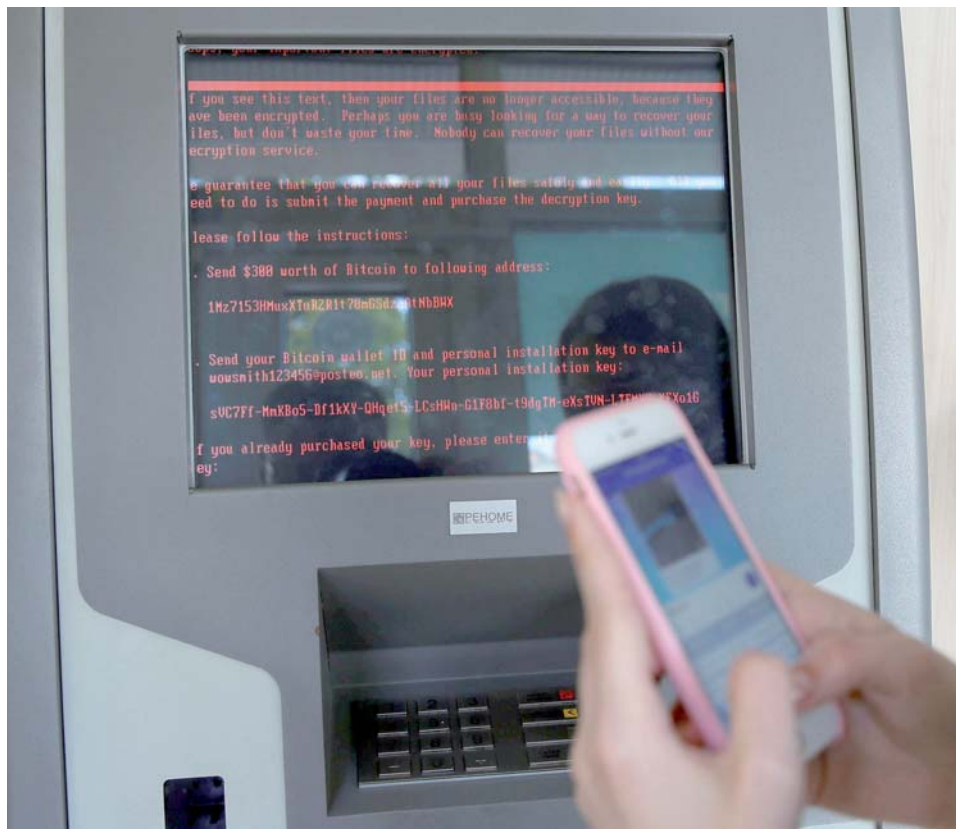
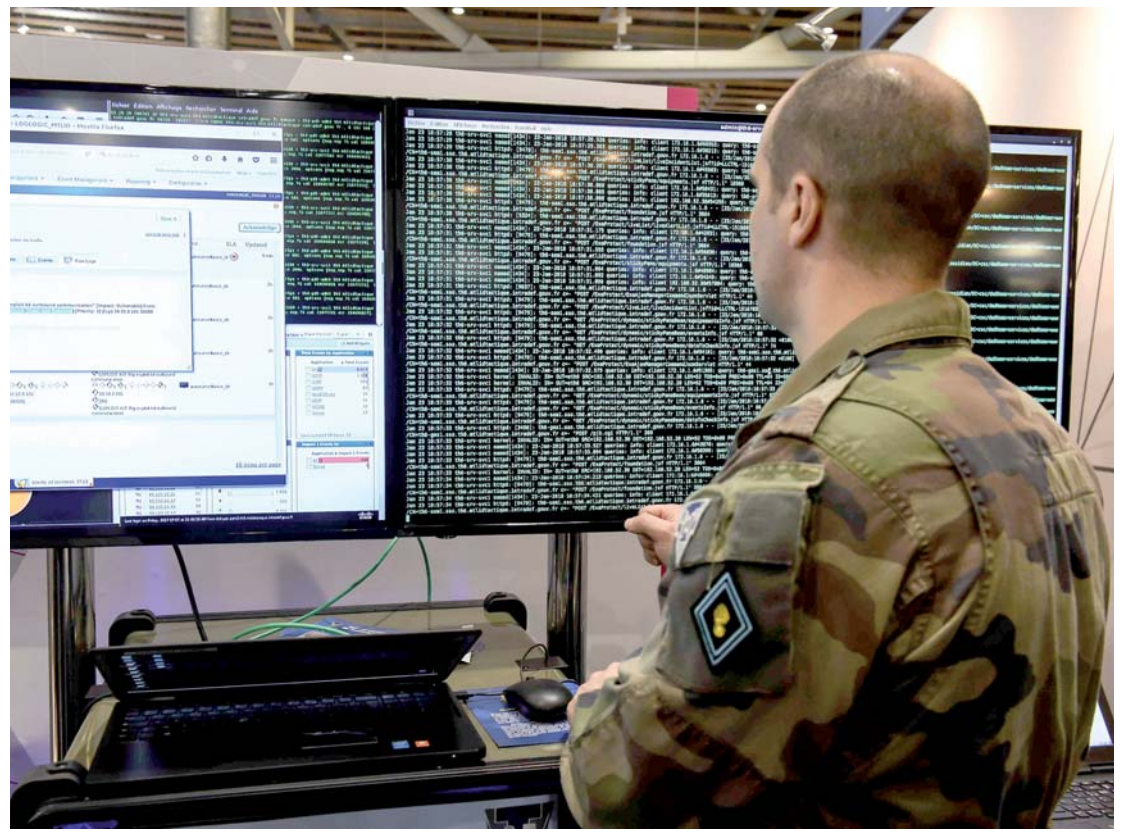
العرب
الأربعاء 2019/08/07
السنة 42 العدد 11431

لا رابح ولا خاسر في سباق التسلح المعلوماتي

القدرة التدميرية للفيروسات الإلكترونية قد تتفوق على الأسلحة النووية



هجوم بأقل كلفة وأكثر نجاعة



الخوارزميات قادرة على بدء الحرب وأيضا على إنهائها

دخل العالم منذ ربع قرن تقريبا في سباق تسلح جديد أقل كلفة وأكثر نجاعة في إصابة الأهداف بكل دقة، تاركا الترسانات العسكرية التقليدية باهظة الكلفة وغير مضمونة النتائج في مخازنها. ومع سرعة تدفق الإنترنت والبيانات حول العالم، بات الفضاء الافتراضي قاعدة لانطلاق هجمات سيبرانية، قد تكون مدمرة في بعض الأحيان، ضد قواعد وبيانات الخصم، ما يشلّ حركته ويهدد أمنه. وتسعى الدول إلى تطوير مناعتها الدفاعية ضد الهجمات الإلكترونية تماما مثلما تفعل مع ترسانتها الصاروخية، إلا أن السباق باتجاه ذلك لا ينتهي، فبمجرد ابتكار مضاد دفاعي إلكتروني يستنبط الخصم وسائل هجوم جديدة غير معروفة وهكذا دواليك لا رابح ولا خاسر في سباق التسلح المضني.

واشنطن - حذّر تقرير حكومي من أن أنظمة التسلّح الأميركية تعاني من هشاشة أمام هجمات قد يشنّها قراصنة معلوماتيون، في ضعف عزاه إلى تخلّف البنتاغون في مجال الأمان المعلوماتي والصعوبات التي يواجهها في توظيف اختصاصيين في هذا المجال.

وجاء في هذا التقرير الذي حمل عنوان "وزارة الدفاع بدأت للتوّ بإدراك مدى نقاط الضعف"، وأعدّه مكتب التدقيق الحكومي الأميركي الموازي لديوان المحاسبة، أنّ التجهيزات العسكرية الأميركية باتت متّصلة أكثر فأكثر بالإنترنت فالطائرات المقاتلة مليئة بالبرامج والأجهزة اللاقطة والقيادة العملانية تتمّ على شاشة عملاقة، تحديد مواقع الجنود على الأرض يتمّ عبر نظام تحديد المواقع الجغرافية (جي.بي.أس)، والسفن الحربية باتت ممكنة أكثر فأكثر.

ينس ستولتنبرغ

الفضاء الإلكتروني سيصبح جزءا من الصراع العسكري

وهذه البرامج والأجهزة اللاقطة تجعل العسكريين أكثر قوة، لكنهم سيكونون أكثر ضعفا أمام هجمات قرصنة معلوماتية محتملة. وقام اختصاصيون في البنتاغون بلعب دور قراصنة معلوماتيين بين عامي 2012 و2017 وتمكنّوا من اختراق وقرصنة أنظمة التسلّح الأميركية بسهولة.

وجاء في التقرير الصادر في أكتوبر 2018 أيضا "في إحدى الحالات لم يكن فريق مؤلف من شخصين بحاجة لأكثر من ساعة لاختراق النظام المعلوماتي لنظام تسلّح، وليوم واحد للسيطرة الكاملة على آلية تشغيله".

وأوضح أن البنتاغون بدأ يعي خطورة الوضع وضرورة ضمان حماية أفضل للأنظمة المعلوماتية، إلا أنه يجد صعوبة في توظيف خبراء حيث يفضّل هؤلاء العمل في القطاع الخاص باعتبار أن المرتبات أفضل منها في الجيش.

وفي الوقت الذين يتّهم فيه الغرب روسيا بشنّ هجمات قرصنة معلوماتية عدة خلال الأشهر الماضية، تواصل حكوماتهم الكفاح من أجل التصدّي لهذه الهجمات دون نتائج تذكر، فالهجمات تتكرر بطرق أخرى، وأساليب جديدة ما يضعهم أمام تحدي تطوير دفاعاتهم في كل لحظة.

وقال وزير الدفاع الروسي سيرجي شويغو إن الجيش الروسي شكّل قوة مكلفة بحرب المعلومات في خطوة من شأنها تأجيج مخاوف الغرب مما تعتبره "أخبارا كاذبة" تطلق برعاية موسكو. ويرى المخططون العسكريون الروس مثل نظرائهم في أي مكان آخر أن الدعاية جزء حيوي من الحروب الحديثة، ويخضع نشاط روسيا في هذا المجال لتدقيق مكثّف بعد أن اتهمت أجهزة مخابرات أميركية الكرملين بشنّ "عملية للتأثير" تستهدف مساعدة دونالد ترامب على الفوز في انتخابات الرئاسة في نوفمبر 2016.

وقالت أجهزة مخابرات أوروبية كذلك إن موسكو تسعى إلى زعزعة استقرار حكومات والتأثير على انتخابات في أوروبا بهجمات على الإنترنت وإطلاق أخبار كاذبة.

ويشكل الردع مفهوما أساسيا في أي سباق تسلّح، فالهدف هو أن تجعل عدوك يعلم قدراتك ومهاراتك حتى لا يفكر أساسا في بدء أي هجوم أو الدخول في أي حرب. ولكن حتى الآن لم نر هذا السلوك في سباق التسلح المعلوماتي وحروب الفضاء الإلكتروني، حيث كل التطورات والأبحاث في هذا المجال سرية وغير مسموح بالاطلاع عليها. ومع مرور الوقت، ستتاح هذه الأسرار للعموم كما في أي تقنيه دفاعيه وعسكرية أخرى، وربما يتطور الموضوع لنرى برامج لنزع السلاح وتخفيض القرات في هذا المجال.

ويعتبر تطوير تقنيات دفاعية ضد فيروسات الكمبيوتر تحديًا حقيقيًا لصناعة أمن المعلومات، خصوصا أن هذه الصناعة ليست موزعة على جميع أنحاء العالم، ولكنّها مقتصرة على عدد محدود من الدول.

فيروس الفدية

وفقا للخبراء في الأمن الإلكتروني يتضح من السابق أن العالم مقبل على حرب إلكترونية يشترك فيها الأفراد وليست فقط حكرا على الدول والحكومات. وأعلت هذه الحروب من شأن الأفراد في استخدام أدوات وتكنولوجيا الاتصال الحديثة على كافة الأصعدة وتبين للدول والحكومات أن شرًا مسيطرا يأتي تجاههم عن طريق تلك الأدوات التي قاموا بتطويرها وتعهدوها بالرعاية، إلى أن دخلوا في مرحلة مواجهة لن تنتهي بأي حال على المدى القريب.

في الواقع، إن الأسلحة الإلكترونية مماثلة للأسلحة النووية والأسلحة الكيميائية والتي يمكن أن تسبّب أضرارا خطيرة للبنية التحتية العالمية والإنتاج والحياة الطبيعية للبلدان. والتطوّر الهائل للأسلحة الإلكترونية من قبل الجيشين الأميركي والروسي، إضافة إلى الصين يؤدي إلى سباق تسلح إلكتروني يهدّد بشكل مباشر الأمن الإلكتروني العالمي.

واتهمت حكومات غربية عام 2017 الجيش الروسي بشنّ هجوم إلكتروني مدمر على دولة أوكرانيا وعدد من الدول الغربية، حيث تضرّرت شركات عالمية كبرى جرّاء الهجوم المعلوماتي، ومن بين هذه الشركات المجموعة العملاقة لصناعة الأدوية "ميرك" وشركة الإعلانات البريطانية "دبليو.بي.بي" والشركة الصناعية الفرنسية "سان غوبان".

ووصل فيروس الفدية "رانسوموير" إلى الآلاف من الكمبيوترات في العالم وتسبّب باضطرابات في عدد كبير من الشركات المتعددة الجنسيات والهياكل الأساسية الحساسة، مثل أجهزة التحكم بموقع كارثة تشيرنوبيل النووية ومرافئ بومباي وأمستردام.

وفي أوكرانيا الدولة الأكثر تضرّرا بالهجوم، تأثرت المعاملات المصرفية وتحدثت السلطات عن هجوم غير مسبوق، فيما ندّدت لندن مرات عدة بأنشطة روسيا المعادية.

وسرعان ما انتشر فيروس "نوتبيتيا"، الذي يشبه عائلة "بيتيا" لفيروسات الكمبيوتر، في أنحاء العالم. وأصاب هذا الفيروس أجهزة الكمبيوتر بالشلل، ثم طلب دفع مبلغ من العملة الرقمية "بيتكوين" لإزالة العوائق المعرقلة.

وتصدّرت فيروسات الفدية عناوين القصص الأمنية لهذا العام، ومن المرجّح أن تواصل تصدرها لأحداث الأعوام القادمة. لكن دافع القراصنة سيتحول تدريجيا من الابتزاز من أجل الأموال إلى الدخول في حرب بين دول، والشيء السيء هنا أن هذا النوع من البرمجيات الخبيثة قد يخرج عن السيطرة، ويضرب بشكل عشوائي ليتحوّل من عملية استهداف لأجهزة حكومية إلى نوع من القصف العشوائي لأجهزة المدنيين.

وستواصل الحكومات والسياسيون علاقة الحب والكراهية مع التشفير، يريدون لهذه الحيلة أن تكون في أقوى شكل ممكن عندما يتعلق الأمر بأسرارهم، بينما يرغبون في أن تكون بأضعف أشكالها لدى أي شخص آخر. ومع هذه الحقيقة سيكون التشفير سيد الموقف في جميع الحالات.

> التجهيزات العسكرية الأميركية باتت متّصلة أكثر فأكثر بالإنترنت فتحديد مواقع الجنود على الأرض مثلا يتمّ عبر نظام تحديد المواقع الجغرافية وهذه البرامج والأجهزة اللاقطة تجعل العسكريين أكثر قوة، لكنهم سيكونون أكثر ضعفا أمام هجمات قرصنة معلوماتية محتملة

الدوران في حلقة مفرغة

من مميّزات سباق تسلح أنه في النهاية كثيرا ما يكون المشاركون فيه في المكان الذي انطلقوا منه بالضبط، فأحيانا يمسك الفهد الصياد بفريسته وأحيانا أخرى يفلت الغزال، وهكذا لا أحد منهما يفوز بالسباق لأنه عند تحسن أحد الأطراف يتحسن خصمه أيضا. وعلى طول الطريق يستهلك كل طرف الكثير من الجهد. ومع ذلك وفي كل مرحلة الشيء الوحيد المعقول هو مواصلة التصعيد.

يمكن أن نسمّي ذلك سباق تسلّح معلوماتي، حيث يحاول أحد الطرفين تضليل العموم بخصوص مسألة أساسية (مثل سلامة دواء ما أو ما إذا كان التغيّر المناخي حقيقيا أو ما إذا كانت اللقاحات خطرة). وفي الوقت نفسه يعمل الطرف الآخر على محاربة هذه الحملة لتقديم المعلومات المضللة.

ومثلما أوضح تقرير روبرت مولر المكلّف بالتحقيق في شبهة التدخل الروسي في الانتخابات الأميركية لسنة 2016، قامت الحكومة الروسية بواسطة مجموعة تسمّى "وكالة البحث على الإنترنت" بجهود على نطاق واسع للتأثير على الناخبين واستقطاب الجماهير الأميركية. وفي أعقاب هذه الحملة تزاحمت مواقع الإعلام الاجتماعي ومجموعات البحث لحماية الجماهير الأميركية ضد التضليل الإعلامي على المواقع الاجتماعية.

واستخدم تويتر خوارزميات تهدف إلى تحديد البوتات وغلق الحسابات المشبوهة، حيث قام بالتخلص من مليون حساب مشابه في اليوم، لكن عندما يصبح تويتر أذكى كذلك تزداد البوتات ذكاء.

ولاحظ تقرير صدر مؤخرا وجود شبكة بوتات جديدة على موقع تويتر مصمّم خصيصا للتفوق على خوارزميات الاستشعار. ومن ضمن التوجّهات الجديدة نجد فاعلين خبثاء يقرصنون حسابات حقيقية.

والشيء المهمّ الذي يجب أن نعترف به حول مثل هذه الوضعية هو مهما كانت التكتيكات التي تنجح الآن فهي لن تعمل لوقت طويل. والسبب وراء ذلك هو أن الطرف الآخر سيتأقلم.

ولا يمكن أن نتوقّع بأننا سنكون قادرين على وضع مجموعة من خوارزميات الاستشعار في مكانها وننتهي من الأمر، فمهما كانت الجهود التي تبذلها مواقع الإعلام الاجتماعي للقضاء على الفاعلين الخبثاء ستصبح عديمة الفائدة في النهاية.

إن الوضع لمُنذر بالخطر نظرا إلى أن الإدارة الأميركية الحالية تتخذ موقف "لا أرى ضررا" تجاه التضليل الإعلامي على الإنترنت، متجاهلة المناشدات التي صدرت عن وزير الأمن الداخلي (المستقيل حاليا) كريستيان نيلسون للانتباه للجهود الروسية التي تزداد تطوّرا لتوجيه السياسة الأميركية.

> سباق التسلح الإلكتروني بين الجيوش الأميركية والروسية والصينية يهدد بشكل مباشر الأمن الإلكتروني العالمي

وبحسب الأمين العام لمنظمة حلف شمال الأطلسي، ينس ستولتنبرغ، فإن "في أي صراع عسكري، سيصبح الفضاء الإلكتروني جزءا من ساحة المعركة".

ولا شك أن هناك أسلحة سيبرانية متطوّرة للغاية تم تطويرها ونشرها ضد أهداف محددة ذات قيمة عالية للغاية، على الرغم من أننا قد لا نسمع عنها، لكن استخدام المزيد من الأسلحة والتقنيات السيبرانية سيصبح أمرا شائعا.

ولا يوجد أي مجال آخر أمام شركات الطاقة والتكنولوجيا والوكالات الحكومية سوى تطوير أدواتها، لأنّ القراصنة المدعومين من دول أخرى يعكفون على دراسة أنظمة هذه الجهات من أجل اختراقها ونشر الفوضى في وقت ما. ويتطلب ذلك الاستعداد لحرب إلكترونية تطال البنى التحتية لتعطيلها، والتسبب في تداعيات كانت سابقا تحدث نتيجة القصف الجوي.

كما رأينا التقدّم المذهل في مجال الأبحاث العسكرية خلال الـ50 عاما الماضية، فسنشهد طفرة ونقلة نوعية جديدة تتركز على أمن وحماية المعلومات وحروب الفضاء الإلكتروني والإنترنت، ربما لم نشاهد أي حرب معلوماتية حقيقية حتى الآن لأنه لم يحدث أي صدام أو حرب بين الدول التي تملك قدرات متقدمة في هذا المجال، ولكن من المؤكد أنه ستكون هناك حرب معلوماتية في الفضاء الإلكتروني في أي أزمة أو صراع مستقبلي.