التوتر الأمريكي الإيراني.. هل نشهد حربًا إلكترونية ضروسًا؟

كتبه مجد أبو ريا | 11 يناير ,2020

دُشّن العام 2020 بتفجير قنبلة قلبت وسائل الإعلام رأسًا على عقب، بعد مقتل قائد فيلق القدس الإيراني الجنرال قاسم سليماني والرجل الثاني في إيران في 3 من هذا الشهر، ما بين مؤيد ومعارض في أوساط الرأي العالمي، لكن الأهم من ذلك هي التكهنات بشأن الرد الإيراني.

انتشرت الأحاديث عن حدوث حرب عالمية ثالثة، ومع صباح اليوم الـ3 من يناير/كانون الثاني، اعتلى وسم #WWIII قوائم الوسوم الأكثر تداولًا في الولايات المتحدة قبل أن يقفز سريعًا ليكون من بين الأكثر تداولًا عالميًا.

لكن أبرز ما يتوقعه المتخصصون بشأن الرد الإيراني هي احتمالية شن إيران "هجمات إلكترونية" ضد شركات ومصالح الولايات المتحدة، خصوصًا أن لدى الطرفين تاريخ في هذا النوع من الهجمات، بل وكثير من هؤلاء المتخصصين أكدوا أن الحرب الإلكترونية تمثل أقوى سلاح إيراني في مواجهة أمريكا.

قد لا يدرك البعض خطورة هذه الأنواع من الحروب وتاريخها بين الدول العظمى، التي يمكن تصنيفها كحرب النجوم في السبعينيات من القرن الماضي، وهنا نلقي نظرة على مفهوم وتاريخ الحرب الإلكترونية.

الحرب السيبرانية (Cyber warfare)

هو صراع تكون شبكة الإنترنت فيه هي الميدان، يتمحور حول هجمات ذات دوافع سياسية على المعلومات ونظمها، حيث يمكنها تعطيل مواقع الويب الرسمية والشبكات وتعطيل الخدمات الأساسية أو سرقة وتعديل البيانات السرية وتخريب الأنظمة المالية، وذلك من بين العديد من الاحتمالات المتعددة.

> هي الحرب التي لن ترى أسلحتها ولن تسمع لها صوتًا ولن تشم رائحة البارود المحترق

يصفها أحد الضباط الأمريكيين المتخصصين في الحرب الإلكترونية والأسلحة غير الميتة، بأنها الحرب التي لن ترى أسلحتها ولن تسمع لها صوتًا ولن تشم رائحة البارود المحترق، لكن إذا نجح العدو في استهدافك، ستحرق طائراته كل شيء، كما يقول الكاتب البريطاني جفري كار في كتابه "داخل الحرب الإلكترونية": "بإمكان أي دولة شن حرب إلكترونية على دولة أخرى بغض النظر عن مواردها، وذلك لأن معظم القوات العسكرية ترتبط بشبكات حاسوبية وتتصل بالإنترنت، ولذلك فهي ليست آمنة، وللسبب ذاته بإمكان الجماعات غير الحكومية وحتى الأفراد شن هجمات حرب إلكترونية".

تاريخ الحرب الإلكترونية وصراع الدول

بدأت أول الحروب الإلكترونية المتواضعة عام 1904 في أثناء الحرب بين روسيا والإمبراطورية اليابانية باستخدام الراديو أو الإشارات اللاسلكية من القوات البحرية في الجيشين، تطورت الأساليب خلال الحرب العالمية الأولى عندما نجح البريطانيون في القيام بعمليات تجسس إلكترونية عالية، نجحت في فك جميع الشفيرات الحربية الألمانية الدقيقة والسرية، كذلك قام الألمان بعمليات مضادة.

وصلت الحرب الإلكترونية إلى مرحلة جديدة في بدايات الحرب العالمية الثانية، عن طريق إدخال تقنيات الرادار لتوجيه الهجمات الإلكترونية، وكانت أشهر معركة تنصت هي تلك التي خاضتها بريطانيا تجاه قائد البارجة الألمانية "بسمارك"، من خلال زرع أجهزة تنصت في إيرلندا تمكن خلالها البريطانيون من الاستماع عن بعد لكل التقارير التي يرفعها القائد الألماني إلى القيادة الألمانية العامة.

وبعد ظهور الثورة التكنولوجية في المعلومات والاتصالات في بداية الثمانينيات، أصبحت هذه الحرب أكثر تعقيدًا وخطورةً، وأصبحت تصنف تحت مفهوم "حرب الاستنزاف"، ويقول الباحثون إن حادثة وقعت عام 1983 كانت نقطة فاصلة في تاريخ هذه الحرب وكذلك في تطور ترسانة الولايات المتحدة للحرب الإلكترونية التي استخدمتها بشكل فاعل في حرب الخليج عام 1991 ثم في صربيا في أواسط التسعينيات وقبل ذلك ضد الاتحاد السوفياتي السابق في سنين الحرب الباردة.

توالت المعارك الإلكترونية بعد ذلك التاريخ، فخلال عام 1995 تعرضت حواسيب وزارة الدفاع الأمريكية إلى 250.000 هجمة، كذلك تعرضت المواقع الفيدرالية للتشويه والاختراق، وكذلك الهجوم الذي يعتقد أن مصدره روسيا واستهدف إستونيا سنة 2007 وأدى إلى تعطيل كل مواقع الويب الحكومية والخاصة ووسائل الإعلام عبر البلاد، والكثير الكثير من المعارك.

هناك سباق بين الدول الغنية لتطوير برمجيات تهدف إلى امتلاك قدرات هجومية وأخرى دفاعية قادرة على التصدي لأي هجمات مشابهة

أما الآن، فهناك سباق بين الدول الغنية لتطوير برمجيات تهدف إلى امتلاك قدرات هجومية وأخرى دفاعية قادرة على التصدي لأي هجمات مشابهة من هذا القبيل، فالولايات المتحدة تبذل جهودًا كبيرة لتطوير أنظمة دفاع تحمي شبكاتها من القراصنة والهجمات المدمرة من جانب حكومات أجنبية، خاصة الصين وروسيا وإيران، كما أنها تسعى للحصول على قدرات هجومية إلكترونية تمكنها من تعطيل شبكات الحاسوب لدى العدو.

وتفيد دراسة لمركز الدراسات الإستراتيجية والدولية CSIS بأن 15 دولة في العالم -وهي الدول التي تمتلك الميزانيات العسكرية الأضخم- تستثمر في مجالات متخصصة من أجل الحصول على قدرات هجومية إلكترونية عن طريق الإنترنت، ودمج القدرات الإلكترونية في عملياتها العسكرية، وبحسب صحيفة واشنطن بوست، فإن الجيش الأمريكي وبقية الجيوش في العالم ترى في البرمجيات التخريبية أداةً أساسية جديدة من أدوات الحرب الإلكترونية.

الحرب الإلكترونية بين الولايات المتحدة وإيران

إن طبيعة هذه الحروب تكون عادة غير علنية، وينتشر خبرها فيما بعد نظرًا لحساسية الموقف، وقد بدأت المعارك بين الطرفين منذ 10 سنوات، ففي عام 2010 أُصيبت أجهزة الطرد المركزي الإيرانية في محطة تخصيب اليورانيوم في مفاعل نطنز بفعل دودة كمبيوتر خبيثة تسمى "ستاكس نت" أعدتها المخابرات الأمريكية والإسرائيلية، وفقًا لتقارير عدة.

وقد تم الكشف عن ستاكس نت لأول مرة عام 2010 وأدت إلى تأخير في عمل المفاعل والتخصيب لمدة لا تقل عن السنتين ونتيجة لذلك خلفت خسائر كبيرة لإيران وإعاقة في البرنامج النووي لديها، وبعدها أدى ذلك لتكثيف إيران قدراتها على الحرب الإلكترونية، وتطورت بشكل ملحوظ في العقد الماضي.

كما كشف اختصاصيون في الأمن المعلوماتي أن إيران تقف وراء هجمات إلكترونية تتعرض لها مؤسسات مالية أمريكية، وذلك ردًا على العقوبات الدولية التي تستهدف الحكومة الإيرانية، وقد أُعلن للمرة الأولى عن هذه الاعتداءات في سبتمبر 2012، حسب شركة "رادوير" المتخصصة بالأمن المعلوماتي.

في حين استهدفت الهجمات الإلكترونية الإيرانية القطاع الخاص في معظم ضرباتها، ففي عام 2014، اختُرقت أنظمة فندق وكازينو ساندس هوتيل، وسرقت ودمرت البيانات، الأمر الذي كلف الكازينو 40 مليون دولار على الأقل، وبين عامي 2011 و2013، اتُهم سبعة إيرانيين يعملون لصالح الحكومة الإيرانية بشن هجمات على وزارة الدفاع وعلى 46 شركة، معظمها من المؤسسات المالية، وفقًا لقرار اتهام من وزارة العدل الأمريكية لعام 2016.

وفي الآونة الأخيرة، شنت أمريكا العديد من الهجمات الإلكترونية الخاصة بها على إيران، منذ يونيو حتى ديسمبر الماضي، وكان ذلك بشكل دفاعي، ودعا المسؤولون والوكالات الحكومية الأمريكيين إلى اتخاذ الاحتياطات الأمنية، وذلك بعد تحذير وكالة الأمن السيبراني وأمن البنى التحتية التابعة لوزارة الأمن الداخلي الأمريكية من أن هناك "ارتفاعًا في النشاط السيبراني الضار الموجه نحو صناعات الولايات المتحدة والوكالات الحكومية من ممثلي النظام الإيراني ووكلائه".

حرب إلكترونية علنية

أشار تقرير نشرته صحيفة "كونفيدنسيال" الإسبانية إلى إمكانية حدوث نزاع أمريكي إيراني، ترجح فيه أن حظوظ الولايات المتحدة في الانتصار كبيرة، ويتحدث عن حاملة الطائرات الأمريكية والحرب الإلكترونية والمقاتلة "إف-35" ضمن الترسانة الأمريكية المتقدمة، وذلك بعد أن بلغت الاستفزازات أشدها بين الطرفين.

توضح الصحيفة أن الميزة الكبرى لصالح الولايات المتحدة في خضم هذا التوتر لا تكمن في قوتها العسكرية المفرطة، بقدر ما تتجلى في قدراتها الاستخباراتية، وفي شنّ حرب إلكترونية، وتعد الاستخبارات المفتاح، حيث يُحتمل أن يكون الأمريكيون على علم بكل مكان وموقع له صلة بكل أهدافهم ذات الأولوية، وأما ما لا يمكنهم معرفته، فسيُخبرهم به حلفاؤهم الإسرائيليون الذين لديهم إمكانات تفوق نوعًا ما الاستخبارات الأمريكية.

أما شركة "فاير آي" المتخصصة في الأمن الإلكتروني، فترى أن إيران ستنفذ هجمات إلكترونية "قرصنة" ضد شركات ومصالح الولايات المتحدة، التي بدورها قد تستهدف قطاعات البنية التحتية الحيوية وقطاعات النفط والغاز في منطقة الشرق الأوسط والولايات المتحدة، لتتحول بعدها إلى حرب إلكترونية معلنة، وهذا سلاح إيران الفعال.

وقد حذر خبراء الأمن السيبراني الأمريكي من ردة فعل إيران على مقتل الجنرال قاسم سليماني، وشدد خبراء على ضرورة استعداد الولايات المتحدة لاحتمال هجمات إلكترونية إيرانية جريئة تهدف إلى إلحاق أضرار مالية كبيرة أو تهديد أرواح الأمريكيين كرد انتقامي.

وقد نشرت صحيفة واشنطن بوست أن إيران قد تكون على استعداد لتخطي الحدود في الفضاء الإلكتروني، فعلى سبيل المثال، يحذر الخبراء من أن المتسللين الإيرانيين قد يشنون هجمات تقطع طاقة الكهرباء أو تدمر سجلات مالية مهمة أو تعطل أنظمة المستشفيات أو النقل بطرق تهدد الأرواح.

وقال جون هولتكويست مدير تحليل الاستخبارات في شركة فاير آي للأمن السيبراني: "نحن في وضع أكثر تصعيدًا مما كنا عليه في الماضي، وهناك بعض الأسئلة الخطيرة عما إذا كان هناك خطوط حمراء"، مضيفًا أن الإيرانيين لا يواجهون مشكلة في إصابة الأشخاص خلال هذه المرحلة.

ويحذر الخبراء أيضًا من أن إيران قد تشن هجمات واسعة النطاق ضد الشركات الأمريكية التي تشفر معلوماتها وتحتفظ بها للحصول على فدية، أو تستهدف المقاولين الحكوميين الأمريكيين

لعاقبتهم على العمل مع البيت الأبيض أو ربما تستهدف طهران حلفاء الولايات المتحدة في الشرق الأوسط أو أهدافًا دبلوماسية أمريكية في الخارج.

فيما يرى خبراء أن إيران اختبرت بشكل روتيني حدود ما يمكن أن تفلت منه في الفضاء الإلكتروني، بما في ذلك تدمير البنوك الأمريكية بعد أن فرضت إدارة أوباما عقوبات جديدة عام 2012، واختراق أنظمة التحكم بسد في نيويورك عام 2013.

وبالنسبة إلى استعداد أمريكا لمواجهة هجمات إيران الإلكترونية، فيرى الخبراء الأميركان أن الولايات المتحدة غير مستعدة، وهم نفسهم الذين حذروا منذ سنوات من أن إيران ستكثف هجماتها الإلكترونية على أمريكا بشكل متكرر وشديد، خاصة منذ انتخاب الرئيس دونالد ترامب، وهو معارض قوي للغاية للنظام الإيراني، وقد سحب الولايات المتحدة من اتفاقها النووي مع إيران.

فيما يعتقد بعض الخبراء أن إيران قد ترغب في تأخير أي هجمات إلكترونية ضارة حتى يتضح إلى أي مدى سيتصاعد النزاع، وهذا أمر محتمل، لأن معظم الهجمات الإلكترونية الضارة جدًا تتطلب شهورًا من العمل المسبق لاقتحام شبكات الحاسوب الخاصة بجهة ما بشكل مفاجئ.

جيك وليامز، مؤسس شركة الأمن السيبراني رينديشن إنفوسيك ومسؤول سابق في وكالة الأمن القومي، يرى أن "إيران ستستخدم بكل تأكيد كل ما لديها، لكنني لا أعتقد أن هناك هجومًا إلكترونيًا كبيرًا في هذه المرحلة.. كل قطعة من البرمجيات الخبيثة التي تستخدمها إيران الآن يمكن أن تتحول لرصاصة يمكنها إطلاقها لاحقًا ليكون لها تأثير أكبر".

رابط المقال : https://www.noonpost.com/35543/