ترجمات

الصين تتفوق في حرب الفضاء السيبراني والولايات المتحدة مطالبة باستراتيجية ردع جديدة*

بقلم: آن نوبرغر

ترجمة: صفا مهدي عسكر

تحرير: د. عمار عباس الشاهين

مركز حمورابي للبحوث والدراسات الاستراتيجية

23 آب 2025

تأسس مركز حمورابي للبحوث والدراسات الإستراتيجية عام 2008 بمدينة بابل (الحلة)، وحصل على شهادة التسجيل من دائرة المنظمات غير الحكومية المرقمة 1Z71874 بتاريخ 2012/12/25، بوصفه مركزا علميا بحثيا يهتم بدراسة الموضوعات السياسية والمجتمعية، فضلاً عن الاهتمام بالقضايا والظواهر الراهنة والمحتملة في الشأن المحلي والإقليمي والدولي، ويتعامل مع باحثين من مختلف التخصصات داخل العراق وخارجه، وتحتضن بغداد المقر الرئيسي للمركز.

- لا يجوز إعادة نشر أي من هذه الأوراق البحثية الا بموافقة المركز، وبالإمكان الاقتباس بشرط ذكر المصدر كاملا.
- لا تعبر الآراء الواردة في الورقة البحثية عن الاتجاهات التي يتبناها المركز وانما تعبر عن رأي كاتبها.
- حقوق الطبع والنشر محفوظة لمركز حمورابي للبحوث والدراسات الاستراتيجية.

للتواصل

العراق - بغداد - الكرادة

+964 7810234002

hcrsiraq@yahoo.com

www.hcrsiraq.net

مركز حمورابي للبحوث والدراسات الاستراتيجية

تُعد الشركات الأميركية في طليعة التكنولوجيا العالمية- سواء في البرمجيات المبتكرة أو الحوسبة السحابية أو الذكاء الاصطناعي أو منتجات الأمن السيبراني، غير أن ما حدث قبل نحو ثلاث سنوات كشف عن ثغرة خطيرة في منظومة الحماية الأميركية فقد تمكّن قراصنة يُعتقد أنهم مدعومون من الحكومة الصينية من تحقيق اختراق واسع النطاق لشبكات الاتصالات الأميركية مكّنهم من نسخ المحادثات وتتبع تحركات ضباط الاستخبارات الأميركية وعناصر إنفاذ القانون داخل الولايات المتحدة. هذا الهجوم الذي أُطلق عليه اسم «Salt Typhoon» (إعصار الملح)، شكّل جزءاً محورياً من حملة عالمية استهدفت شركات الاتصالات، واخترق أنظمة العديد من مزوّدي الخدمة الأميركيين إلى درجة تجعل من شبه المستحيل معرفة حجم القدرات الاستخباراتية التي أحرزتها الصين للتجسس على الاتصالات الأميركية.

لكن «Salt Typhoon» لم يكن مجرد نجاح استخباراتي عابر للصين بل عكس واقعاً أكثر خطورة فبعد عقود قليلة من انتشار الإنترنت وظهوره كساحة جديدة للتنافس الجيوسياسي تسعى الصين لفرض هيمنتها على فضاء الصراع الرقمي، فيما تراجعت الولايات المتحدة عن حماية جبهتها الداخلية الرقمية الممتدة وما يرتبط بها من أصول مادية، وفي ظل أن الفضاء السيبراني بلا حدود فإن الداخل الأميركي أصبح جزءاً دائماً من ساحة المواجهة فالمستشفيات وشبكات الكهرباء وخطوط الأنابيب ومحطات معالجة المياه وأنظمة الاتصالات تمثل جميعها خطوط تماس مباشرة ومعظم البنية التحتية الحيوية الأميركية غير مجهّزة لخوض هذه الحرب.

كما تمتد الهيمنة الصينية أبعد من نطاق التجسس على الاتصالات إذ عُثر على برمجيات خبيثة صينية مزروعة داخل أنظمة الطاقة والمياه والأنابيب ووسائل النقل الأميركية، هذه الاختراقات لا توحي بعمليات جمع معلومات تقليدية بل تبدو مُهيأة للتخريب ما يمنح الصين القدرة على تعطيل الحياة اليومية للأميركيين وإعاقة العمليات العسكرية الأميركية في أوقات الأزمات، ففي حال نشوب مواجهة مستقبلية يمكن لبكين استخدام هذه القدرات لتعطيل الحشد العسكري أو شلّ أنظمة المراقبة الجوية أو التسبب بانقطاع واسع في الطاقة، وحتى دون هجوم مباشر فإن مجرد امتلاك هذه القدرات يكفي لردع الولايات المتحدة عبر التلويح بتهديد تعطيل الداخل.

ويعود نجاح «Salt Typhoon» إلى الفارق الجوهري بين النهج الاستبدادي لبكين في إدارة أمنها السيبراني والنهج الديمقراطي لواشنطن، فالقيم الأميركية تمنع الرقابة الشاملة التي تُعد ركناً أساسياً في منظومة الدفاع الصينية وهو ما يمنح بكين مساحة أكبر لممارسة الهجوم السيبراني دون خوف كبير من الرد، وإضافة إلى ذلك فإن مسؤولية إدارة البنية التحتية الحيوية الأميركية موزعة بين جهات خاصة متعددة تحت إشراف حكومي محدود واستثماراتها في الأمن السيبراني متفاوتة وتخضع لاعتبارات ربحية ما يجعل من الصعب ضمان طرد القراصنة بشكل نهائي حتى بعد اكتشافهم.

---

* Anne Neuberger, China Is Winning the Cyberwar America Needs a New Strategy of Deterrence, FOREGIN AFFAIRS, August 13, 2025.

ورغم أن الصين تمثل التحدي الأكبر فإنها ليست وحدها، فقد كشفت السنوات الأخيرة عن استغلال روسيا وإيران لثغرات في أنظمة المياه في عدة ولايات أميركية فيما تسببت مجموعات قرصنة معظمها روسية في تعطيل مئات المستشفيات الأميركية، وبذلك يتضح أن واشنطن قادرة -وملزمة- على بذل جهود أكبر لحماية بنيتها التحتية وردع الهجمات الصينية، ومع بروز ثورة الذكاء الاصطناعي قد تتفاقم مواطن الضعف الأميركية إذا لم يُعَد النظر سريعاً في الاستراتيجية المتبعة.

إن المطلوب اليوم هو تبني سياسة ردع سيبراني جديدة قائمة على مبدأ أن الدفاع القوي يمكّن من هجوم فعال، وهنا يبرز الذكاء الاصطناعي كعنصر حاسم إذ ينبغي على الولايات المتحدة استثمار تفوقها فيه لإطلاق مشروع وطني يهدف إلى محاكاة شبكات البنية التحتية الحيوية ورصد أهم نقاط الضعف ومعالجتها مع ضمان امتلاك القدرات الهجومية اللازمة لردع الصين، كما يجب أن تُوضح واشنطن بشكل لا لبس فيه أن التمركز المسبق في أنواع معينة من البنى التحتية يمثل خطاً أحمر مع إرسال رسائل مدروسة بشأن قدرتها على الرد.

وبالاعتماد على دفاعات مدعومة بالذكاء الاصطناعي واستثمارات استراتيجية في القدرات الهجومية، تستطيع الولايات المتحدة تحويل استراتيجيتها الحالية من حالة قصور إلى سياسة ردع استباقي، ولا يمكن لواشنطن إيصال رسالة حازمة إلى بكين بأنها ماضية في حماية حياة الأميركيين إلا عبر كشف الثغرات الأكثر حساسية في بنيتها التحتية الرقمية وتأمينها.

السلاح السري

كان هجوم «**Salt Typhoon**» (**إعصار الملح**) عملية متقدمة ومتعددة المراحل، للحصول على صلاحيات إدارية داخل شبكات الاتصالات استغل المهاجمون ثغرات في منتجات الأمن السيبراني لشركات الاتصالات الأميركية- مثل الجدران النارية-واستخدموا كلمات مرور مسروقة من عمليات اختراق أخرى غير مرتبطة بالهجوم، وبمجرد التسلل قام القراصنة بزرع برمجيات خبيثة والسيطرة على عمليات وبرامج مشروعة لضمان استمرار وجودهم، ثم استخدموا أجهزة الحواسيب والخوادم والموجّهات وغيرها من المعدات المخترقة للانتقال عبر شبكات الشركات المختلفة والتمركز في مواقع مثالية للتجسس.

تكمن جذور التفوق السيبراني الصيني في الفوارق البنيوية بين الأنظمة الاستبدادية والديمقراطية، ففي بدايات الهجمات السيبرانية مع ظهور الإنترنت كانت الصين والولايات المتحدة تواجهان مستوى متقارباً من الهشاشة، لكن بكين عملت بشكل منهجي على بناء دفاعاتها السيبرانية بينما واجهت واشنطن صعوبة في الموازنة بين حماية فضائها السيبراني والحفاظ على الحريات المدنية. لقد أثار النمو المتسارع للإنترنت في التسعينيات قلق القيادة الصينية التي خشيت من قدرته على تعزيز حرية التعبير، وكما هو متوقع من نظام سلطوي اختارت بكين فرض قيود مشددة ففي أواخر التسعينيات، نشرت الحكومة الصينية مجموعة من القوانين والتقنيات لفرض الرقابة على المحتوى وحجب المواقع والتطبيقات الغربية.

وغالباً ما يصف المراقبون الخارجيون «الجدار الناري العظيم» بأنه مجرد أداة للرقابة الداخلية لكن بعد أن أدت هذه الوظيفة اكتشفت بكين أنه يوفر فائدة أخرى بالغة الأهمية، فإلى جانب مراقبة المحتوى «التخريبي» يمكن لتقنيات هذا الجدار التعرف على الشيفرات الخبيثة قبل وصولها إلى الأنظمة الحيوية مما زود الصين بأدوات دفاعية متقدمة ضد الهجمات السيبرانية، ونتيجة لذلك تعمل محطات معالجة المياه وشبكات الطاقة والاتصالات والبنية التحتية الحيوية الأخرى في الصين بمستويات حماية متراكبة تفتقر إليها الأنظمة الأميركية في معظم الحالات. أما في الولايات المتحدة فالوضع مختلف تماماً إذ تخضع البنية التحتية الحيوية لملكية آلاف الشركات الخاصة التي تختلف في مستوى وعيها الأمني وقدراتها التقنية، على سبيل المثال تعمل محطة صغيرة لمعالجة المياه في أوهايو وفق إمكاناتها المحدودة وغالباً ما تعتمد على برمجيات ضعيفة الحماية أو كلمات مرور افتراضية أو أنظمة قديمة يسهل اختراقها، كما أن القوانين الأميركية تمنع الحكومة من مراقبة شبكات هذه الشركات دون موافقتها الصريحة التزاماً بالحظر الدستوري على «التفتيش والمصادرة» في الاتصالات الخاصة، وبهذا اضطرت واشنطن إلى الاعتماد على نهج متشتت يقوم على مسؤولية الشركات المالكة والمشغلة للبنى التحتية الحساسة في حماية أنظمتها مع رقابة حكومية محدودة.

الروبوتات الخضراء الصغيرة

هذا الفراغ الدفاعي أتاح للصين تطوير قدرات هجومية مع هامش أوسع من الأمان، إذ استثمرت بكين بكثافة في برامج هجومية سيبرانية أصبحت اليوم تضاهي نظيراتها الأميركية من حيث الحجم والتعقيد، وقد دمجت الصين هذه القدرات ضمن عقيدتها العسكرية الأشمل القائمة على مبدأ «الدفاع النشط»، أي أن أفضل وسيلة للدفاع هي توجيه الضربة الاستباقية. بدأ الانخراط الدبلوماسي بين واشنطن وبكين حول التجسس السيبراني عام 2015 عندما توصل الرئيس الأميركي باراك أوباما ونظيره الصيني شي جينبينغ إلى اتفاق يحظر سرقة الملكية الفكرية من أجل مكاسب تجارية، لكن الصين سرعان ما انتهكت الاتفاق وفي عام 2017، تبنت إدارة الرئيس دونالد ترامب نهجاً قائماً على العقوبات والملاحقة القضائية بدلاً من الانخراط الدبلوماسي حيث أصدرت في آذار 2018 لوائح اتهام وعقوبات بحق قراصنة مرتبطين ببكين سرقوا بيانات من شركات وهيئات أميركية.

ومع تولي الرئيس جو بايدن السلطة في 2021 بادرت إدارته إلى تكثيف الحوار الدبلوماسي رفيع المستوى مع الصين لإدارة التنافس الاستراتيجي بين القوتين بما في ذلك في الفضاء السيبراني، فقد حصل بايدن على تعهد من شي بعدم التدخل في انتخابات 2024 الأميركية، غير أن الإدارة الأميركية سرعان ما أدركت أن الحملات السيبرانية الهجومية الصينية تتصاعد. ففي عام 2023 استغل قراصنة ترعاهم الدولة الصينية ثغرة في خدمات «مايكروسوفت» السحابية لاختراق البريد الإلكتروني لمسؤولين كبار، وفي كانون الثاني 2024 حذر مدير مكتب التحقيقات الفدرالي كريستوفر راي أمام لجنة في مجلس النواب من أن القراصنة المرتبطين بالحكومة الصينية يستهدفون البنية التحتية الحيوية الأميركية ويستعدون لإلحاق «أذى واقعي» بالأميركيين.

لقد باتت العمليات السيبرانية الصينية تهديداً مباشراً للأمن القومي الأميركي، فقد كُشف عن اختراقات في أنظمة المياه والكهرباء وغيرها من البنى التحتية الحيوية داخل الولايات المتحدة وتتبع هذه الهجمات نمطاً ثابتاً، الحصول على صلاحيات إدارية تثبيت القدرة على البقاء داخل الأنظمة لفترات طويلة ثم الانتظار في وضعية «كمون» مع الاحتفاظ بالقدرة على تفعيل الشيفرات الخبيثة عند الحاجة.

وتكشف الأهداف المختارة عن حسابات استراتيجية دقيقة إذ إن محطات معالجة المياه تؤدي دوراً مزدوجاً يخدم المدنيين والقواعد العسكرية وشبكات الطاقة تمكّن من تشغيل المستشفيات وإنتاج الذخائر فيما تُعد الاتصالات ركناً أساسياً لكل من الحياة المدنية ونظم القيادة العسكرية، ومن خلال زرع أدوات هجومية داخل هذه الأنظمة المزدوجة الاستخدام، تهيّئ الصين نفسها لفرض كلفة مدنية كبيرة بالتوازي مع إضعاف الفعالية العسكرية الأميركية.

وفي سيناريو أزمة حول تايوان قد تكون لهذه القدرات نتائج حاسمة، فمجرد التهديد بتعطيل شبكات السكك الحديدية أو التسبب في انقطاعات واسعة للطاقة على الساحل الشرقي قد يدفع صناع القرار الأميركيين لإعادة حساباتهم السياسية والعسكرية، ولا تحتاج بكين إلى تنفيذ هذه الهجمات فعلياً إذ يكفي التلويح بها لزيادة الكلفة السياسية لأي تدخل خارجي أميركي. وتسعى الصين أيضاً لتحقيق أهداف تكتيكية من خلال استهداف البنى التحتية المدنية التي يعتمد عليها الجيش الأميركي في الطاقة والمياه والاتصالات، ما يسمح بإعاقة التعبئة العسكرية دون استهداف مباشر للقواعد وبالتالي تفادي التصعيد الذي قد ينتج عن قصف منشآت عسكرية أميركية، وبالمثل فإن تعطيل الموانئ والمطارات قد يؤخر عمليات الدعم في المحيط الهادئ مع الإيحاء بأن الاستهداف يقتصر على بنى تحتية مدنية.

ويؤكد المنظّرون العسكريون الصينيون هذه المقاربة معتبرين أن الهجمات السيبرانية الهجومية تمثل شكلاً من «الردع الاستراتيجي»، وعلى خلاف أشكال الردع التقليدي توفر العمليات السيبرانية قدراً من الإنكار المعقول إذ تستطيع بكين التلويح بقدرتها على شل البنى التحتية المدنية مع الادعاء بأن أي أعطال ناجمة قد تكون نتيجة إخفاقات داخلية في الأنظمة المستهدفة لا هجمات مقصودة، ولهذا السبب تنفي الصين باستمرار مسؤوليتها عن هجوم «Salt Typhoon» أو عن البرمجيات الخبيثة المكتشفة في البنية التحتية الأميركية.

الرؤية المزدوجة

لقد جعل عنصر الإنكار الدائم من الدبلوماسية التقليدية أداة ضعيفة في التعامل مع الحرب السيبرانية فلم يعد بإمكان الولايات المتحدة الاعتماد على المفاوضات المباشرة بل يتوجب عليها الإسراع في تعزيز منظومتها الدفاعية وفي هذا السياق لجأت إدارة بايدن إلى استخدام الصلاحيات الطارئة لفرض معايير إلزامية جديدة للأمن السيبراني على شبكات الأنابيب، وأنظمة السكك الحديدية والمطارات ومرافق المياه متجاوزة عقوداً من المقاومة الحزبية تجاه فرض معايير أمنية على القطاع الخاص

وقد أدت هذه الإجراءات بالفعل إلى تحسين مستوى الحماية الأساسية كما منحت الهيئات التنظيمية الحكومية مثل إدارة أمن المواصلات المسؤولة عن تنظيم خطوط الأنابيب القدرة على إجراء عمليات تفتيش دورية لمنظومات الدفاع السيبراني لدى مالكي البنى التحتية وتقديم الإرشادات اللازمة. وعلى الرغم من أهمية هذه الخطوة فإنها تظل أقل فاعلية مقارنة بقدرات بكين على المراقبة المباشرة لشبكاتها الوطنية، فبينما ألزمت الإدارة الأميركية شركات الأنابيب والمياه والسكك الحديدية وقطاع الرعاية الصحية بالإبلاغ عن الحوادث السيبرانية بعد وقوعها يتمتع الصينيون بقدرة على الرصد الفوري الذي يتيح منع الهجمات قبل حدوثها، أما القيود الجديدة المفروضة على مرافق المياه الأميركية فقد جُمّدت بعد أن طعنت بعض الولايات في قانونيتها مما ترك هذا القطاع مكشوفاً.

تشبه العمليات السيبرانية في طبيعتها أشكال الحرب التقليدية- كالغارات الجوية أو المعارك البحرية والبرية- من حيث احتواؤها على البعدين الدفاعي والهجومي معاً، ففي حين تعتمد الولايات المتحدة في ردع التهديدات التقليدية على تفوقها العسكري فإنها تفتقر إلى مثل هذا التفوق في الفضاء السيبراني حيث يرتبط الهجوم والدفاع ارتباطاً وثيقاً، ومن ثم يواجه الرؤساء الأميركيون معضلة حقيقية إذ لا يمكنهم إطلاق تهديدات ردعية مقنعة في ظل غياب الثقة الكافية بقدرة الدفاعات الأميركية على الصمود أمام هجمات متبادلة قد تؤدي إلى تصعيد خطير، وعليه تحتاج واشنطن إلى سياسة تعترف بواقع الصراع السيبراني وتستثمر في الوقت نفسه تفوقها التكنولوجي لإعادة التوازن الاستراتيجي. وتتمثل الأولوية الأولى في إدراك مكامن الضعف داخل منظومة الدفاع السيبراني الأميركية، ففي الحروب التقليدية تستند الاستراتيجيات إلى مقارنات القوة المباشرة فالجيش الأميركي مثلاً يجري بانتظام اختبارات لمحاكاة قدرته على التصدي للهجمات الصاروخية الروسية، أما في المجال السيبراني فإن الحكومة لا تستطيع تقييم قدرة البنى التحتية الحيوية على مواجهة الهجمات الصينية لافتقارها إلى رؤية واضحة حول طبيعة أنظمة الحماية المنتشرة لدى آلاف المنشآت المملوكة للقطاع الخاص.

وهنا يبرز الذكاء الاصطناعي كفرصة جديدة بفضل قدرته المتنامية على تحليل كمٍّ هائل من البيانات ما يفتح الباب أمام سياسة ردع سيبراني قائمة على ما يُعرف بـ التوائم الرقمية، والتوأم الرقمي هو نسخة افتراضية لنظام أو كيان مادي (كمحطة طاقة أو شبكة كهرباء) تعتمد على بيانات فورية وحساسات لتجسيد سلوك نظيرها الواقعي وأدائه، وتتيح هذه النماذج الديناميكية مراقبة الأصول المادية وتحليلها وتحسينها عن بُعد.

لقد ضاعفت الطفرات الأخيرة في الذكاء الاصطناعي من فاعلية التوائم الرقمية عبر قدرتها المتزايدة على محاكاة كيانات ضخمة ومعقدة، وقد سارعت الشركات الصناعية إلى اعتمادها فشركة رولز رويس على سبيل المثال تستخدم توائم رقمية لمحركاتها النفاثة لمراقبة أدائها كما طورت شركات مثل فورد و BMW توائم رقمية لعمليات التصنيع بهدف تعزيز الكفاءة، وحتى الحكومات باتت تستثمر في هذه التقنية إذ أنشأت سنغافورة توأماً رقمياً لشبكات المياه والطاقة لديها واستخدمت الناتو أنظمة مماثلة في تدريباته السنوية للدفاع السيبراني.

بالنسبة للولايات المتحدة فإن إطلاق جهد وطني لتطوير توائم رقمية لمئات من أكثر أنظمة البنى التحتية حساسية - بالتعاون مع القطاع الخاص- سيتيح للفرق الأمنية اختبار سيناريوهات الهجمات الخطيرة في بيئة افتراضية آمنة مما يساعد على تحديد الثغرات الأكثر خطورة وتوجيه الموارد المحدودة لمعالجتها بفاعلية، كما ستسمح هذه النماذج برصد أنماط سلوك معيارية تساعد على اكتشاف أي شذوذ قد يشير إلى هجمات سيبرانية قبل وقوع أضرار مادية.

إن تبني هذه المقاربة سيتيح أيضاً محاكاة سيناريوهات الانهيار المتسلسل لشبكات الطاقة الإقليمية أو محاولات تلويث شبكات المياه الحضرية، بما يمكّن من تصميم إجراءات وقائية وتدابير استجابة طارئة أكثر دقة، وعلى المدى البعيد ستسمح التوائم الرقمية بإجراء مقارنات "قوة مقابل قوة" شبيهة بتلك المعتمدة في الحروب التقليدية الأمر الذي يمنح صانعي القرار أدوات تقييم أشمل وأكثر تطوراً. ويمكن لوزارة الطاقة الأميركية أن تطلق سريعاً مشروعاً تجريبياً لتطوير توائم رقمية لشبكة الطاقة الوطنية مستفيدة من النماذج المتوفرة لديها ومن خبرات مختبرات مثل لورانس ليفرمور وساندیا، إضافة إلى شراكاتها الوثيقة مع شركات الطاقة الأميركية، على أن تُستخدم الدروس المستخلصة من هذا المشروع لاحقاً في تطوير نماذج مماثلة لقطاعات حيوية أخرى.

ومع أن بناء توائم رقمية شاملة سيواجه تحديات تقنية كبيرة كتوفير البيانات التفصيلية لأنظمة البنى التحتية وحماية حقوق الملكية الخاصة فإنه يمثل الجسر المطلوب بين العالمين المادي والرقمي، ولا يمكن للولايات المتحدة أن تعتمد ببساطة على تكرار النموذج الصيني القائم على الرقابة الشاملة للدولة لكن التوائم الرقمية توفر بديلاً ذكياً يسمح للسلطات الأميركية بامتلاك صورة متواصلة عن وضعها الدفاعي السيبراني وتقييم جاهزيتها بشكل لحظي، وعليه فإن أي رئيس أميركي مقبل يواجه اعتداءً صينياً محتملًا سيكون قادراً على الاطلاع فوراً على محاكاة دقيقة لأداء البنى التحتية تحت ضغط هجوم مستمر وهي ميزة استخبارية تكتيكية تفتقر إليها واشنطن بشدة اليوم.

إرسال رسالة مباشرة

حتى الدفاعات المدعومة بالذكاء الاصطناعي لا تستطيع سدّ فجوة الأمن السيبراني التي تمنح الصين تفوقاً هيكلياً، فالقانون الأميركي الحالي يمنح مشغّلي البنى التحتية سلطة كاملة لمراقبة شبكاتهم كما أن التشريع الفيدرالي الصادر عام 2015 يتيح لهم تبادل المعلومات مع نظرائهم ومع الحكومة الفيدرالية لتعزيز الدفاع المشترك ومع ذلك ما يزال بعض القطاعات الأساسية يفتقر إلى إلزامية قيام المالكين والمشغّلين بمراقبة شبكاتهم فعلياً ، أما في القطاعات التي طُبقت فيها هذه المتطلبات فينبغي على الجهات التنظيمية فرض رقابة أكثر صرامة لضمان التزام المشغّلين بالحفاظ على دفاعاتهم السيبرانية والتعاون مع نظرائهم ومع الحكومة الفيدرالية.

ومهما بلغت درجة تطور الدفاعات فإنها وحدها لا تكفي لمواجهة مكامن التفوق الصيني، فالردع الحقيقي يتطلب القدرة على إضعاف قدرات الخصم بشكل مستمر والاستعداد لفرض تكاليف غير مقبولة عليه، وعلى الولايات المتحدة أن تطوّر وتحتفظ بقدرات هجومية في الفضاء السيبراني يمكنها تهديد أهداف حيوية بالنسبة لبكين مع إيصال رسالة واضحة بأنها قادرة ومستعدة لتوجيه ضربات إذا تجاوزت الصين الخطوط الحمراء الأميركية، وبدلاً من الدخول في عمليات اختراق متبادلة للبنى التحتية المدنية الصينية يمكن لواشنطن أن تركّز على استهداف الأصول العسكرية التي تعتمد عليها بكين في أوقات الأزمات وهو ما يتوافق مع القانون الدولي وقد يترك أثراً أوضح على حسابات الحكومة الصينية.

كما يتعين على الولايات المتحدة تعزيز خطابها الاستراتيجي إذ يجب أن توضّح أن استهداف البنى التحتية المدنية الحيوية والتي قد يؤدي تعطيلها إلى آثار مجتمعية جسيمة أمر غير مقبول حتى في حال شنّ هجمات تمهيدية، وبذلك تُبنى الرسالة على ما أعلنه الرئيس بايدن لبكين بأن الهجمات السيبرانية ذات الآثار المادية ستُعامل كعمل حربي، وينبغي على واشنطن أن تلتزم بثلاثة مبادئ أساسية وهي: سنُحمّل الفاعلين مسؤولية هجماتهم، نحن قادرون على الصمود، وسنردّ بالمثل.فالمصداقية تكمن في الوضوح والتهديدات المبهمة تشجّع الخصوم على الاختبار والمجازفة في الحسابات. ويجب أن تكون الرسالة الأميركية موثوقة ومتواصلة بحيث تكشف تفاصيل كافية لإثبات أن القدرات الهجومية الأميركية حقيقية من دون أن تمنح الخصم فرصة لإغلاق ثغراته، ويُظهر مثال روسيا حين استخدمت هجمات سيبرانية لإحداث انقطاعات في شبكة الكهرباء الأوكرانية قبل سنوات من غزوها الشامل عام 2022، خطورة الإفصاح المفرط عن القدرات السيبرانية إذ دفعت تلك التجربة أوكرانيا إلى تعزيز دفاعات شبكتها الكهربائية بشكل كبير.

ثمة أسباب وراء تأخر الولايات المتحدة في تعزيز دفاعاتها السيبرانية بعضها سياسي وبعضها تقني، فالكونغرس لا يُبدي رغبة كافية في توسيع السلطات القانونية وتخصيص الاستثمارات المستدامة التي يتطلبها بناء دفاع شامل، فيما تعارض الشركات الخاصة فرض متطلبات أمنية إلزامية تزيد من تكاليفها.

لكن نهج الانتظار والترقب لم يعد مقبولاً، فإذا لم تتحرك واشنطن بسرعة فإن الذكاء الاصطناعي لن يفعل سوى تسريع التفوق الصيني، فالولايات المتحدة تمتلك القدرات التقنية والموارد الاقتصادية والطاقة الابتكارية التي تمكّنها من استعادة المبادرة في ساحة الصراع الرقمي، وما تحتاجه الآن هو الرؤية والإرادة السياسية لاتخاذ خطوات شاملة. فالعالم كلّه يترقب، إن نجحت الولايات المتحدة فإنها ستقدم نموذجاً يبيّن كيف يمكن تحقيق فوائد الرقمنة وإنترنت حر من دون التفريط بالأمن القومي، أما إذا فشلت فسيُستخلص درس آخر أن الديمقراطيات أقل قدرة على حماية نفسها من التهديدات السيبرانية، الأمر الذي سيمنح استراتيجية الصين القائمة على "الردع النشط" مزيداً من القوة على الصعيد العالمي.