العرب
الأربعاء 2021/05/26
السنة 43 العدد 12070

الهجمات الإلكترونية في الغرب: الجميع منازلهم من زجاج

ترجيح الميل الهجومي على الدفاعي يخلّ بالتوازن العالمي

أثارت الموجة الأخيرة من القرصنة المعلوماتية وطلبات الفدية انطلاقا من روسيا قلق الدول الغربية التي باتت عرضة لهجمات إلكترونية مربكة تضع أمنها الرقمي في خطر. وفيما تشير غالبية من الخبراء إلى أن التصعيد الأخير للقراصنة و الهجمات الإلكترونية المتزايدة يعريان مكامن الضعف لدى أقوى أجهزة الاستخبارات في العالم، فإن آخرين يحذرون من أن السلاح الإلكتروني سيزيد من حدة المنافسة والنزاع بين القوى الدولية، حيث أن ترجيح الميل الهجومي على الميل الدفاعي يضع التوازن العالمي على شفا الاختلال.

الأمن الرقمي لأقوى دول العالم في خطر

باريس - سلّطت سلسلة من الهجمات الإلكترونية في الدول الغربية الضوء على مكامن الضعف لدى الشركات والهيئات الحكومية، وعلى الرهان الذي يشكله مجال يصعب التحكم به في العقود المقبلة.

وأصدر الرئيس الأميركي جو بايدن قبل فترة قصيرة مرسوما عاجلا يطلب من الإدارات تعزيز الأمن الرقمي بعد سلسلة من الهجمات المقلقة.

فإلى جانب عملية القرصنة التي استهدفت نهاية 2020 شركة سولاروينذز لتصميم برمجيات الإدارة المعلوماتية، شهدت الولايات المتحدة الدولة الأولى عالميا في الفضاء الافتراضي قبل فترة قصيرة شللا تاما أصاب شركة "كولونيال بايبلاين" المشغلة لخطوط أنابيب رئيسية في البلاد.

إلا أن الولايات المتحدة ليست الوحيدة المعرضة لهذه الهجمات. فالمملكة المتحدة تطالب بتحالف دولي ضد الهجمات الإلكترونية، متهمة روسيا والصين وإيران وكوريا الشمالية بالوقوف وراءها. ورأت وزيرة الجيوش الفرنسية فلورانس بارلي أخيرا أن الهجمات التي تعرضت لها فرنسا زادت أربع مرات في غضون سنة.

لكن ما مرد هذا الضعف؟ هنا تجيب سوزان سبولدينغ من مركز الدراسات الإستراتيجية والدولية في واشنطن بالقول "لقد شهدنا عددا كافيا من الهجمات الإلكترونية لكي يدرك الجميع خطورة وأهمية" هذه المسألة.

وتضيف "لم تعطَ هذه المسألة أولوية كافية" مشيرة في الوقت نفسه إلى أنه من الصعب إقناع أصحاب القرار بضرورة الاستثمار لاتقاء تهديد محتمل. وتشير إلى مقولة باتت مستخدمة كثيرا في صفوف المحللين ومفادها "أن ثمة نوعين من الشركات في العالم: تلك التي تعرضت للقرصنة وتلك التي لم تدرك الأمر بعد".

مواجهة كامنة

في المقابل، بات هذا الإدراك قويا في صفوف الجيوش. فقد استحدثت كل القوى العظمى قيادة للهجمات الإلكترونية. ويقول جوليان نوسيتي الباحث في معهد البحث الرقمي في جامعة باريس 8 "منذ العقد الأخير بات ذلك ضمن مجموعة الأدوات المتوافرة للجيوش وأجهزة الاستخبارات في إطار مواجهة ليست بالضرورة مفتوحة إلا أنها كامنة".

ويضيف "الفضاء الإلكتروني هو في آن عملي جدا وغامض جدا لأنه يسمح بإزالة الحدود نوعا ما بين العالم المدني والعالم العسكري وبين إطار الحرب وإطار السلم وبين الدول والمجموعات التي تشكل شبه دول والقطاع الخاص".


آدم سيغال
ليس مستبعدا أن يؤدي هجوم تقليدي إلى الرد بهجوم إلكتروني

وفي العقد الأخير حصلت انعطافة في الإدراك الغربي مع التدخلات في الانتخابات الأميركية والهجوم في مقابل فدية نوتبيتيا الذي نسب إلى روسيا والبرمجية الخبيثة "واناكراي". ودفع ذلك الغربيين إلى تعزيز دفاعاتهم وتطوير أساليب الهجوم.

ويرى جوليان نوسيتي "تصنف أوروبا والولايات المتحدة أحيانا كثيرة على أنهما ضحية وأنهما الأخيار في هذه المسألة.. لكنهما لا تكتفيان بالدفاع. فثمة نقص في التحاليل حول عملياتنا"، مشيرا إلى أن "الموضوع يعتبر من المحرمات نوعا ما بسبب الرابط الوثيق مع الاستخبارات".

ورغم إسراع الدول الغربية إلى توجيه أصابع الاتهام إلى المتشبه فيهم المعتادين أي موسكو وبكين وبيونغ يانغ وطهران، لا يمكن لأحد أن يملي دروسا على الآخر. فقد دخل الفضاء الإلكتروني إلى كل أجهزة الاستخبارات. ويقول مسؤول فرنسي رفيع المستوى طلب عدم الكشف عن اسمه "الأمر أشبه بالوضع الذي كان قائما في الغرب الأميركي: فلا أصدقاء لك فيه وكل الضربات مشروعة".

لكن، هل كل الضربات مسموحة؟ هذا هو السؤال المطروح. وفي هذا الإطار اجتمع فريق من الخبراء الحكوميين من 25 دولة مرات عدة في العقد الأخير في إطار الأمم المتحدة في محاولة لتحديد الخطوط الحمر.

نزاع مفتوح

حسب الخبراء فالجميع يمارس التجسس. لكن سوزان سبولدينغ تؤكد وجود "نشاطات مسؤولة وأخرى غير مسؤولة". وتشير مساعدة وزير الأمن الداخلي الأميركية السابقة إلى روسيا موضحة "لا يمكن قطع التيار الكهربائي عن أوكرانيا في نهاية فصل الشتاء. هذا غير مقبول".

هذه المفاوضات متوقفة راهنا فيما لا يبشر ترجيح الميل الهجومي على الميل الدفاعي بالخير على صعيد التوازن العالمي.

ويقول فاديم كوزيولين الباحث في الأكاديمية الدبلوماسية في موسكو في تصريحات صحافية "نعيش في منزل من زجاج. على جميع الدول أن تتذكر أننا جميعا مترابطون. فالنزاع المفتوح سيكون مدمرا ليس فقط للعدو بل للمهاجم أيضا"، آملا في أن يصبح المجال الإلكتروني سلاح ردع فقط.

أما آدم سيغال مدير البرنامج الرقمي والفضاء الإلكتروني في مجلس العلاقات الخارجية وهو مؤسسة بحث أميركية، فيشير إلى أن قلة من الدول قادرة على تصميم برمجية شبيهة بـ"ستاكسنت" وهو فايروس نسب إلى الأميركيين والإسرائيليين أدى في العام 2010 إلى سلسلة من الأعطال في مجمع إيراني لأجهزة الطرد المركزي التي تستخدم في تخصيب اليورانيوم.

ويشير إلى أن السلاح الإلكتروني "ليس من أسلحة الدمار الشامل" إلا إنه يبقى سلاحا ولم يعد أي طرف يستبعد أن يؤدي هجوم تقليدي إلى الرد بهجوم إلكتروني. وسيغال مقتنع بذلك موضحا أن "أحد أسباب عدم تبادل الولايات المتحدة وروسيا والصين قطع الكهرباء في بلدانهم، هو الخوف من ردة الفعل".

الاستراتيجية الروسية للأمن الإلكتروني: قرصنة، تضليل فإنكار

موسكو - على مرّ السنوات واجهت موسكو الكثير من المزاعم التي تفيد بتنفيذها هجمات إلكترونية أدت إلى عقوبات مختلفة وطرد لدبلوماسييها. وأصبح مصطلح "قرصنة" مرادفا لروسيا.

ومن "مزارع المتصيّدين" إلى المقرصنين الذين يزعم أنهم يخضعون لسيطرة الأجهزة الأمنية في البلاد، تطورت جرائم الإنترنت الروسي.

وكانت روسيا لعقود أرضا خصبة لخبراء المعلوماتية. فخلال الحقبة السوفييتية، دفعت الحكومة من أجل إحراز تقدم في مجال العلوم والتكنولوجيا، وفي البرمجة، مع ظهور أجهزة الكمبيوتر الأولى.

ومع سقوط الاتحاد السوفييتي في العام 1991، تحول بعض المبرمجين الموهوبين الذين كانوا يتقاضون أجورا منخفضة، إلى الجريمة الإلكترونية وسرعان ما أصبح الروس مشهورين بسرقة بطاقات الائتمان في كل أنحاء العالم.

وأوضح كيفين ليمونييه من معهد "انستيتو فرانسي دو جيوبوليتيك"، أنه "في التسعينات سادت ثقافة التحايل على القواعد".

ويقول خبراء إنه في مواجهتها المستمرة مع الغرب، تعتمد روسيا بشدة على قدراتها في مجال الحرب الإلكترونية والمعلوماتية.

ويشتبه في أن الكثير من مجموعات القرصنة الأكثر شهرة تعمل لصالح الأجهزة الأمنية في البلاد، وقد أنشأت وزارة الدفاع الروسية "وحدات إلكترونية" خاصة بها العام 2012.

ويعود أول هجوم واسع النطاق منسوب إلى روسيا إلى العام 2007 عندما واجهت إستونيا موجة من الهجمات الإلكترونية طالت صحفا ومصارف ووزارات.

وتقول الولايات المتحدة إن قراصنة مديرية الاستخبارات العسكرية الروسية سعوا إلى التلاعب بالانتخابات الرئاسية الأميركية للعام 2016 من خلال اختراق اللجنة الوطنية للحزب الديمقراطي وحملة هيلاري كلينتون.

ومجموعة التجسس الإلكتروني الأكثر شهرة والتي تنسب إليها العشرات من الحالات تعرف باسم "فانسي بير" أو "ابت 28"، ويعتقد أنها تعمل تحت رعاية الحكومة الروسية.

وبحسب واشنطن، فإن الهجوم الذي استهدف الشركة الأميركية لتطوير البرمجيات "سولار ويندز"، نفذتها خدمة الاستخبارات الخارجية الروسية وعرّضت وكالات حكومية أميركية والمئات من الشركات الخاصة للخطر.

وأكدت وكالة الاستخبارات الألمانية في العام 2016، أن "الهجمات الإلكترونية التي تنفذها أجهزة الاستخبارات الروسية هي جزء من عمليات دولية على مدى سنوات تهدف إلى الحصول على معلومات استراتيجية"، في إشارة إلى عمليات تجسس وتخريب.


أندريه سولداتوف
الهجمات الإلكترونية الروسية تتزايد مقارنة بالسنوات الأخيرة

وتطول قائمة الهجمات الروسية المزعومة: قرصنة البرلمان الألماني العام 2015 واستهداف وحدات المدفعية الأوكرانية بين العامين 2014 و2016 واختراق شبكة تلفزيون فرنسية العام 2015 وتدخل في الانتخابات الرئاسية الأميركية في 2016 و2020 واستهداف معاهد بحوث للقاحات مضادة لفايروس كورونا العام 2020.

ويشير خبراء إلى أن الهجمات الإلكترونية أصبحت أكثر تعقيدا من أي وقت مضى.

وأشار الخبير الروسي في أجهزة الاستخبارات أندريه سولداتوف إلى أن "الهجمات الإلكترونية الروسية تتزايد مقارنة بما كانت عليه الحال قبل ثلاث أو أربع سنوات".

وقال "نعلم عن العمليات التي أمكن كشفها، لكن ثمة الكثير من العمليات المستمرة".

واتهمت روسيا أيضا بشن حملات تضليل واسعة النطاق من أجل التأثير على العمليات الديمقراطية في الغرب وتأجيج الخلافات الاجتماعية عبر الإنترنت.

ويعتقد أن البلاد تدير "مزارع متصيّدين" على الإنترنت تختلق معلومات مزيفة وتنشرها على نطاق واسع في محاولة للتأثير على مستخدمي الإنترنت.

ووجّهت اتهامات إلى كل من وسائل الإعلام الحكومية، بما فيها "روسيا اليوم" (آر تي)، وحلفاء الكرملين مثل يفغيني بريغوزين، وهو رجل أعمال يشتبه في أنه وراء "مزارع المتصيّدين" في روسيا وأفريقيا.

واشنطن تعمل في الظل لمواجهة الغزوات الجريئة للقراصنة الروس والصينيين

واشنطن - ترد الولايات المتحدة بنشاط على الهجمات الإلكترونية التي تطالها، إلا أنها تعمل بسرية تامة ما قد يظهرها في موقع ضعف في وجه غزوات قراصنة روس وصينيين تزداد جرأة.

ولفتت تغريدة أخيرة لكتيبة 780 في سلاح البر الأميركي الانتباه. فقد أعادت وحدة المقاتلين في الفضاء الإلكتروني هذه بث إعلان لشركة الأمن الإلكتروني "ريكورديد فيوتشر" تؤكد تعطيل خوادم قراصنة المعلوماتية "دارك سايد".


إليسا سلوتكين
علينا التواصل مع الشعب الأميركي ليدرك أننا لسنا ضعفاء

ولا يعرف أحد من سيطر على "دارك سايد" وهي منظمة مقرها في روسيا تقف وراء الهجوم الإلكتروني على شركة "كولونيال بايبلاين" الأميركية المشغلة لخطوط أنابيب رئيسية في البلاد.

شكلت هذه التغريدة رسالة إلى قراصنة المعلوماتية في محاولة لثنيهم عن شن هجمات مماثلة، مع أن محللين يعتبرون أن الردع غير موجود في الفضاء الإلكتروني.

ويقول جون لينداساي الخبير في الأمن الإلكتروني في جامعة تورنتو في تصريحات صحافية "الردع هو القيام بالتهديد. وقد يكون له جانب عقابي، لكن من يتعرض للعقاب؟ الوضع غامض جدا". ومن شبه المستحيل تحديد من يقف وراء الهجوم بالتأكيد.

وسمع الجمهور العريض للمرة الأولى بهجوم إلكتروني أميركي في العام 2010 عندما شل الفايروس "ستاكسنت" الذي نسب بشكل واسع إلى إسرائيل والولايات المتحدة من دون أي إعلان مسؤولية، مجمع لأجهزة طرد مركزي تستخدمها طهران لتخصيب اليورانيوم.

لكن منذ ذلك الحين تعرضت الكثير من الهيئات والشركات الأميركية لهجمات قراصنة صينيين سرقوا قواعد بيانات وأسرارًا صناعية، وروس تدخلوا في الانتخابات وكوريين شماليين سرقوا بتكوين، فضلا عن قراصنة معلوماتية اختلسوا الملايين من الدولارات من شركات وسلطات محلية ومستشفيات.

وأمام هذه الهجمات لزمت وزارة الدفاع الأميركية الصمت وأعطت الانطباع بأنها لا تبذل أي جهد للرد.

إلا أن الجنرال بول ناكاسون الذي يشرف على وكالة الاستخبارات العسكرية (وكالة الأمن القومي) والقيادة الأميركية للفضاء الإلكتروني (سايبركوم) أكد قبل فترة قصيرة أن هذا الانطباع غير صحيح.

وقال أمام لجنة في الكونغرس "عندما نرى أطرافا ينشطون من الخارج نحاول أن نجعلهم يدفعون أغلى الأثمان إن كان ذلك عبر الكشف عن هوياتهم علنا أو تشارك المعلومات مع مجموعة من الحلفاء أو عندما نحصل على الإذن لشن عمليات ضدهم".

لكنه رفض إعطاء أمثلة محددة عن هجمات مضادة.

إلا أن النائبة عن ميشيغان إليسا سلوتكين المحللة السابقة في وكالة الاستخبارات المركزية الأميركية "سي. آي.أي" تقول إن "الانطباع المهيمن هو أن الردع مفقود وأن مجموعة صينية أو روسية يمكنها أن تهاجمنا من دون عقاب".

وتضيف "يجب إيجاد طريقة لعدم الاكتفاء بالعمل في الظل والتواصل مع الشعب الأميركي ليدرك أننا لسنا ضعفاء".

وفي السنتين الأخيرتين كشف الجيش الأميركي وإن بتقتير عن بعض نشاطاته في الفضاء الإلكتروني.

وأكد مسؤولون أميركيون لم يكشفوا عن هوياتهم في يونيو 2019 أن هجوما إلكترونيا أمر به البيت الأبيض عطل أنظمة إطلاق صواريخ إيرانية.

وفي يناير 2020 كشفت قيادة "سايبركوم" أنها شوشت "بنجاح" الدعاية الإلكترونية لتنظيم الدولة الإسلامية خلال عملية نفذت اعتبارا من العام 2016.

ويكمن السبب الرئيسي وراء حذر البنتاغون في صعوبة نسب هجوم ما بالتأكيد إلى حكومة أخرى أو جماعة إجرامية على ما توضح إليزابيث بودين – بارون من مركز "راند" للأبحاث.

وقد يكون للكشف عن عمليات البنتاغون تأثير رادع إلا أنه سيف ذو حدين كذلك على ما تنبه المحللة.

وتضيف "البعض يقول إنه في حال لم نعط أمثلة عن الأماكن التي اخترقناها أو ما قمنا به، لن يصدقنا أحد"، لكن إذا تم التأكد من هوية الطرف الذي يقف وراء الهجوم فإن تسميته علنا "قد تكشف بعض الأمور عن قدراتنا الخاصة".

ويفيد جون لينداساي أن إستراتيجية الفضاء الإلكتروني تغيرت منذ "ستاكسنت".

ويوضح "في تلك الفترة كان الهجوم الإلكتروني يعتبر بمثابة سلاح دمار شامل" قادر على معاقبة خصم أو تهديده، مضيفا "كانت عملية سرية رفيعة المستوى تحت إشراف رئاسي" تشن لأغراض إستراتيجية.

أما اليوم فبات الفضاء الإلكتروني مسرح قتال مثل أي مسرح آخر يخضع لإشراف وثيق من السلطة التنفيذية حيث الأوامر الصادرة تنص على "القتال المتواصل" على ما يؤكد لينداساي. والحرب السرية التي تشن في الفضاء الإلكتروني بمثابة تجسس متطور وخفي.

الولايات المتحدة: تعرض أكبر مشغل لخطوط أنابيب النفط لهجوم إلكتروني