الخليج

كتب و كتاب

4 نوفمبر 2023 21:59 مساء

ديناميات التصعيد في الفضاء السيبراني

عن المؤلف

إيريكا لونيرجان و شون دبليو لونيرجان
إيريكا لونيرجان.. أستاذة مساعدة في المعهد السيبراني العسكري في الأكاديمية العسكرية الأمريكية في ويست بوينت.
**
شون دبليو لونيرجان.. ضابط برتبة مقدّم في قيادة الابتكار رقم 75 في احتياطي الجيش الأمريكي. كان ضابطاً إلكترونياً في الخدمة، ولعب أدواراً رئيسية في وكالة الأمن القومي.

• الفضاء السيبراني جاهز للتصعيد وهو قاب قوسين أو أدنى

تأليف: إيريكا لونيرجان وشون دبليو لونيرجان

عرض وترجمة: نضال إبراهيم

كان المراقبون يشعرون بالقلق إزاء التصعيد السيبراني لعقود من الزمن، ولكنه لا يزال موضع نقاش، وتكتسب هذه القضية أهمية متزايدة بالنسبة إلى السياسة الدولية، مع قيام المزيد من الدول بتطوير واستخدام القدرات السيبرانية الهجومية، ومع تزايد تميز النظام الدولي بالتعددية القطبية الناشئة.

في كتابهما «ديناميكيات التصعيد في الفضاء السيبراني»، يتناول كل من إيريكا لونيرجان وشون دبليو لونيرجان بشكل مباشر السؤال التالي: «إلى أي مدى تزيد عمليات الفضاء الإلكتروني من مخاطر التصعيد بين الدول القومية المتنافسة؟»، حيث يقدمان نظرية شاملة تشرح الظروف التي قد تؤدي في ظلها العمليات السيبرانية إلى التصعيد.
يضم الكتاب ثمانية فصول: الأول: لماذا لا يوجد تصعيد في الفضاء السيبراني؟. الثاني: أربع سمات للعمليات السيبرانية. الثالث: نظرية التصعيد السيبراني. الرابع: ضبط النفس والتكيف: كيف يمكن للعمليات السيبرانية نزع فتيل الأزمات. الخامس: أنماط التصعيد في الفضاء السيبراني. السادس: العمليات السيبرانية وتهدئة الأزمات الدولية.
السابع: سيناريوهات التصعيد المحتملة في المستقبل: العمليات السيبرانية في سياق القتال. الثامن: الآثار المترتبة على صنع السياسات.
ويقدم هذا الكتاب الصادر عن مطبعة أكسفورد 2023، رؤى حول كيفية تأثير الفضاء السيبراني في السياسة الدولية، من خلال استكشاف دور العمليات السيبرانية في المنافسة الروتينية والأزمات، والقتال.
لماذا لا يوجد تصعيد في الفضاء الإلكتروني؟
في صيف عام 2021، وبعد أشهر قليلة من توليه منصبه، حذر الرئيس الأمريكي، جوزيف بايدن، في خطاب ألقاه من أنه إذا اندلعت «حرب حقيقية مع قوة كبرى»، فسيكون سببها «اختراق سيبراني لانتهاكات كبيرة». وليست هذه هي المرة الأولى ـ ولن تكون الأخيرة على الأرجح ـ التي يعرب فيها أحد كبار صناع السياسات علناً، عن مخاوفه من صراع وشيك ناجم عن أحداث في الفضاء الإلكتروني. والواقع أن الخبراء ظلوا على مدى عقود من الزمن يتنبأون بحدوث «بيرل هاربور الإلكتروني»، أو«11 سبتمبر الإلكتروني»، وهو هجوم حاسم ومدمر ومفاجئ، في كثير من الأحيان، من قبل جهة فاعلة شائنة في الفضاء الإلكتروني، والذي من شأنه أن يؤدي إلى عدم الاستقرار، بل وحتى الحرب. والمشكلة في هذه المخاوف هي أنها ببساطة لم تتحقق، على الرغم من حقيقة مفادها أن الفضاء السيبراني

أصبح أكثر خطورة، بمرور الوقت. ويعمل المزيد من الدول على تطوير القدرات السيبرانية العسكرية، وأصبحت المنظمات الإجرامية أكثر تطوراً، وتنتشر الأدوات الهجومية، ويتزايد النشاط في الفضاء السيبراني. ومع ذلك، حتى الآن، لم يتسبب أي هجوم سيبراني واحد بردّ دولة ما باستخدام القوة العسكرية، أو التسبب بدوامة تصعيدية. وهذا يطرح السؤال التالي: لماذا لم يشهد النظام الدولي تصعيداً سيبرانياً ملموساً؟

يهدف الكتاب إلى الإجابة عن هذا السؤال، من خلال تقديم وجهة نظر واحدة حول الأسباب التي لا تجعل العمليات السيبرانية تؤدي إلى التصعيد. وعلى وجه التحديد، يقدم المؤلفان إطاراً نظرياً يأخذ في الاعتبار الخصائص الفريدة للعمليات السيبرانية، ويتتبعان الآليات التي من المرجح أن تؤدي الأنشطة في الفضاء السيبراني، بشكل أو بآخر، إلى ديناميكيات تصعيدية بين الدول. ومن خلال القيام بذلك، يميّزان بين التصعيد في حالات الأزمات التي لا تصل إلى حد الحرب وأنماط التصعيد المحتملة أثناء الصراع المباشر.

المنافسة الاستراتيجية

يعلق المؤلفان بالقول: «لقد حدثت العمليات في سياق المنافسة الاستراتيجية السابقة بين الدول التي تقع تحت مستوى الصراع المسلح. وفي هذه المواقف، لا يوجد دليل يذكر على أن العمليات السيبرانية تؤدي إلى التصعيد. وبدلاً من ذلك، نجد أن نفس الخصائص التي تجعل العمليات السيبرانية أدوات سيئة للتصعيد، يمكن أيضاً أن تمكّن الدول من استخدام العمليات السيبرانية لنزع فتيل الأزمات. في المقابل، نفترض أن العمليات السيبرانية قد تكون أكثر عرضة للمساهمة في ديناميكيات التصعيد بمجرد بدء الصراع بالفعل، ولكن هذا يرجع إلى منطق مختلف تماماً، عن ذلك الذي يعمل أثناء المنافسة الروتينية أو الأزمات بين الدول».

ويضيفان: «أصبح سؤال إذا ما كانت التكنولوجيات الناشئة قد تساهم في الاستقرار الدولي، وكيف يمكن أن تساهم في ذلك، شائعاً بين الخبراء وصناع السياسات. وتبلورت الجهود الأكاديمية لفهم ديناميكيات التصعيد والتنبؤ بها خلال الحرب الباردة وأصبحت حادة بشكل خاص خلال أزمة الصواريخ الكوبية عندما أصبح تهديد الإبادة النووية فجأة، حقيقياً تماماً». ويشير ريتشارد سموك، إلى أن مفهوم التصعيد «لم يظهر في القواميس، أو في الأدبيات العسكرية أو العلمية، أو في التصريحات العامة للمسؤولين الحكوميين، قبل عام 1960 تقريباً».

مخاطر الحرب

ويشيران إلى أنه «خلال العقود التالية، دفعت القوة التدميرية الهائلة الكامنة في الأسلحة النووية الخبراء إلى النظر في المسارات التي يمكن أن تساهم فيها هذه القدرة الجديدة في مخاطر الحرب واستقرار الأزمات، والتصعيد، أو التخفيف منها. وكان الردع والتصعيد بمثابة الإطارين الأساسيين لتفسير الاستقرار النظامي، أو عدم الاستقرار. فمن ناحية، كان من المفترض أن يؤدي الردع المتبادل من خلال التهديد المتبادل والموثوق بحرب نووية كارثية إلى ضخ الاستقرار في العلاقات بين القوتين العظميين في الحرب الباردة، ومنع أي منهما من إطلاق العنان للتأثيرات المدمرة للأسلحة النووية من ناحية أخرى. ومن ناحية أخرى، فإن احتمال التصعيد غير المقصود يهدد بتقويض الاستقرار ذاته الذي يُزعم أنه تم تحقيقه من خلال الردع الاستراتيجي المتبادل، والذي يُطلق عليه، غالباً، مفارقة الاستقرار وعدم الاستقرار. وبشكل متصل، فإن فكرة التصعيد المتعمد ـ التي تم وصفها بشكل ملحوظ في «سلّم التصعيد» الشهير لهيرمان كان ـ تصور تفاعلاً استراتيجياً يمكن من خلاله لدولة واحدة ردع السلوك غير المرغوب فيه وتحقيق النصر من خلال الحفاظ على «هيمنة التصعيد» على الخصم في المنطقة. لكن الأسلحة السيبرانية (إذا كان من المناسب استخدام مصطلح السلاح للإشارة إلى القدرات السيبرانية الهجومية) لا يمكن مقارنتها بالأسلحة النووية. وعلى الرغم من ذلك، حاول الباحثون وصناع السياسات في العصر الراهن، على حد سواء، تطبيق نماذج الردع التي تعود للحرب الباردة على الفضاء السيبراني، خاصة في الولايات المتحدة.

ويؤكد المؤلفان أنه «في الواقع، لا يزال الردع بمثابة الإطار المفاهيمي الأساسي لاستراتيجية حكومة الولايات المتحدة

السيبرانية. إن الردع السيبراني معقد بسبب عدد من العوامل، بما في ذلك انتشار مجموعة متنوعة من الجهات الفاعلة السيبرانية، ومشاكل الإسناد، وحدود المصداقية وآليات الإشارة، والتحديات المتعلقة بإظهار القدرات السيبرانية للانتقام، على سبيل المثال لا الحصر، علاوة على ذلك، تحدد نماذج الردع النووي النتائج بمصطلحات ثنائية، حيث النجاح هو الغياب التام للاستخدام النووي، وهذا ليس له معنى عند تطبيقه على الفضاء الإلكتروني، حيث، على النقيض من عدم استخدام الأسلحة النووية منذ عام 1945، اتسمت التفاعلات بين القوى السيبرانية بالاستخدام الروتيني للقدرات السيبرانية لتعريض البنية التحتية الحيوية للخصم للخطر، والقيام بحملات تجسس على نطاق واسع، وتعطيل عمل الأنظمة الحيوية، وحتى إحداث تأثيرات مدمرة ضد الأصول الاستراتيجية. على سبيل المثال، حدد تقرير لعام 2020، وهو أحد المصادر الموثوقة التي تتتبع الاتجاهات (Verizon Data Breach) استقصائي صادر عن السنوية في خروقات بيانات القطاع الخاص عبر مجموعة من الصناعات في الولايات المتحدة، 157,525 حادثاً إلكترونياً، بما في ذلك 32,002 حادث أمني، في عام 2020 وحده. وهذا لا يمثل سوى مجموعة فرعية واحدة من الحالات من عموم الحوادث السيبرانية».

الردع السيبراني

يجد المؤلفان أنه إذا كان الردع السيبراني بعيد المنال أو يمثل مشكلة في الفضاء السيبراني، وإذا تم قبول الردع بشكل عام كمحدد رئيسي للاستقرار الاستراتيجي، فسيكون من المعقول استنتاج أن التفاعلات الاستراتيجية بين المنافسين في الفضاء السيبراني يجب أن تتميز بعدم الاستقرار المتوطن، ومخاطر التصعيد المستمرة. وفي الواقع، هناك مجموعة كبيرة وصريحة من الباحثين والممارسين الذين يؤكدون أن الفضاء السيبراني جاهز للتصعيد، وإذا لم يحدث التصعيد بعد، فهو قاب قوسين أو أدنى. على سبيل المثال، يؤكد جيسون هيلي أنه «من المرجح أن يكون «الصراع السيبراني» أكثر تصعيداً من الأنواع الأخرى من الصراع». ويؤكد أيضاً أن الطرق التي تعمل بها الدول عادة على تعزيز الردع، وبالتالي تعزيز الاستقرار ـ مثل التلويح بالقدرات للإشارة إلى العزم ـ من المرجح أن تؤدي إلى زعزعة الاستقرار، وتحمل آثاراً تصعيدية في الفضاء السيبراني من خلال دفع الأهداف إلى المبالغة في رد الفعل بدلاً من الردع.

ويضيفان: «ويحذر آخرون من مخاطر التصعيد الناجمة عن الأضرار الجانبية غير المقصودة وزيادة مخاطر العدوى من العمليات السيبرانية، والتي تفاقمت بسبب القيادة والسيطرة الفضفاضة التي غالباً ما تمارسها الدول على الجهات الفاعلة التي تجري، ويرى مارتن ليبيكي أنه، مع الحفاظ على شدة المصالح المعرضة للخطر، من المرجح أن تكون إدارة الأزمات أكثر صعوبة في الفضاء الإلكتروني مقارنة بالمجالات التقليدية. ويفترض ليبيكي أيضاً أن التصعيد غير المقصود أكثر احتمالاً في الفضاء الإلكتروني بسبب الاختلافات في كيفية تحديد أطراف الأزمة للعتبات الحرجة؛ وتورط أطراف ثالثة في النزاعات السيبرانية وما يترتب على ذلك من صعوبات في تحديد المصدر؛ وبسبب تفاقم مشاكل القيادة والسيطرة. ويحذر روجر هورويتز من خطر الصراع والتصعيد في الفضاء السيبراني نتيجة لسباقات التسلح السيبراني، والتصورات التي مفادها أن الهجوم له ميزة على الدفاع في الفضاء السيبراني. فهجوم واسع النطاق، وطويل الأمد على شبكة إنتاج الغذاء أو توزيع الإمدادات، يمكن أن يؤدي إلى خسائر مدمرة يمكن مقارنتها بضربة نووية صغيرة النطاق. وأشار القادة العسكريون إلى أن الأعداء المجهزين (بالقدرات السيبرانية الهجومية) يمكن أن يكونوا عرضة للهجوم الوقائي والتصعيد السريع في أي أزمة مستقبلية، لأن كلا الجانبين سيكون لديه الحافز للضرب أولاً».

سمات العمليات السيبرانية

ويحاول المؤلفان في الكتاب تطوير نظرية للتصعيد السيبراني تعمل على توسيع الحجج التقليدية حول التصعيد في أدبيات الدراسات الأمنية، مع الأخذ في الاعتبار السمات الفريدة للعمليات السيبرانية. ويقولان: «إن التصعيد، سواء كان متعمداً، أو غير مقصود، هو في نهاية المطاف قرار سياسي ينفذه بشر يعملون داخل المنظمات، ولا يحدث من خلال القوة المطلقة للتكنولوجيا، وحدها. والأهم من ذلك، أن ما يمكن اعتباره عملاً تصعيدياً، بغضّ النظر عن القدرات

التي يمكن توظيفها، يجعل المتغيرات السياسية والتنظيمية والنفسية ضرورية لتحليل الظروف التي من المحتمل أن يحدث فيها التصعيد. ومع ذلك، فإن التكنولوجيا نفسها ـ الفرص التي تقدمها والقيود التي تحتويها ـ تحدد معالم الممكن. إن القدرة، على سبيل المثال «تمكّن قوة عسكرية من القتال بمزيد من السرعة والمدى والفتك، ستمكن تلك القوة من عبور عتبات التصعيد بشكل أسرع». إن مجموعة ضيقة من الشروط، قد تخفف من مخاطر التصعيد. وفي هذا الكتاب، يركزان على الجوانب الفنية للعمليات السيبرانية، والقيود والفرص التي توفرها للقادة، لأنها أساس ضروري لاستكشاف الجوانب السياسية لعملية صنع القرار حول مصالحهم.

ويعتمد تحليلهما لديناميات التصعيد على أربع سمات للعمليات السيبرانية: السرية، وإمكانية الإنكار المعقول؛ ،متطلبات تخطيط وتنفيذ العمليات الهجومية: القيود المفروضة على توليد التكلفة؛ ودور الاستخبارات. وفي حين أن كل واحدة من هذه القدرات، على حدة، قد لا تكون فريدة بالنسبة للفضاء السيبراني، إلا أنه في المجمل هناك عدد قليل من القدرات العسكرية المماثلة التي تحتوي على كل هذه الميزات. وتؤدي هذه الجوانب من العمليات السيبرانية إلى العديد من الآثار المترتبة على التصعيد. أولاً، تحتوي العمليات السيبرانية على قيود متأصلة على توظيفها، ما يقلل من احتمال أن تؤدي العمليات السيبرانية إلى التصعيد أثناء الأزمات الدولية. ثانياً، قد تجعل هذه العوامل نفسها العمليات السيبرانية مفيدة لنزع فتيل حالات الأزمات بدلاً من تفاقمها. وأخيراً، على الرغم من هذه القيود، هناك عدد صغير، ولكنه مهم، من السيناريوهات المعقولة التي يمكن أن تؤدي فيها العمليات السيبرانية إلى زيادة مخاطر التصعيد بشكل غير مباشر، وعلى طول مسار التصعيد هذا. وفي حين أن التأثيرات المباشرة للعمليات السيبرانية لا تزال طفيفة وعابرة، فإن الآثار الثانوية على القدرات الحركية ـ تلك القدرات العسكرية التي يمكن أن تسبب في الواقع مستوى من الضرر يكفي للتسبب في التصعيد ـ يمكن أن تؤدي إلى التصعيد.

عن المؤلفين:

إيريكا لونيرجان.. أستاذة مساعدة في المعهد السيبراني العسكري في الأكاديمية العسكرية الأمريكية في ويست بوينت.

**

شون دبليو لونيرجان.. ضابط برتبة مقدّم في قيادة الابتكار رقم 75 في احتياطي الجيش الأمريكي. كان ضابطاً إلكترونياً في الخدمة، ولعب أدواراً رئيسية في وكالة الأمن القومي.

الصورة

ترجمة وعرض:

نضال إبراهيم