لماذا تحتاج الولايات المتحدة إلى تطوير أنظمتها الفضائية؟

ترجمة وتحرير نون بوست

في سبتمبر عام 2014، استطاع هاكرز (قراصنة إنترنت) من الصين اختراق شبكة الإدارة الوطنية للمحيطات والغلاف الجوي في الولايات المتحدة (NOAA)، وذلك في محاولة منهم لتعطيل البيانات المتعلقة بالتخطيط لمواجهة الكوارث والطيران، وأي معلومات أخرى يمكن الحصول عليها من الأقمار الصناعية الأمريكية؛ وكان هذا الخرق هو الأحدث في سلسلة الهجمات الإلكترونية على الأنظمة الفضائية التي تستهدف نقاط الضعف في أجهزة الكمبيوتر والمعلومات التي تستحدثها هذه الأجهزة وتنقلها، وقد أصبحت هذه الهجمات الإلكترونية التي بدأت تتزايد في جميع المجالات الصناعية، تشكّل تهديدًا كبيرًا لاسيّما على النظم الفضائية التي يتم استخدامها على نطاق واسع في جميع العمليات التجارية والعسكرية؛ مما يجعلها أهدافًا مغرية بالنسبة للقراصنة.

على الرغم من أن البلدان القادرة على إطلاق الأقمار الصناعية إلى الفضاء لا تتجاوز العشر دول، إلّا أن مليارات الأشخاص في جميع أنحاء العالم يعتمدون على النظم الفضائية في مختلف جوانب حياتهم العصرية تقريبًا؛ حيث تقوم الأقمار الصناعية بتوفير الدعم للهواتف الذكية والإنترنت والنظم المصرفية، كما أنها تُستخدم لمراقبة حركة المرور البرية والبحرية والجوية، ولتسهيل عمليات الاتصالات العالمية، وهي تساهم في نقل الأخبار الإعلامية بشكل فوري، وتساعد على مراقبة التغيّرات المناخية أو التهديدات الجوية القاسية والكوارث الطبيعية التي يمكن أن تحدث على الأرض، فضلاً عن استخدام الأقمار الصناعية في جمع المعلومات الاستخباراتية وإرسال الإنذارات المبكرة عن إطلاق الصواريخ الباليستية؛ لذلك لا عجب بأن يكون الاقتصاد العالمي يعتمد على الأقمار الصناعية والاتصالات وأنظمة الملاحة لرصد الأرض.

الخدمات الفضائية فريسة سهلة لقراصنة الإنترنت:

البنية التحتية للخدمات الفضائية تتكون من 1.200 قمرًا صناعيًا يدورون حاليًا حول مدار الأرض، وفي حال تمت مهاجمة هذه الأقمار الصناعية، فإن هذا سيتسبب بحدوث أضرار كبيرة وملموسة في الأنظمة الفضائية الوطنية أو العالمية على مستوى جميع البلدان والقارات، فحتى الأخطاء الصغيرة التي يمكن أن تُصيب هذه الأنظمة يمكن أن تتسبب بحدوث مشاكل كبيرة؛ فمثلاً، في أبريل من عام 2014، حدث عطل في نظام جلوناس (Glonass)، وهو نظام روسي يشابه نظام تحديد المواقع الأمريكي الـ (GPS)، وكان العطل راجعًا لحدوث خطأين رياضيين صغيرين في البرنامج؛ أي أنه لم ينجم عن عمليات قرصنة، وعلى الرغم من بساطة الأخطاء إلا أن إصلاح النظام استغرق أكثر من 13 ساعة عمل؛ وتسبب هذا العطل الذي لم يدم سوى نصف يوم بحدوث اضطرابات شديدة في استقبال الجلوناس؛ مما أثّر على مستخدمي جهاز الأيفون 5 (iPhone5)؛ بناء عليه فمن السهل أن نخمّن أن النظم الفضائية هي الحلقة الأضعف التي يمكن من خلالها تنفيذ جميع الجرائم الإلكترونية، فاختراقها لا يتطلب الكثير من الجهد ونتائج الاختراق تحدث آثارًا بالغة التأثير، وبذلك يمكن للمخترقين إلحاق أضرار أكبر بالأهداف التي يسعون لاختراقها.

يتكوّن النظام الفضائي أساسًا من ثلاثة قطاعات مترابطة: الأولى هي الأقمار الصناعية والمركبات الفضائية التي تدور حول الأرض، والثانية هي المحطات الأرضية، والثالثة تتمثل بأنظمة الاتصالات التي تشكّل صلة الوصل ما بين القطاعين السابقين؛ ولا يحتاج قراصنة الإنترنت إلا للعثور على نقاط الضعف في أحد هذه القطاعات، فعلى سبيل المثال، يمكن لأي شخص أن يضحّي ببضع مئات من الدولارات، لشراء جهاز تشويش صغير يتم وصله على الإنترنت ليستطيع التدخل في الإشارات الصادرة عن الأقمار الصناعية، لذلك يحذّر العقيد برادفورد باركنسون، الذي ترأس إنشاء نظام الـ (GPS) بقوله "يجب علينا جعل أنظمة الملاحة عبر الأقمار الصناعية أكثر قوة"، ويضيف "إن أبراج الهاتف المحمول متزامنة مع نظام الـ (GPS)، وإذا فقد هذا التزامن؛ فستتوقف الأبراج عن العمل بعد وقت قصير، وهذه الأخطار قد تشمل الشبكة الكهربائية المتزامنة أيضًا مع نظام الـ (GPS) وأيضًا الأنظمة المصرفية".

من الواضح أن النظم الفضائية كانت هدفًا للقرصنة في أكثر من مناسبة، ففي يوليو من عام 2013، تمكّنت الولايات المتحدة من تحديد هوية المواطن البريطاني الذي يبلغ من العمر 28 عامًا والذي استطاع اختراق عدد من الشبكات الحكومية بما في ذلك وكالة ناسا، وحاول الاستيلاء على بيانات حساسة للغاية، وادّعى أنه كان سيستخدمها في بعض المواقف الهزلية، وبعد ذلك بأربعة أشهر، في نوفمبر من عام 2013، أُصيبت أجهزة الكمبيوتر التي تستخدم في محطة الفضاء الدولية بفيروسات، ولم تقتصر هجمات القرصنة على الولايات المتحدة الأمريكية كون وكالة الفضاء اليابانية اكتشفت أيضًا وجود بعض الفيروسات داخل عدد قليل من أجهزة الكمبيوتر لديها في يناير من عام 2012، كما وعانى مركز الفضاء الألماني مؤخرًا من هجوم تجسسي، حيث تمت قرصنة العديد من أجهزة الكمبيوتر لديه ببرامج تجسسية، كما أن إذاعة (BBC) عانت منذ عام 2009 من وجود اختلالات في برامجها الإذاعية والتلفزيونية الناطقة باللغة الفارسية، ووجهت أصابع الاتهام في هذه الاختلالات إلى طهران التي اتُهمت بالتشويش على البث الفضائي الدولي الذي يبث إلى إيران، ولم تتوقف هذه الهجمات إلا بعد قيام الاتحاد الأوروبي بتقديم شكوى دبلوماسية للضغط على إيران للتوقف والكف عن أفعالها، وكذلك الأمر عندما قامت كوريا الشمالية بتشويش إشارات الـ (GPS) التابعة لكوريا الجنوبية في أبريل 2012؛ مما أدى إلى التشويش على أكثر من 250 رحلة جوية، والقائمة بهذه العمليات تطول.

أحد أهم الأسباب التي تجعل من أنظمة الفضاء، وخاصة التجارية منها، فريسة سهلة لقراصنة الإنترنت، هي أنها غالبًا ما تستعمل برامج عفا عليها الزمن؛ حيث إن عملية تطوير النظم الفضائية تستلزم عدة سنوات وذلك تبعًا لمدى تعقيد النظام، وبمجرد أن يصبح النظام جاهزًا للعمل، يستمر العمل لعدة

سنوات على الأقل، وأحيانًا حتى أكثر من عقد من الزمان؛ لذا فإن عملية تحديث البرمجيات الأمنية للأنظمة الفضائية هي عملية غير متداولة، وعلاوة على ذلك، ففي كثير من الحالات، فإن نظم المعلومات التي يتم استخدامها لإدارة النظم الفضائية تستند في معظمها على برمجيات تجارية جاهزة، وهذه البرمجيات تتميز بانخفاض مستويات الأمان وتضم العديد من نقاط الضعف، خاصة عندما تتم مقارنتها بالنظم العسكرية المتطورة.

في عام 2014، قامت بعض المؤسسات الفكرية، من مجلس العلاقات الخارجية في تشاتام هاوس في لندن، إضافة إلى شركة المعلومات الأمنية (IOActive)، بدق ناقوس الخطر عن طريق إجراء دراسة أشاروا فيها إلى مدى ضعف النظم الفضائية بمواجهة الهجمات الإلكترونية، حيث حذّر تقريرهم من سهولة اختراق النظم الفضائية عن طريق استخدام طرق ثانوية في مجال البرمجيات، أو عن طريق البرمجيات الغير مؤمنة، أو البروتوكولات غير المحمية والقنوات غير المشفرة؛ وقدمت الدراسة بعض التوصيات التي تتضمن اتباع إجراء فوري يشمل إزالة جميع تحديثات البرامج من المواقع الإلكترونية العامة للعديد من الشركات التي تقدم خدمات ومعدات خاصة بالأقمار الصناعية، وذلك من أجل منع قراصنة الإنترنت من إجراء هندسة عكسية لشفرة المصدر، ولكن على الرغم من هذه التحذيرات، فإن الصناعات الفضائية مازالت تتجاهل هذه المخاطر وماتزال ردودها بطيئة تجاه إيجاد الحلول لها، وهنا يكمن التحدي، حيث إنه لا بد من وضع معايير وقوانين لتنظيم نشاط الشركات متعددة الجنسيات والجهات التجارية التي تعمل في مجال تكنولوجيا الفضاء.

المضي قدمًا باتجاه الحلول:

في العام الماضي، بدأت العديد من الدول التي ترتاد الفضاء بمعالجة نقاط الضعف الكامنة في أنظمتها الفضائية؛ فقبل ثلاثة أشهر، أعلن سلاح الجو الأمريكي بأنه يأمل في تطوير تقنيات جديدة من شأنها أن تمنع قراصنة الإنترنت من التشويش على الأقمار الصناعية التابعة للجيش، كما تعتزم روسيا إحداث تحديثات كبيرة في قوة وأمن النظام العسكري والحكومي لاتصالاتها عبر الأقمار الصناعية بحلول عام 2025.

ولكن على الرغم من هذه الخطوات الإيجابية التي اتخذتها بعض الدول، فإنه يتوجب على الحكومات الوطنية والهيئات الدولية تغطية المزيد من حالات القصور الأمني التي تعتري الأنظمة الفضائية، حيث يتعين عليها أولاً أن تزيد من جهودها لرفع مستوى الوعي بشأن التهديدات المتزايدة الناجمة عن الهجمات الإلكترونية والمتخذة ضد النظم الفضائية التجارية والحكومية، وثانيًا يتوجب على الحكومات والشركات أن تتبع نهج حماية شامل لحماية القطاعات الفضائية بدلاً من استخدام النهج التدريجي، حيث يتوجب أن يتم توجيه الحلول نحو اتخاذ إجراءات شاملة تضمن حسن أداء جميع النظم وخدماتها، بدلاً من حماية نظام واحد محدد بذاته، فعلى سبيل المثال، إذا افترضنا بأن الأقمار الصناعية ستتعرض باستمرار لأضرار جرّاء الهجمات الإلكترونية التي تستهدفها، فإن الإجراء المتخذ يجب أن يشمل إعادة تصميم الأنظمة الفضائية لتعمل بشكل سلس ومتكامل، ولتستطيع تفادي الأخطاء بسرعة، وهذه الإجراءات هي أكثر أهمية من ضمان أمن وسلامة قمر صناعي واحد فقط.

من جهة ثالثة يجب على الجهات الفاعلة مدنيًا وعسكريًا وتجاريًا في مجال صناعة الفضاء، إجراء المزيد من المناقشات بهدف تعزيز الحماية الشاملة، حيث يمكن الوصول إلى تطبيق هذه الحماية عن طريق تبادل المعلومات والعمل المشترك لإصدار معايير وقوانين تنظّم العمل في مجال تكنولوجيا الفضاء بشكل أفضل، أما الإجراء الرابع، فيشمل اتخاذ جهد حكومي ودولي لتوحيد بروتوكولات حماية النظم الفضائية، فعلى سبيل المثال، عندما تم اختراق شبكة الإدارة الوطنية للمحيطات والغلاف الجوي في الولايات المتحدة (NOAA) في سبتمبر، لم تعترف الإدارة بحصول الاختراق واقتصر الأمر على قيام

مشرف الشبكة، بانتقاد نقاط الضعف في أمن نظم المعلومات الفضائية، ولم تعترف الإدارة بوقوع هذا الاختراق إلا بعد شهر من حصوله، علمًا بأن إخفاء مثل هذه المعلومات يعوق المناقشة المجدية التي يجب أن تتخذ في الوقت المناسب حول هذه القضية، ويؤخّر أيضًا اتخاذ أية إجراءات أو تدابير وقائية كان من المفروض اتخاذها، وأن الاتفاق على إيجاد بروتوكول قياسي موحد قد يعمل على حل مثل هذه المشاكل، وأخيرًا، فإن حماية النظم الفضائية يجب أن تتخذ عن طريق جهد دولي موحد، حيث يتعين على الدول القادرة على ارتياد الفضاء أن تعمل سويًا لتحقيق تعاون دولي لتطبيق جميع الخطوات المذكورة أعلاه والمتمثلة برفع مستوى الوعي، وتبادل المعلومات، ووضع معايير موحدة.

أخيرًا، فإن الضرر الهائل الذي قد ينجم عن السهولة النسبية لإجراء هجوم إلكتروني على أنظمة الفضاء، يشكّل تهديدًا حقيقيًا مترصدًا بنا في كل لحظة، وهذا الخطر سيزداد في حال لم يقم مجتمع الفضاء الدولي بحشد الإرادة السياسية لمواجهة التحديات المتنامية للنظم الفضائية.

المصدر: فورين آفيرز