير الجيش الإلكتروني الإيراني جار بشكل سريع وعلى مستوى متقدّم؛ وذلك نظرًا لكثرة الأجهزة والهيئات والمنظمات والمؤسسات والقطاعات التي تمّ إنشاؤها خلال السنوات القليلة الماضية، والتي تلعب بشكل أو بآخر دورًا مهمًّا في زيادة قدرات البلاد فيما يتعلق بالحرب الإلكترونيّة كل ضمن اختصاصاته، ولعل من أبرز هذه المؤشرات:

في مارس/ آذار من العام 2013، أعلن المرشد الأعلى علي خامنئي إنشاء المجلس الأعلى للفضاء الإلكتروني، والذي يضم رئيس البلاد، والمتحدث باسم البرلمان، ورئيس القضاء الأعلى، قائد قوات الحرس الثوري، قائد قوات الشرطة، وممثل خامنئي في المجلس الأعلى للأمن القومي، والمسئولين عن قطاعات البث الرسمي، وتكنولوجيا المعلومات والعلوم.

دعم إنشاء وتطوير عدد كبير من مؤسسات الأبحاث المرتبطة بعلوم الكمبيوتر وتكنولوجيا المعلومات.

إنشاء وتطوير المؤسسات الحكوميّة الخاصة المرتبطة بهذا الحقل كمركز الأبحاث الإيراني للاتصالات السلكية واللاسلكية التابع لوزارة المعلومات والاتصالات، والذي يلعب دورًا في تخريج المتخصصين لاسيما في أمن المعلومات، ومكتب التعاون التكنولوجي التابع للمكتب الرئاسي، ويحمل على عاتقه إطلاق مبادرات للأبحاث في مجال تكنولوجيا المعلومات.

دعم العديد من الأجهزة والمؤسسات والأذرع ذات الشأن والمرتبطة بالجانب العسكري الدفاعي، كقيادة الدفاع الإلكتروني العاملة تحت إطار منظمة الدفاع الإيراني المحسوبة على رئاسة الأركان في القوات المسلّحة الإيرانيّة، ومهمتها تطوير عقيدة للدفاع الإلكتروني في مواجهة التهديدات المحتملة، بالإضافة إلى مركز "ماهر" لأمن المعلومات الذي يعمل تحت إشراف وزارة الاتصالات وتكنولوجيا المعلومات، ناهيك عن وحدات محليّة كوحدة الشرطة الإلكترونية.

دعم وتعزيز عمل الأجهزة والمجموعات والفرق ذات الطابع الهجومي، ومعظمها مرتبط بالحرس الثوري الإيراني كفريق "أشييان" للأمن الرقمي، ومجلس الفضاء الإلكتروني التابع للباسيج (قوات التعبئة الشعبية) والذي تم إنشاؤه في العام 2010، وغيرها من المجموعات كمجموعة "جيش إيران الإلكتروني" الذي يحسب على الحرث الثوري.

لماذا يعدّ الفضاء الإلكتروني مغريًا لإيران؟

من الواضح أن هذه القدرات الهجوميّة هي جزء من إستراتيجية البلاد في خوض حروب غير متوازية، أو لا تناظرية مثل تكتيكاتها الأخرى ضمن هذه الإستراتيجية، والتي تتضمن توظيف حرب العصابات والعمليات الإرهابية التي تستخدم من قبل إيران بفعالية كبيرة جدًا ضد الخصوم الأكثر تقدمًا منها على الصعيد العسكري والتكنولوجي.

وفي هذا الإطار، يعدّ المجال الإلكتروني مغريًا جدًا لإيران ولغيرها من الدول خاصّة تلك التي تضع الحروب اللاتناظرية في صلب عقيدتها القتالية نظرًا لعدم تمتّعها بالتفوق العسكري التقليدي أو التكنولوجي، أو حتى لكلفة هذه الخيارات في كثير من الأحيان مقارنة بما يمكن تحقيقه في المجال الإلكتروني، حيث يمكننا تعداد أربعة أسباب رئيسة، هي:

حروب الإنترنت هي حروب لا تناظرية (Asymmetric): فالتكلفة المتدنية نسبيًا للأدوات اللازمة لشن هكذا حروب يعني أنّه ليس هناك حاجة لدولة ما مثلاً أن تقوم بتصنيع أسلحة مكلفة جدًا كحاملات الطائرات والمقاتلات المتطورة لتفرض تهديدًا خطيرًا وحقيقيًا على دولة مثل الولايات المتّحدة الأمريكية على سبيل المثال.

تمتّع المهاجم بأفضلية واضحة: في حروب الإنترنت يتمتع المهاجم بأفضلية واضحة وكبيرة على المدافع، فهذه الحروب تتميز بالسرعة والمرونة والمراوغة. وفي بيئة مماثلة يتمتّع بها المهاجم بأفضليّة،

من الصعب جدًا على عقليّة الدفاع والتحصّن لوحدها أن تنجح. فالتحصين بهذا المعنى سيجعل من هذا الطرف عرضة لمزيد من محاولات الاختراق، وبالتالي المزيد من الضغط. كما أنّ هناك صعوبة في تحديد مصدر الهجوم إذا لم يعلن المهاجم عن نفسه.

فشل نماذج "الردع" المعروفة: يعد مفهوم الردع الذي تمّ تطبيقه بشكل أساسي في الحرب الباردة غير ذي جدوى في حروب الإنترنت. فالردع بالانتقام أو العقاب لا ينطبق على سبيل المثال على هذه الحروب. فعلى عكس الحروب التقليدية، حيث ينطلق الصاروخ من أماكن يتم رصدها والرد عليها، فإنه من الصعوبة بمكان -بل ومن المستحيل في كثير من الأحيان- تحديد الهجمات الإلكترونية ذات الزخم العالي. بعض الحالات قد تتطلّب أشهرًا لرصدها، وهو ما يلغي مفعول الردع بالانتقام وكثير من الحالات لا يمكن تتبع مصدرها في المقابل، وحتى إذا تم تتبع مصدرها وتبين أنها تعود لفاعلين غير حكوميين، فإنه في هذه الحالة لن يكون لديهم أصول أو قواعد حتى يتم الرد عليها.

المخاطر تتعدى استهداف المواقع العسكرية: لا ينحصر إطار حروب الإنترنت باستهداف المواقع العسكرية، فهناك جهود متزايدة لاستهداف البنى التحتية المدنية والحسّاسة في البلدان المستهدفة، وهو أمر أصبح واقعيًّا في ظل القدرة على استهداف شبكات الكهرباء والطاقة، وشبكات النقل والنظام المالي، والمنشآت الحساسة النفطية أو المائية أو الصناعية، بواسطة فيروس يمكنه إحداث أضرار ماديّة حقيقية تؤدي إلى انفجارات أو دمار هائل، أو تعطيل كامل، وهو ما يعني المزيد من الخسائر بأقل قدرة ممكنة من التكاليف عند الطرف المهاجم.

نقلاً عن مجلة المجلة.

رابط المقال: https://www.noonpost.com/1435/