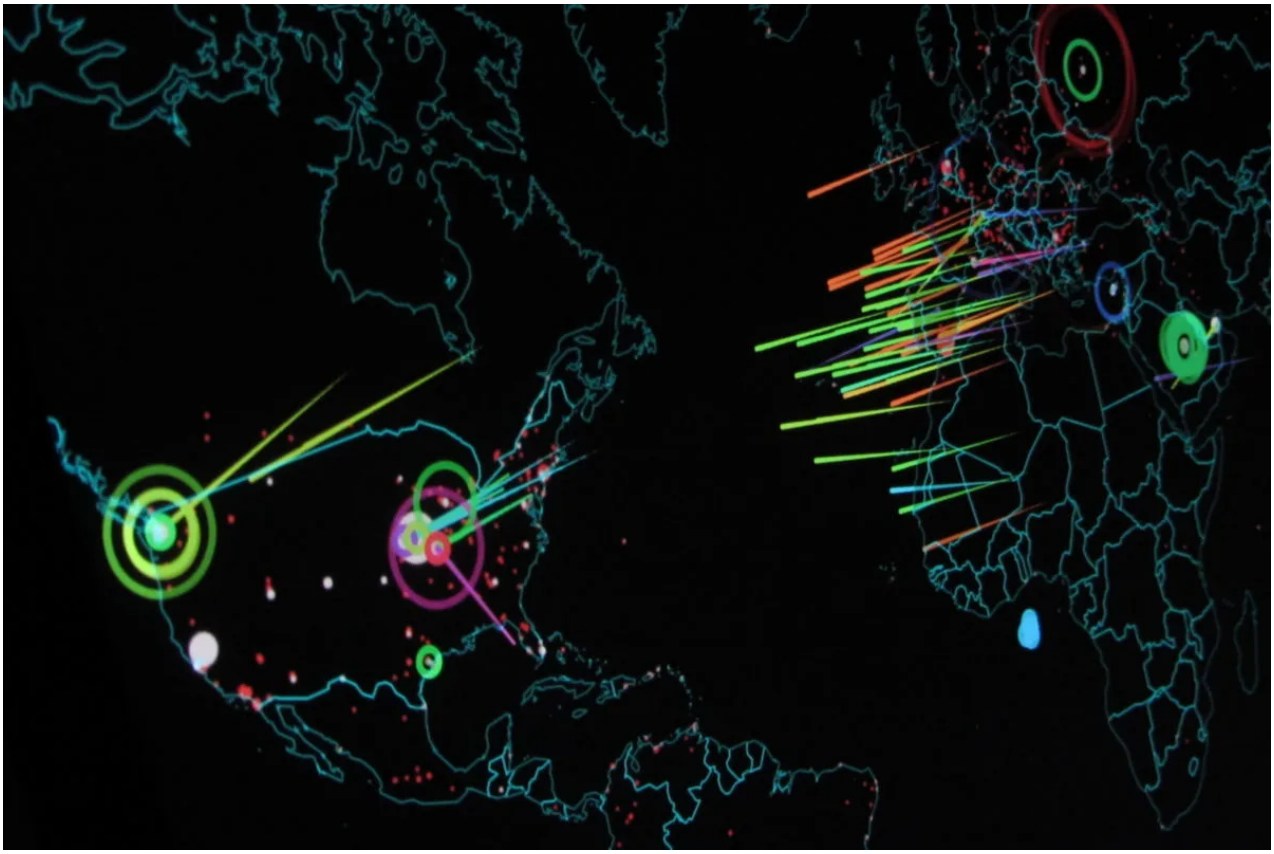
التهديد المباشر في المنطقة هو الحرب الإلكترونية لا الانتشار النووي



ترجمة وتحرير: نون بوست

على الرغم من أن انسحاب الولايات المتحدة بشكل أحادي من الاتفاق النووي الإيراني في سنة 2018 خلال إدارة دونالد ترامب، بدا أمرا سيئًا بالنسبة للجمهورية الإسلامية الخاضعة للعقوبات، إلا أنه منحها بشكل أساسي الفرصة للعودة إلى العمل على برنامج التطوير النووي الخاص بها، ولكن هذه المرة فقط بوثوقية أكثر.

في السنة الماضية، قررت إيران – التي أصبحت محبطة على نحو متزايد – زيادة اليورانيوم المخصب وتطوير أجهزة الطرد المركزي انتقامًا لانسحاب ترامب من الاتفاق وما أسفر عنه ذلك من تداعيات. كما هددت بمزيد تعزيز طموحاتها النووية الشهر الماضي عندما وافق البرلمان في طهران على مشروع قانون زيادة تخصيب اليورانيوم على أساس شهري. حتى أن وزارة الخارجية أعلنت عن عدم استعدادها لإعادة التفاوض على شروط الاتفاق مع إدارة بايدن في واشنطن. يبدو أن الأوان قد فات، فقد خانت الولايات المتحدة إيران بالفعل.

حددت المملكة العربية السعودية أيضًا طموحاتها النووية على مدى السنة الماضية، من خلال العمل على بناء منشأة لخام اليورانيوم بمساعدة من الصين. وعلى الرغم من أن هذا البرنامج، حسب ما تفيد به التقارير، يخدم أغراضا سلمية فقط، إلا أن ولي العهد السعودي محمد بن سلمان قال قبل سنتين إنه سيطور أسلحة نووية إذا قامت إيران بنفس الأمر.

بطبيعة الحال، أصبحت "إسرائيل" والولايات المتحدة أكثر قلقًا بشأن تصاعد التوتر في المنطقة. كانت إيران منذ فترة طويلة مصدر قلق بسبب طموحاتها وقيادتها لـ "محور المقاومة" ضد "إسرائيل"

والولايات المتحدة، لكن حتى السعودية الآن تشعر بالقلق من الحلفاء الصهاينة بسبب طموحاتهم الإقليمية المتجددة. وبالفعل، أعربت "إسرائيل" عن قلقها إزاء برنامج المملكة النووي. وحتى مع احتمال قيام الرياض بتطبيع العلاقات مع تل أبيب في المستقبل القريب، فإن المملكة العربية السعودية المسلحة نوويًا هي آخر ما تريد "إسرائيل" رؤيته.

مع ذلك، تظل السعودية في الوقت الحالي أقل أهمية من إيران، التي يُنظر إليها على أنها التهديد الرئيسي لدولة الاحتلال. لا تزال "إسرائيل" والولايات المتحدة ملتزمتين بتدمير طموحات إيران النووية أو الحد منها بشكل جدي، ومن هنا جاء اغتيال العالم النووي محسن فخري زاده في شوارع طهران الشهر الماضي، حيث وُجهت أصابع الاتهام للإسرائيليين.

إن الأساليب التقليدية لمنع تطور دولة منافسة، مثل التجسس والاغتيال، تشكل محور الاهتمام في الوقت الحالي. ولكن هناك أداة أكثر معاصرة تستخدم أيضا لإحباط جهود أي دولة للتفوق: ألا وهي الحرب الإلكترونية.

بفضل ويكيليكس، أصبحنا ندرك الآن أن أجهزة الاستخبارات الأمريكية والإسرائيلية أنشأت هذا الفيروس في إطار برنامج سري

يتمثل التطور الأكثر ثورية في هذا المجال في اختراع فيروس الكمبيوتر "ستوكسنت" منذ عقد من الزمان، القادر على استغلال الثغرات الموجودة في أنظمة الكمبيوتر المعروفة بنقاط الضعف التي لا تدوم يومًا بعد يوم واختراق هذه الثغرات. إن فيروس ستوكسنت متطور للغاية ولديه قدرات قرصنة إلكترونية لم تكن معروفة من قبل.

استهدف هذا الفيروس أجهزة الطرد المركزي الإيرانية التي كانت تستخدم في إنتاج اليورانيوم المخصب اللازم للأسلحة النووية، حيث جعلها تشتغل بسرعة أكبر لإفساد المعدات بينما كانت بيانات الكمبيوتر الرئيسي تشير إلى أن كل شيء على ما يرام. أدى هذا الهجوم إلى إرباك العلماء والسلطات الإيرانية، ولم يُجر التشخيص إلا بعد فوات الأوان ووقوع الضرر. في سنة 2010، اكتشف مجتمع الاستخبارات والأمن الإلكتروني ستوكسنت وأدرك أن نوعًا مختلفًا تمامًا من التهديد السيبراني قد ظهر.

بفضل ويكيليكس، أصبحنا ندرك الآن أن أجهزة الاستخبارات الأمريكية والإسرائيلية أنشأت هذا الفيروس في إطار برنامج سري أطلق عليه "عملية الألعاب الأولمبية". أطلق البرنامج في عهد إدارة الرئيس جورج دبليو بوش واستمر في عهد أوباما، كان الهدف منه استهداف طموحات إيران النووية وغيرها من التهديدات التي قد تبرز لاحقا.

لم تعترف واشنطن أو تل أبيب رسميًا بدورهما في تطوير ستوكسنت، بيد أن مقطع فيديو يحيي ذكرى تقاعد رئيس الأركان الإسرائيلي غابي أشكنازي في 2011 أدرج الفيروس ضمن أحد نجاحاته.

لم يكن هذا الفيروس الذي يصيب الحواسيب مجرد تهديد لبرنامج إيران النووي فحسب، بل كان يمتلك أيضًا القدرة على التسلل إلى البنية الأساسية للدولة وتعطيلها على نطاق أوسع. اتخذت الهجمات السيبرانية عدة أشكال، من بينها الهجمات التي طالت مواقع أوكرانية والتي تسبب أحدها في سنة 2015 في إخراج شبكة الكهرباء بنجاح عن السيطرة، وقد تبين أن من قام بذلك قراصنة روس.

كانت روسيا أيضًا الجاني المحتمل وراء هجوم طال مصنعًا للبتروكيماويات في المملكة العربية السعودية في سنة 2018، حيث قيل إن قراصنة الإنترنت كانوا على صلة بالبرامج الضارة المعروفة باسم "تريتون" التي تم استخدامها. ثم استخدمت الولايات المتحدة قدراتها السيبرانية لمهاجمة شبكة الكهرباء الروسية في العام الماضي، في رسالة واضحة إلى موسكو.

لا تزال واشنطن وتل أبيب تتمتعان بالتفوق في المجال السيبراني، ويحتاج العاملون على برنامج إيران

النووي المتجدد إلى أن يأخذوا بعين الاعتبار احتمال وقوع هجمات إلكترونية

ما تُظهره كل هذه الهجمات هو أن الحكومات أصبحت قادرة بشكل متزايد على إتلاف المعدات والبنية التحتية بطريقة تكون أكثر ضررًا للمدنيين، وذلك دون استعمال أسلحة تقليدية أو القنابل النووية.

حاليا، يوجد قلق حقيقي للغاية وهو أنه إذا كان ممكنا اختراق شبكة كهربائية ومنشأة كيميائية عن طريق مهاجمة نظام الكمبيوتر، فإن المواقع الأخرى ذات الأهمية المماثلة أو الأكبر يمكن أن تكون معرضة للخطر كذلك. كان هذا هو الحال في الشرق الأوسط خلال العام الماضي، مع زيادة وتيرة الصراع السيبراني بين "إسرائيل" وإيران.

في التاسع من أيار/ مايو، على سبيل المثال، تعرض ميناء الشهيد رجائي الإيراني على الخليج العربي لهجوم إلكتروني كبير أدى إلى توقف كل شحناته. ويبدو أن أجهزة الكمبيوتر التي تنظم حركة المرور في الميناء استُهدفت من قبل قراصنة إسرائيليين ردًا على محاولة إيران السابقة لاستهداف البنية التحتية للمياه في إسرائيل. كالعادة، ردت "إسرائيل" بطريقة أكثر تدميرًا.

في سنة 2005، أطلقت إيران "الجيش السيبراني" وزاد تمويله بشكل حاد على مر السنين. إنه يشكل تهديدًا أكبر لإسرائيل والولايات المتحدة على حد سواء، وقد يستمر في تشكيل مصدر تهديد.

لا تزال واشنطن وتل أبيب تتمتعان بالتفوق في المجال السيبراني، ويحتاج العاملون على برنامج إيران النووي المتجدد إلى أن يأخذوا بعين الاعتبار احتمال وقوع هجمات إلكترونية مماثلة لتلك التي حدثت في سنة 2010 أو للهجوم الذي شنته "إسرائيل" على منشأة نطنز النووية في وقت سابق من هذا العام، وهو الأمر الذي تحاول طهران الحد منه. يبدو أن الانتشار النووي في الشرق الأوسط يلوح في الأفق، لكن التهديد المباشر والأكثر خطورة هو الحرب الإلكترونية.

المصدر: ميدل إيست مونيتور

رابط المقال: https://www.noonpost.com/39203/