معايير دولية في الفضاء السيبراني

2015-05-20بروجيكت سنديكيت

جوزيف ناي

كمبريدج ــ في الشهر الماضي، استضافت هولندا المؤتمر العالمي للفضاء السيبراني لعام 2015، والذي جمع ما يقرب من الألفين من المسؤولين الحكوميين والأكاديميين وممثلي الصناعات، وغيرهم. وقد توليت رئاسة لجنة من الخبراء لمناقشة الفضاء السيبراني (الإلكتروني) والأمن، وقد ضمت اللجنة نائب رئيس شركة ميكروسوفت واثنين من الوزراء الأجانب. وكان هذا المؤتمر الذي ضم أطرافاً متعددة من أصحاب المصلحة هو الأحدث في سلسلة من الجهود الرامية إلى إرساء قواعد الطريق من أجل تجنب الصراع السيبراني.

إن القدرة على استخدام الإنترنت لإلحاق الضرر أصبحت الآن راسخة ثابتة. ويعتقد العديد من المراقبين أن الحكومتين الأميركية والإسرائيلية كانتا وراء الهجوم السابق الذي دمر أجهزة طرد مركزي في منشأة نووية إيرانية. ويقول البعض إن هجمة حكومية إيرانية دمرت الآلاف من أجهزة الكمبيوتر في أرامكو السعودية. وهناك من يتهم روسيا بشن هجمات "رفض الخدمة" على إستونيا وجورجيا. وفي ديسمبر/كانون الأول الماضي، عزا الرئيس الأميركي باراك أوباما الهجوم على شركة أفلام سوني إلى حكومة كوريا الشمالية.

حتى وقت قريب كان الأمن السيبراني حِكراً إلى حد كبير على مجموعة صغيرة من خبراء الكمبيوتر. عندما تم إنشاء شبكة الإنترنت في سبعينيات القرن العشرين، شَكَّلَ أعضاؤها قرية افتراضية؛ فكان الجميع يعرفون بعضهم البعض، ومعاً صمموا نظاماً مفتوحاً لم يكن يهتم بالأمن إلا قليلا.

ثم في أوائل التسعينيات، ظهرت الشبكة العنكبوتية العالمية، وتنامت من بضعة ملايين من المستخدمين آنذاك إلى أكثر من مليار مستخدم اليوم. وفي غضون ما يزيد على الجيل قليلا، أصبحت شبكة الإنترنت الركيزة الأساسية للاقتصاد العالمي والحوكمة في مختلف أنحاء العالم. وسوف يضاف عدة مليارات أخرى من المستخدمين في العقود التالية، فضلاً عن عشرات المليارات من الأجهزة، التي تتراوح بين منظمات الحرارة إلى أنظمة التحكم الصناعية ("إنترنت الأشياء").

وكل هذا الترابط المتعاظم يعني ضمناً نشوء نقاط الضعف التي تستطيع الحكومات أو الجهات الفاعلة غير الحكومية استغلالها. وفي الوقت نفسه، بدأنا للتو نتصالح مع العواقب المترتبة على ذلك في ما يتصل بالأمن الوطني. الواقع أن الدراسات الاستراتيجية للمجال السيبراني تشبه الاستراتيجية النووية في الخمسينيات: فالتحليلات لا تزال غير واضحة حول معنى الهجوم، والدفاع، والردع، والتصعيد، والمعاير، والحد من التسلح.

ويُستَخدَم مصطلح "الحرب السيبرانية" على نحو غير محكم على الإطلاق لوصف مجموعة واسعة من السلوكيات بدءاً من الاستطلاعات البسيطة وتشويه المواقع والحرمان من الخدمة إلى التجسس والتدمير. وهو في هذا يعكس تعريفات القواميس لكلمة "حرب"، والتي تشمل أي جهد منظم "لوقف أو إلحاق الهزيمة بشيء يُنظَر إليه باعتباره خطراً أو سيئا" (على سبيل المثال "الحرب على المخدرات".

والتعريف الأكثر نفعاً للحرب السيبرانية هو أي عمل عدائي في الفضاء الإلكتروني يضخم أو يعادل في التأثير العنف البدني الجسيم. وتحديد ما إذا كان عمل ما يلبي هذا المعيار قرار لا يستطيع أن يتخذه سوى الزعماء السياسيين لدولة ما.

وهناك أربع فئات رئيسية للتهديدات السيبرانية للأمن الوطني، وكل منها تحتل فترة زمنية مختلفة وتتطلب (من حيث المبدأ) حلولاً مختلفة: الحرب السيبرانية والتجسس الاقتصادي، وهو ما يرتبط إلى حد كبير بالدول، وفئة الجريمة السيبرانية والإرهاب السيبراني، وهو ما يرتبط في الأغلب بجهات فاعلة غير تابعة لدولة. وتنبع أعلى التكاليف حالياً من التجسس والجرائم، ولكن الفئتين الأخريين ربما تصبحان أعظم تهديداً على مدى العقد القادم مقارنة بحالهما اليوم. وعلاوة على ذلك، مع تطور

التحالفات والتكتيكات، ربما تتداخل الفئات بشكل متزايد.

أثناء الحرب الباردة، كانت المنافسة الإيديولوجية سبباً في تقييد التعاون بين الولايات المتحدة والاتحاد السوفييتي، ولكن إدراك الجانبين للدمار النووي قادهما إلى وضع مدونة سلوك بسيطة لتجنب المواجهة العسكرية. وكانت قواعد الحيطة الأساسية هذه تشمل عدم الدخول في قتال مباشر، والامتناع عن الاستخدام الأول للأسلحة النووية، واتصالات الأزمة، مثل الخط الساخن بين موسكو وواشنطن، وتدابير الحوادث، واتفاقيات حوادث البحر.

كان أول اتفاق رسمي للحد من التسلح في عام 1963 هو معاهدة حظر التجارب النووية المحدودة، والتي يمكن اعتبارها في الأساس معاهدة بيئية. وكان الاتفاق الرئيسي الثاني معاهدة منع الانتشار النووي في عام 1968، والتي كانت تهدف إلى الحد من انتشار الأسلحة النووية. وكانت نظرة الولايات المتحدة والاتحاد السوفييتي إلى الاتفاقيتين باعتبار كل منهما صفقة تعود بالفائدة على الجميع، لأنها شملت الطبيعة أو أطراف ثالثة.

وعلى نحو مماثل، كانت المجالات الواعدة للتعاون الدولي المبكر حول تأمين الفضاء السيبراني هي المشاكل التي تفرضها أطراف ثالثة مثل المجرمين والإرهابيين. وقد سعت روسيا والصين إلى إبرام معاهدة للإشراف الواسع النطاق من قِبَل الأمم المتحدة على الإنترنت. ورغم أن رؤية البلدين "لأمن المعلومات" قد تضفي الشرعية على الرقابة الحكومية الاستبدادية، وهي بالتالي غير مقبولة لدى الحكومات الديمقراطية، فربما كان من الممكن تحديد واستهداف السلوكيات التي هي غير قانونية في أي مكان. والحد من كل الانتهاكات أمر مستحيل، ولكن من الممكن أن نبدأ بالجريمة السيبرانية والإرهاب السيبراني. والدول الكبرى لديها مصلحة في الحد من الضرر من خلال الاتفاق على التعاون في دراسة عناصر الجريمة والضوابط.

إن القياسات والمقارنات التاريخية غير دقيقة وغير كاملة بطبيعة الحال. ومن الواضح أن التكنولوجيا السيبرانية تختلف تماماً عن التكنولوجيا النووية، خاصة وأن الجهات الفاعلة غير الحكومية من الممكن أن تستغلها بقدر أكبر كثيراً من السهولة.

ورغم هذا فإن بعض المؤسسات، الرسمية وغير الرسمية، تحكم بالفعل العمل الأساسي لشبكة الإنترنت. فتعتزم الولايات المتحدة بحكمة تعزيز مؤسسة الإنترنت غير الحكومية للأسماء والأرقام المخصصة (ICANN) بتكليفها بالإشراف على "دفتر عناوين" الإنترنت. وهناك أيضاً اتفاقية جرائم الإنترنت التي أقرها مجلس أوروبا في عام 2001، حيث يعمل الإنتربول واليوروبول على تسهيل التعاون بين قوات الشرطة الوطنية. وكانت مجموعة الأمم المتحدة للخبراء الحكوميين تعكف على تحليل كيفية ارتباط القانون الدولي بالأمن السيبراني.

من المرجح أن يستغرق إبرام الاتفاقيات بشأن القضايا الخلافية مثل الاقتحام السيبراني لأغراض مثل التجسس وإعداد ساحة المعركة وقتاً أطول. ورغم ذلك فلا ينبغي لعدم القدرة على تصور اتفاقية شاملة للحد من التسلح السيبراني أن يمنع التقدم بشأن بعض القضايا الآن. إن المعايير الدولية تميل إلى التطور ببطء. فقد استغرق الأمر عقدين من الزمان في حالة التكنولوجيا النووية. وكانت الرسالة الأكثر أهمية التي أبرزها المؤتمر الهولندي الأخير هي أن نقاط الضعف السيبرانية الهائلة تقترب الآن من هذه النقطة.

* سكرتير مساعد وزير الدفاع السابق، وأستاذ في جامعة هارفارد، مؤلف كتاب القوة الناعمة، أحدث مؤلفاته كتاب بعنوان مستقبل القوة

.....

* الآراء الواردة لا تعبر بالضرورة عن رأي شبكة النبأ المعلوماتية