التوصل إلى اتفاق مع الصين بشأن الفضاء الإلكتروني

سكوت وارين هارولد (Scott Warren Harold)، ومارتن سي. ليبيكي (Martin C. Libicki)، وأستريد ستوث سيفالوس (Astrid Stuth Cevallos)

RAND CORPORATION

التوصل إلى اتفاق مع الصين بشأن الفضاء الإلكتروني

سكوت وارين هارولد (Scott Warren Harold)،
ومارتن سي. ليبيكي (Martin C. Libicki)،
وأستريد ستوث سيفالوس (Astrid Stuth Cevallos)

تم تحضيرها لمؤسسة RAND - البحث والتطوير الداخلي

للحصول على مزيدٍ من المعلومات حول هذا المنشور، الرجاء زيارة www.rand.org/t/rr1335

بيانات النشر المفهرسة لدى مكتبة الكونجرس
الرقم الدوليّ المعياريّ للكتاب 978-0-8330-9249-6

تم النشر بواسطة مؤسسة RAND، سانتا مونيكا، كاليفورنيا.

صورة الغلاف: الرئيس الأمريكي باراك أوباما (Barack Obama) يصافح الرئيس الصيني شي جين بينغ (Xi Jinping) بعد مؤتمر صحفي في حديقة الورود (Rose Garden) في البيت الأبيض بتاريخ 25 سبتمبر/ أيلول 2015 في واشنطن العاصمة. الرئيس أوباما (Obama) يرحّب بالرئيس جين بينغ (Jinping) أثناء حفل استقبال رسمي. تصوير أوليفير دوليري (Olivier Douliery)/ABACA (Sipa) عن طريق صور AP).

مؤسسة RAND هي منظمة بحثية تعمل على تطوير حلول للتحديات التي تواجه السياسات العامة وذلك للمساعدة في جعل المجتمعات في جميع أنحاء العالم أكثر أمانًا وسلامةً وصحةً وازدهارًا. مؤسسة RAND هي مؤسسة غير ربحية وحيادية وملتزمة بالصالح العام.

لا تعكس منشورات مؤسسة RAND بالضرورة آراء العملاء ورعاة الأبحاث الذين يتعاملون معها.

ادعم RAND

ادعم مؤسسة RAND وتبرع بمساهمة معفاة من الضريبة
www.rand.org/giving/contribute

www.rand.org

تمهيد

منذ تأسيس جمهورية الصين الشعبية، عام 1949، اتسمت العلاقة بين الولايات المتحدة والصين بقدر كبير من الصراع والتحدي والريبة الاستراتيجية. وقد ازداد ثقل التوترات التي تفرق بين البلدين في السنوات الأخيرة. وللأسف، تنعكس هذه التوترات على الفضاء الإلكتروني بقدر ما تنعكس على العلاقات في العالم الفعلي. وفي الواقع، من بين جميع المجالات التي اضطربت فيها العلاقة بين الطرفين، كان مجال الفضاء الإلكتروني أكثرها إثارة للخلاف. حيث شرعت كل من الولايات المتحدة والصين في بدء مفاوضات رسمية عام 2013 سعيًا لتسوية هذه الخلافات، إلا أنها توقفت فجأة عام 2014، وذلك عندما أوقفت الصين المفاوضات ردًا على إدانة الولايات المتحدة لعدد من الضباط العسكريين الصينيين باتهامات تتعلق بأنشطة تجسس إلكتروني.

وجاء هذا التقرير كنتيجة لغياب الحوار الرسمي وليستكشف خيارات السياسة الأمريكية لإدارة العلاقات مع الصين بشأن هذا الموضوع السياسي الشائك. وينظر التقرير في مسألتين أساسيتين: هل يمكن لكل من الولايات المتحدة والصين العودة إلى المفاوضات الرسمية المجدية بشأن القواعد والقوانين الخاصة بالفضاء الإلكتروني؟ وفي تلك الحالة، ما هي أكثر المجالات التي من المرجح أن يتم التوصل فيها إلى اتفاق، وما الأمور التي يمكن استبدالها بأخرى؟

يتعين أن يكون التحليل الوارد هنا مهمًا لمجموعتين: المجموعة المعنية بعلاقات الولايات المتحدة مع الصين، وتلك المعنية بوضع قواعد السلوك في الفضاء الإلكتروني، ولاسيما القواعد التي تعزِّز الأمن والحرية.

تم تمويل هذا التقرير، جزئيًا، من قِبل المتبرعين وبواسطة المخصصات المستقلة للبحث والتطوير لعقود مؤسسة RAND والمخصصة لتشغيل مراكز البحوث والتطوير التابعة لها والتي تعمل بتمويل فدرالي من وزارة الدفاع الأمريكية.

المحتويات

الملخص

منذ تأسيس جمهورية الصين الشعبية في عام 1949، اتسمت العلاقات بين الولايات المتحدة والصين بقدر كبير من الصراع والتحدي والريبة الاستراتيجية. بحلول منتصف عام 2015، لاحظ العديد من الخبراء الأمريكيين البارزين المختصين بالشأن الصيني تدهورًا سريعًا في العلاقات الثنائية بما يمكن وصفه بأنه تنافس شامل، ويطالب المحللون الأمريكيون الآن باستراتيجية شاملة جديدة إزاء الصين لموازنة قوتها المتصاعدة. ويرى عدد متزايد من المراقبين الصينيين، بشكل مشابه، "المنافسة الصامتة" التي تعكسها العلاقات بين أقوى دولتين في العالم.[1]

وللأسف، ينعكس هذا النمط من التوترات المتصاعدة بنفس القدر على الفضاء الإلكتروني، إذ أصبح الفضاء الإلكتروني فعليًا من أكثر المناطق المثيرة للخلاف. وحسب بعض التقارير، فإن التوترات في هذا المجال هي إحدى المسببات الرئيسية للمزيد من التدهور في العلاقات. وفي حين يؤثر سخط الولايات المتحدة على السلوك الصيني في الفضاء الإلكتروني تأثيرًا كبيرًا على الولايات المتحدة للصين، فإن قلق الصين من سلوك الولايات المتحدة في الفضاء الإلكتروني ذو أثر أقل على تشكيل رؤية الصين للولايات المتحدة إجمالًا، ما قد يفسر سبب محدودية نجاح الطرفين في متابعة الحوار حول هذه القضية حتى اليوم. شرعت الولايات المتحدة والصين في مباحثات ثنائية رسمية بخصوص الفضاء الإلكتروني في عام 2013، إلا أن الصين أوقفت هذه المباحثات في 2014، بعد إدانة الولايات المتحدة لخمسة ضباط بجيش التحرير الشعبي لتجسسهم

[1] مقال للكاتب ديفيد شامبو (David Shambaugh) بعنوان "التأقلم مع الصين وهي في حالة نزاع" بصحيفة واشنطن كوارترلي *Washington Quarterly* العدد 34 رقم 1، شتاء 2011، ص 27-7: ومقال جين بيرليز (Jane Perlez) بعنوان "مقطع فيديو شديد اللهجة للجيش الصيني يعتبر الولايات المتحدة تهديدًا للصين" بصحيفة نيويورك تايمز *New York Times*، 31 أكتوبر/تشرين الأول 2013؛ ومقال إدوارد وونج (Edward Wong) بعنوان "آراء العقيد الصيني المتشددة تنتشر في وجهات نظر الأغلبية" بصحيفة نيويورك تايمز *New York Times*، 3 أكتوبر/تشرين الأول 2015

الإلكتروني على أهداف تابعة للولايات المتحدة. رغم التخلي عن نهج مجموعة العمل الثنائية المختصة بالفضاء الإلكتروني (Cyber Working Group)، جرت بالفعل مباحثات بشأن الفضاء الإلكتروني في الحوار الاستراتيجي والاقتصادي الثنائي في صيف 2015، وتصدر الاتفاق المبدئي للمضي قدمًا في القضية قائمة النتائج التي عقدت بين شي (Xi) وأوباما (Obama) في واشنطن في سبتمبر/أيلول 2015. رغم ذلك، تبقى أسئلة جوهرية حول العلاقة بين الدولتين فيما يخص الفضاء الإلكتروني. وفي غياب مجموعة معايير وإجراءات تفصيلية كاملة لضبط الأنشطة المثيرة للقلق وقواعد راسية خاصة بالفضاء الإلكتروني، ستستمر هذه المشكلة في تشكيل خطر كبير على تلك العلاقة الثنائية وعلى السلام والاستقرار الإقليميين والنظام العالمي.

ومن وجهة نظر الولايات المتحدة، ثمة قضايا ثلاث رئيسية. تمثلت الشكوى الأساسية في اختراقات الصين المتعددة والمتكررة لشبكات الشركات لسرقة الملكية الفكرية ومعلومات الملكية التجارية. وكان المصدر الثاني للقلق هو الاختراق المتزايد للأنظمة الأمريكية عبر الفضاء الإلكتروني لأغراض تجسس تقليدية تتعلق بالأمن الوطني (على سبيل المثال، اختراق مكتب إدارة شؤون الموظفين الذي تم الكشف عنه في منتصف عام 2015، وذلك ربما لتجميع قواعد بيانات ضخمة حول المواطنين الأمريكيين [ومن المحتمل أيضًا جهات الاتصال الصينية الخاصة بهم] للنظر في تجنيدهم أو ابتزازهم. ويتمثل المصدر الثالث للقلق في احتمال أن تكون الصين على أهبة الاستعداد لشن هجوم إلكتروني بهدف تدمير البنية التحتية الأساسية الأمريكية في حال حدوث أزمة. ويتمثل المصدر الرابع للقلق في عدم الوضوح بشأن استخدام أي من الطرفين للهجوم الإلكتروني في حالة الحرب وخطر التصعيد.

ومن جانب الصين، فإنها تشجب اتهامات الولايات المتحدة لها بالقرصنة وتدعي بأنها هي التي تتعرض للهجمات الإلكترونية الصادرة من الولايات المتحدة. ويشكو المسؤولون والمحللون الصينيون من القيود التي تفرضها الولايات المتحدة على دخول شركات الاتصالات الصينية إلى الأسواق مثل هواوي (Huawei) وشركة زد.تي.إي (ZTE Corporation). كما ينتقد الجانب الصيني تمويل الولايات المتحدة لتكنولوجيا التحايل على الرقابة على الإنترنت ويؤيد حق الدول في الرقابة على المعلومات المتاحة للأفراد داخل حدودها (وهو مفهوم يُعرف بـالسيادة الإلكترونية). كما يدين المراقبون الصينيون ما يصفونه "بالهيمنة" الأمريكية على الإنترنت، ويشيرون إلى أن العديد من الموجهات والخوادم وكذلك البرامج المستخدمة لدعم البنية التحتية للإنترنت في الصين، تصنعها أو تتحكم بها الشركات الأمريكية.

وفي ظل هذه الآراء المتفاوتة، وبعد تخلي الصين عن المباحثات الرسمية حول الأمن الإلكتروني مع الولايات المتحدة، دفعتنا وحفزتنا عدة تساؤلات عاجلة حول

السياسات لكتابة هذا التقرير. هل يمكن لكل من الولايات المتحدة والصين العودة إلى المفاوضات الرسمية المجدية بشأن القواعد والقوانين الخاصة بالفضاء الإلكتروني؟ وفي تلك الحالة، هل يمكن أن تؤدي مباحثات كتلك، بين البلدين، إلى تفاهم مشترك حول قواعد الفضاء الإلكتروني؟ ما هي المسارات الممكنة للتوصل إلى اتفاقات مثمرة في مجال الفضاء الإلكتروني؟ ما هي المجالات التي يُرجح أن يتم التوصل فيها إلى اتفاق، وما الأمور التي يمكن استبدالها؟ وبسبب تفكيرنا في كيفية إدارة التحدي الشائك بشأن العلاقات بين الولايات المتحدة والصين، أجرينا أبحاثًا مكثفة أفضت إلى هذا التقرير. ويساهم التقرير بشكل أساسي في جدل السياسات العامة الدائر حول العلاقات بين الولايات المتحدة والصين بشأن الفضاء الإلكتروني على ثلاثة مستويات.

أولًا، يعرض التقرير بإيجاز هذه القضية للقارئ، ويقدم وثيقة واحدة تستعرض المراجع الموسعة التي أجريت حول هذه المسألة ويجردها إلى عناصرها الأساسية.

ثانيًا، يعرض التقرير وجهات نظر من مقابلات مع كبار الخبراء الصينيين والأمريكيين في سياسات الفضاء الإلكتروني من الحكومات والجيوش ومراكز الأبحاث والأوساط الأكاديمية في البلدين، ما يبرز منهجية لم تُستخدم من قبل والتي تسمح للقارىء بالاطلاع على كل من المخاوف الصينية والأمريكية مباشرةً من كبار المفكرين من الجانبين.

وثالثًا، يعرض التقرير مجموعة جديدة من الاستنتاجات، إذ تقترح أنه للحصول على الموافقة الصينية بشأن القواعد المستهدفة والمطلوبة للفضاء الإلكتروني، قد تكون الولايات المتحدة بحاجة إلى تحفيز الصين على الجلوس على طاولة المفاوضات واستكمال التفاوض، عبر زيادة تكاليف رفض التفاوض بشأن قواعد الأمن الإلكتروني والتشجيع على قبوله.

وتوصلنا إلى أنه رغم الاتفاق الظاهري بين الرئيس الأمريكي باراك أوباما (Barack Obama) والرئيس الصيني شي جين بينغ (Xi Jinping) في سبتمبر/ أيلول 2015، يرجح أن يبقى الطرفان على خلاف شديد بشأن الفضاء الإلكتروني، إلا إذا دخلا في مفاوضات رسمية بشأن مجموعة أكبر وأكثر فعالية من الاتفاقات التي تتضمن تفاصيل بشأن المصطلحات ومقاييس ومعايير الإثبات، والقواعد. وفي الجوهر، تختلف رؤى الولايات المتحدة والصين كثيرًا حول تطوير الفضاء الإلكتروني، وما يمكن أن تطلبه كل دولة من الأخرى. وتختلف رؤى الدولتين، كذلك، حول الأدوار التي تلعبها الأعراف وشرعية الإجراءات التي تتخذها الدول لتنفيذ تلك القواعد. ولا يعني هذا استحالة التوصل إلى اتفاق. وقد تلبي الصين رغبات الولايات المتحدة بغية الحد

من ضغط الولايات المتحدة، ولكن ليس من الواضح ما إذا كانت تلك الاتفاقات ستنفذ إلى ما هو أبعد من منفعتها قصيرة الأجل في مساعدة الصين على تجنب العقوبات (وهو تفسير محتمل للأسباب التي أدت إلى الاتفاق المفاجئ بشأن الفضاء الإلكتروني في سبتمبر/أيلول 2015). ونحن نرى أن السبيل للوصول إلى اتفاق دائم يتطلب من الصين الالتزام بتغيير سلوكها بشأن الفضاء الإلكتروني، مع الاستمرار على هذا النحو. لكن إقرارنا بصعوبة أو قلة إمكانية حدوث هذا الأمر لا يعني أنه مستحيل. ويستعرض ملخص العمل الوارد أدناه كيف توصلنا إلى هذه الاستنتاجات.

نهتم بوضع الأساس لفهم مواقف كلا الطرفين بشأن قضايا الأمن الإلكتروني من خلال وصف طريقتين شديدتي التباين تستطيع بهما الدول فهم قواعد الدول الأخرى وقوتها ودورها ومصالحها. ونطرح اثنين من الأنماط النموذجية. الأول هو الردع الأحمر، المستمد من الممارسات الصينية. والنمط الآخر هو الردع الأزرق، المستمد من الممارسات الأمريكية. تنظر الدول التي تمارس "الردع الأحمر" إلى الأعراف على أنها انعكاس لتوازن القوى الكامنة للدولة ومصالحها. وترى أن علاقات القوى بين الدول أمر سياسي وأن سلوكها تجاه القواعد يعد أمرًا ثانويًا. وترى الدول التي تمارس "الردع الأزرق" الأعراف على أنها أقرب إلى القوانين والحدود الحيادية المتفق عليها بشكل متبادل والتي تعمل لخدمة الصالح العام لجميع الأطراف في النظام الدولي. وتولي الأعراف التي توجِّه السلوك أهمية أكبر على نحو جوهري، وترى أن علاقات القوى بين الدول لا تتعلق كثيرًا بضرورة ضمان فرض الأعراف.

إليكم مثالًا على الفروق الناشئة عن اتباع أحد النوعين النموذجيين: لقد سعت الولايات المتحدة إلى معاقبة كوريا الشمالية لهجومها على شركة سوني بيكتشرز إنترتينمينت (Sony Pictures Entertainment) لتوجِه رسالة إلى جميع الدول أنه لا يمكن شن الهجمات الإلكترونية والإفلات من العقوبة (مثال على عرف مفترض). وعزفت الصين عن اتخاذ أي إجراءات ضد كوريا الشمالية عقب هذا الهجوم الإلكتروني، ويرجع ذلك جزئيًا إلى كون الاختراق أمرًا ثانويًا في نطاق علاقة أكثر تعقيدًا مع جارتها الصعبة. ومن المرجح أن يزيد احتمال سوء التفاهم إلى الحد الذي تظن فيه الولايات المتحدة أن الصين تتصرف على نحو متشائم (عندما تفضل النفوذ على القوانين)، وتظن الصين أن الولايات المتحدة تتصرف على نحو زائف (عندما تستخدم القوانين لإخفاء النفوذ).

إن فهم المسارات المحتملة للمفاوضات الناجحة بخصوص حفظ توازن العلاقة الإلكترونية بين الولايات المتحدة والصين يتطلب فهم المشكلات الأساسية

بين البلدين في مجال الفضاء الإلكتروني ومنظورهما تجاه تلك القضايا. يحفل تاريخ البلدين بالمشكلات بينهما بخصوص قضية الأمن الإلكتروني التي بدأت مع الاختراقات الصينية لمعامل وزارة الطاقة، والوكالات الحكومية، وكليات الدراسات العليا العسكرية، وشركات الدفاع، وكذلك استمرارها في تعريض شبكات الكثير من الشركات للخطر، وتحديدًا شركات الإعلام والشركات التي تجري أعمالها في الصين. أما الشكاوى الصينية فتجنح إلى أن تكون أقل تحديدًا؛ فهي تركز على هيمنة الولايات المتحدة على الفضاء الإلكتروني، خاصةً من خلال نجاح شركات البرمجيات الأمريكية وسيطرتها على مؤسسات توجيه وحوكمة الإنترنت. ومن الأمور التي قلما نوقشت على الساحة كانت مجموعات الاختراق الأمريكية للأنظمة الصينية، وهي قضية أبرزتها ادعاءات إدوارد سنودن (Edward Snowden) - المتعاقد السابق بوكالة الأمن القومي الأميركية. وأبدى المسؤولون الصينيون امتعاضهم من الشكاوى الأمريكية، ليس فقط بشأن الاختراقات الصينية بل وبشأن قمع الصين لحرية الإنترنت. يعتمد التقرير على مراجعتنا للمراجع الغربية ذات الصلة من المصادر غير المباشرة، وعلى تحليلنا للمؤلفات الصينية عن الأمن الفضائي، بالإضافة إلى نتائج المحاولات السابقة لإحراز تقدم في مجال الفضاء الإلكتروني من خلال المباحثات غير الرسمية بين مركز الدراسات الاستراتيجية والدولية، ومعاهد الصين للعلاقات الدولية المعاصرة، ومجموعة العمل الرسمية بين الولايات المتحدة والصين بشأن الفضاء الإلكتروني.

إضافةً إلى ذلك، في شهر مايو/آيار 2015، أجرينا مجموعة لقاءات مع محاورين رفيعي المستوى ومشاركين في الحوار من الصين. في بعض الحالات، نعرض مباشرةً ما سمعناه. وفي حالات أخرى، كنا نستخدم اللقاءات لننظر في مناهج ومواقف تفاوضية بديلة (مثل المباحثات الثنائية في مقابل المباحثات المتعددة الأطراف، المباحثات التزامنة في مقابل اللاتزامنية). وفيما يلي وجهات النظر الأولية.

تظل الصين مصرَّة بشكل رسمي على أنه لا يمكنها التفاوض بينما يبقى ضباط جيش التحرير الشعبي قيد الاتهام – لكنها مستعدة لإجراء مباحثات غير رسمية، بل أنها اقترحت حلولًا بديلة في حالات كثيرة. حتى أن أحد المحاورين رفيعي المستوى صرح أن "الصين لا تنوي السماح لمشكلة واحدة بإعاقة العلاقة الأشمل."[2] ويدل هذا الأمر على احتمال وجود حلول بديلة لرفض الصين للتفاوض، ما قد يفسر عرض الرئيس شي

[2] لقاء مع محاور صيني رفيع المستوى، بكين، مايو/آيار 2015.

لقبول صيغ الولايات المتحدة للأعراف التي تستهدف الفضاء الإلكتروني خلال اجتماع القمة الذي أجري في سبتمبر/ أيلول 2015.

ونادرًا ما حاول الصينيون الذين تحدثنا معهم، حتى ولو شكليًا، نفي قيام الصين بالتجسس الإلكتروني عمومًا أو بالتجسس الإلكتروني ذي الدوافع الاقتصادية على وجه الخصوص.

ويظن الصينيون الذين أجرينا معهم اللقاءات أن الولايات المتحدة قد عسكرت الفضاء الإلكتروني – ويصرون على أنهم لن يكونوا في آخر مراتب المنافسة كما يرونها (وإن كانت منافسة يندمون على الدخول فيها).

يرى الصينيون أن المباحثات حول الأمن الإلكتروني تعد بمثابة وسيلة لتهدئة غضب الولايات المتحدة أكثر منها لتحقيق شيء محدد. وفي المقابل، تؤكد الولايات المتحدة كثيرًا على استغلال هذه المباحثات لحل قضايا الأمن الإلكتروني.

لا يبدو أن للصينيين مجموعة مطالب معدة بشكل جيد – حتى أنهم لا يطالبون بتقليص حجم التجسس الإلكتروني الأمريكي – بحيث يكونون على استعداد للمطالبة بها مقابل أي وقف فعلي لأعمال التجسس الإلكتروني ذي الدوافع الاقتصادية (ناهيك عن جميع فئات التجسس الإلكتروني). لذا، يصعب اعتبار أن هذا التجسس الإلكتروني يدخل ضمن نطاق التجارة الإلكترونية.

لا يقبل الصينيون اقتراح الولايات المتحدة الذي يفيد بأنه يحق للدولة الرد على الهجمات الإلكترونية من جانب واحد باعتبار أن ذلك يخضع لقانون النزاع المسلح.

وكانت الفكرة التي تم طرحها هي تخلي الدولتين عن شن الهجمات على البنية التحتية الحيوية للدولة الأخرى. لقي هذا المقترح قبولًا معقولًا، حتى بعد اقترانه بشرط أن يتخلى الطرفان كذلك عن التجسس الإلكتروني على تلك الأهداف. ودارت نقطة الخلاف حول الإسناد. تظن الولايات المتحدة أنه يمكنها ضبط الصين أثناء غشها وتريد منهجية يُعترف بها بالغش بمجرد الكشف عنه كي تتبعها العواقب (وليست تلك مجرد عواقب تضر بالسمعة). وترى الصين أنه لا يمكنها ضبط غش الولايات المتحدة وتشعر بالقلق حيال أي اتفاق قد يضعهما في وضع غير مواتٍ لبعضهما البعض. هكذا، تتطلب أي اتفاقات جادة منهجية يثق بها الطرفان أو أي طريقة أخرى لزيادة ثقة الصين في قدراتها الإسنادية. يعد هذا تحديًا صعبًا، لكنه في رأينا ليس مستحيلًا، بشرط أن يقبل الطرفان العمل عليه بنية حسنة. و إذا شرعت كل من الولايات المتحدة والصين في هذا الأمر، نقدم مجموعة مبدئية من الأفكار التي يمكن البحث فيها حول كيفية المضي قدمًا في هذه المسألة. غير أنه لا يتضح إذا كانت الصين تطمح إلى التوصل إلى اتفاق في هذه القضية – أي التوصل إلى حل فعلي لها من خلال تحديد

أعراف يتم الاتفاق عليها، وتحظى بالاحترام فيما يتعلق بتحديد الأهداف في الفضاء الإلكتروني – بقدر رغبتها في التخلص ببساطة من هذه المشكلة. إذا كان هذا التقييم سليمًا، فلا يُرجح أن تجد الولايات المتحدة اتفاقيتها التي تفاوضت عليها مؤخرًا مع الصين حول الفضاء الإلكتروني مؤدية إلى تغيرات دائمة في إجراءات الصين بخصوص الفضاء الإلكتروني.

الاختصارات

CBM	معايير بناء الثقة
CICIR	معاهد الصين للعلاقات الدولية المعاصرة
CPC	الحزب الشيوعي الصيني
CSIS	مركز الدراسات الاستراتيجية والدولية
DoD	وزارة الدفاع الأمريكية
EMCE	التجسس الإلكتروني ذو الدوافع الاقتصادية
ICANN	هيئة الإنترنت للأسماء والأرقام المخصصة
IP	بروتوكول الإنترنت
ITU	الاتحاد الدولي للاتصالات
LOAC	قانون النزاع المسلح
NSA	وكالة الأمن القومي
OPM	مكتب إدارة شؤون الموظفين
PLA	جيش التحرير الشعبي
PRC	جمهورية الصين الشعبية
S&ED	الحوار الاستراتيجي والاقتصادي
SCO	منظمة شنغهاي للتعاون
TRIPS	الجوانب المتصلة بالتجارة من حقوق الملكية الفكرية
UN	الأمم المتحدة
USCYBERCOM	القيادة الإلكترونية الأمريكية

"مشكلة الفضاء الإلكتروني" في العلاقات بين الولايات المتحدة والصين

منذ تأسيس جمهورية الصين الشعبية في عام 1949، اتسمت العلاقة بين الولايات المتحدة والصين بقدر كبير من الصراع والتحدي والريبة الاستراتيجية. وقد زاد ثقل التوترات التي تقسم الطرفين في السنوات الأخيرة، وفق ما جاء في ملاحظات كبار الخبراء من كل من الولايات المتحدة والصين.[1] وفي الواقع، بحلول منتصف عام 2015، أشار عدة خبراء أمريكيين مختصين بالشأن الصيني إلى التدهور السريع في العلاقات الثنائية، إلى الحد الذي وصف فيه أحد هؤلاء الخبراء العلاقة بين الولايات المتحدة والصين بأنها دخلت في "نقطة تحول"، وكان هناك إنذار آخر بأن "العلاقات بين الولايات المتحدة والصين باتت الآن تسيطر عليها المنافسة الشاملة" ونادى مسؤولان حكوميان سابقان رفيعا المستوى "بإعادة النظر في الاستراتيجية الأمريكية الشاملة تجاه الصين" وذلك من أجل موازنة قوة الصين الصاعدة بشكل أفضل.[2]

---

[1] Kenneth N. Lieberthal and Wang Jisi, *Addressing U.S.-China Strategic Distrust*, Washington, D.C.: مركز جون إل ثورنتون (الصين)، مؤسسة بروكينغز، 2012. انظر أيضًا الدراسة المفصلة للعلاقات بين الولايات المتحدة والصين في مجال الفضاء الإلكتروني التي أجراها جون ليندسي Jon Lindsay، وتاي مينغ Tai Ming، وديريك ريفيرون Derek Reveron: كتاب لجون آر ليندسي، وتاي مينغ شونغ وديريك ريفيرون بعنوان الصين والأمن الإلكتروني: التجسس والاستراتيجيات والسياسة في الفضاء الرقمي، أكسفورد مطابع أكسفورد الجامعية، Oxford University Press, 2015.

[2] مقال ديفيد إم. لامتون David M. Lampton بعنوان "وصلنا إلى نقطة تحول في العلاقات بين الولايات المتحدة والصين،" *US-China Perception Monitor*، 11 مايو/آيار 2015؛ ومقال ديفيد شامبو David Shambaugh بعنوان "في نقطة تحول كبيرة، دخلت الصين والولايات المتحدة الآن في منافسة شاملة،" *South China Morning Post* 14 يونيو/حزيران 2015؛ وروبرت دي. بلاكويل Robert D. Blackwill وآشلي جي تيليس (Ashley J. Tellis) مراجعة استراتيجية الولايات المتحدة الكبرى تجاه الصين *Revising U.S. Grand Strategy Toward China*]، واشنطن العاصمة: مجلس العلاقات الخارجية، تقرير المجلس الخاص رقم 72، مايو/آيار 2015.

وترى الصين بدورها اضطرابًا شديدًا في علاقاتها بالولايات المتحدة وتصف إعادة التوازن الأمريكي لمنطقة آسيا والمحيط الهادئ بأنه "أسوأ حالًا من الاحتواء الأمريكي للموقف،" وتدعي أن التوتر بين الصين وجاراتها في السنوات الأخيرة نابع من جهود الولايات المتحدة في تشجيع الأطراف الفاعلة الإقليمية أو التلاعب بها كي تتخذ وضع المواجهة مع بكين.[3] وبالفعل بدت الدهشة على قادة الصين بعد استمرار الجهات الفاعلة الإقليمية في الترحيب بالولايات المتحدة، بعد توقعاتهم بأن الوزن الاقتصادي المتنامي للصين سيؤدي تلقائيًا إلى انهيار نظام التحالف المتمركز حول الولايات المتحدة.[4] كما تشعر الصين بالقلق تجاه جهود الولايات المتحدة لدعم اليابان بخصوص جزر سينكاكو ودعوات الولايات المتحدة لوقف البناء في بحر الصين الجنوبي رغم استمرار انخراطها في ممارسات حرية الملاحة. ويُنظر إلى دعم الولايات المتحدة المستمر لمبادئ حقوق الإنسان وانتقادها المتواصل للصين لعدم استيفائها لتلك المعايير الدولية للسلوك المتحضر على أنه تهديد لنظام الحكم من شأنه أن يؤدي إلى "ثورة ملونة" لربما تطيح بالحزب الشيوعي الصيني.

وللأسف، ينعكس هذا النوع من التوترات المتصاعدة على الفضاء الإلكتروني بقدر ما ينعكس على العلاقات في العالم المادي، وذلك وفق منظور الطرفين. وفي الواقع، من بين جميع المجالات التي اضطربت فيها العلاقة بين الطرفين، كان مجال الفضاء الإلكتروني أكثرها إثارة للخلاف. وفي حين شرع الجانبان في بدء مباحثات ثنائية رسمية بخصوص الفضاء الإلكتروني في عام 2013، إلا أن الصين أوقفت هذه المباحثات في 2014. كما أن غياب الالتزام الجاد بالقواعد التي تحكم الأنشطة في هذا المجال الجديد وإرساء قواعد الطريق فيما يتعلق بالفضاء الإلكتروني يعرض العلاقة الثنائية، والأمن والاستقرار الإقليميين، والنظام العالمي لخطر كبير.

وجاء هذا التقرير كنتيجة لغياب الحوار الرسمي وليستكشف خيارات السياسة الأمريكية لإدارة العلاقات مع الصين بشأن هذا الموضوع السياسي الشائك. وينظر التقرير في مسألتين أساسيتين: هل يمكن للولايات المتحدة والصين العودة إلى

---

[3] لايل جيه. غولدستين (Lyle J. Goldstein)، "كيف ترى الصين التحركات الأمريكية في آسيا: أسوأ حالاً من احتواء الموقف،" المصلحة القومية National Interest، 29 أكتوبر/تشرين الأول 2014؛ آندرو جيه نيثان (Andrew J. Nathan) وأندرو سكوبيل (Andrew Scobell)، "كيف ترى الصين أمريكا: مجموعة مخاوف بكين،" الشؤون الخارجية *Foreign Affairs*، سبتمبر/أكتوبر (أيلول/تشرين الأول) 2012.

[4] مقال بعنوان "آراء الصين المتغيرة تجاه التحالف الكوري الأمريكي بين 2012- 1953،" للكاتب جاي هو شونغ في دورية الصين المعاصرة، العدد 23، رقم 87، ص 442-425.

المفاوضات الرسمية المجدية بشأن القواعد والقوانين الخاصة بالفضاء الإلكتروني؟ وفي تلك الحالة، ما هي أكثر المجالات التي من المرجح أن يتم التوصل فيها إلى اتفاق، وما الأمور التي يمكن استبدالها بأخرى؟

في جيل سابق، عندما ظهرت الأسلحة النووية التي تحملها الصواريخ الباليستية العابرة للقارات التي توجهها أنظمة استهداف واستطلاع فضائية في السماء، لم تسنح الفرصة للخبراء الأمريكين للتواصل مباشرة مع نظرائهم السوفيت لفهم طريقة تعرفهم على المشكلات المرتبطة بالردع، أو أفكارهم بشأن المعايير الدولية، أو تقييماتهم لوسائل إرسال الإشارات أو رؤاهم حول أفضل طريقة لتناول التعاون والتهدئة. تغلب المبالغة وعدم الدقة على المقارنات التي تجرى بين قضايا الفضاء الإلكتروني والقضايا النووية، إلا أن أحد القواسم المشتركة بينها هي حقيقة أن إدراك مواطن الضعف في الساحتين كان ولا يزال له عظيم الأثر السلبي على الاستقرار الثنائي بين القوتين الدوليتين البارزتين. لكن لحسن الحظ، وبعكس ما دار في الحرب الباردة، تمكن الباحثون في الولايات المتحدة والصين من تبادل وجهات النظر بشكل دوري بشأن قضايا الساعة الهامة ما مهد الطريق أمام تعزيز التفاهم ودقة تقييم التحديات الأمنية المرتبطة بإدارة علاقتهما الثنائية.

ورغم هذه الفرص لتبادل المعلومات الخاصة بالأمن الإلكتروني، إلا أنه لا تزال آفاق التعاون حول الفضاء الإلكتروني غير واعدة حتى اليوم. ولنعرض نهجين للتعاون (لكننا لا نؤيدهما بالضرورة)، نود الإشارة إلى اقتراح كارل راوشر Karl Rauscher ويونغلين جو Yonglin Zhou من معهد إيست-ويست EastWest Institute بعنوان "مكافحة التطفل من أجل تعزيز الثقة،" بينما اقترح كل من كينيث ليبيرثول Kenneth Lieberthal وبيتر دابليو سينغر Peter W. Singer من معهد بروكينغز مجموعة تدابير تعاونية شاملة.[5]

في السنوات التالية لنشر تلك الدراسات، لم تزد العلاقات بين الدولتين إلا سوءًا بسبب قضية الفضاء الإلكتروني. وفي هذا الشأن تشير خبيرة الفضاء الإلكتروني الصينية إيمي شانغ Amy Chang إلى "استمرار الدولتين في مواجهة العقبات الكبيرة

[5] مقال للكاتبين كارل فريدريك روشر وجو يولين بعنوان مكافحة الاحتيال من أجل بناء الثقة، نيويورك: معهد إيست ويست، 2011؛ للكاتبين كينيث ليبيرثول وبيتر دابليو سينغر، بعنوان الفضاء الإلكتروني والعلاقات بين الولايات المتحدة والصين، واشنطن العاصمة: مبادرة الدفاع للقرن الحادي والعشرين، مركز جون إل. ثورنتون (الصين)، مؤسسة بروكينغز، فبراير/شباط 2012.

أمام بناء الجهود التعاونية وتحسين التفاهم المشترك" بشأن قضية الفضاء الإلكتروني إلى الحد الذي "تحولت فيه العلاقات إلى انعدام شبه كامل للثقة في دوافع وإجراءات ومخططات كل منهما، ما أثر على الجوانب الأخرى للعلاقات الثنائية." وتستطرد شانغ وتؤكد على التالي:

> تتحرك سياسات الأمن الإلكتروني بدافع هدف الحزب الشيوعي الصيني في الحفاظ على قوته الحاكمة...[عبر ضمان] الاستقرار المحلي، وسلامة الأراضي والتحديث والنمو الاقتصادي مع التأهب، في الوقت نفسه، لاحتمالية نشوب نزاع إلكتروني عسكري في المستقبل.[6]

وبالمثل، يلاحظ الخبير بالفضاء الإلكتروني جيمس لويس (James Lewis) أن "الخلافات السياسية والمنافسة على النفوذ الإقليمي والرغبة العارمة في تقويض وضع الولايات المتحدة في آسيا" هي السمة الغالبة على سياسات الصين تجاه الأمن الفضائي، ما يعرقل إمكانيات التعاون بين الولايات المتحدة والصين.[7] وتتفق وجهة نظر شانغ مع هذه الرؤية وتلاحظ "قلة الحوافز الموجودة أمام الصين لتتعاون بجدية مع الدول المتقدمة بشأن الحد من سرقة الملكية الفكرية أو الجرائم الإلكترونية."[8]

في الوقت الذي يرى فيه الكثير من الخبراء الأمريكيين آمالًا ضئيلة أمام التعاون القوي في المستقبل القريب، يؤكد عدد من المراقبين الصينيين - من المسؤولين والخبراء بمراكز الأبحاث والباحثين - على أهمية إيجاد حل لهذه القضية، إما عبر المفاوضات الثنائية أو الاتفاقيات متعددة الأطراف أو كليهما. فمقترح الحكومة الصينية، على سبيل المثال، الذي يحمل عنوان "مدونة قواعد السلوك الدولية لأمن المعلومات"، والذي تم تقديمه إلى الأمم المتحدة في فبراير/شباط 2014، يؤكد على غياب "قوانين شاملة لنقل المعلومات" ويسلط الضوء على الرغبة في "وجود عملية واضحة

---

[6] إيمي شانغ (Amy Chang)، حالة التأهب: استراتيجية الأمن الإلكتروني للصين، واشنطن العاصمة: مركز الأمن الأمريكي الحديث، ديسمبر/كانون الأول 2015، صفحة 7 و10.

[7] جوليا أوه (Julia Oh)، "التعاون الإلكتروني في شمال شرق آسيا: مقابلة مع جيمس لويس (James Lewis)،" المكتب القومي للأبحاث الأسيوية، أسئلة وأجوبة في السياسات، 17 مارس/آذار 2015.

[8] Chang, 2015, p. 22.

ومستدامة للحصول على إجماع دولي" بخصوص قضايا الفضاء الإلكتروني.[9] وعلى نحو مماثل، قال ما شين مينغ (Ma Xinming) نائب المدير العام لإدارة المعاهدات والقوانين بوزارة الخارجية بالصين، في خطابه في واشنطن في ديسمبر/كانون الأول 2014، إنه يتعين على الولايات المتحدة والصين العمل معًا من أجل "المساهمة في تأسيس النظام الأساسي للفضاء الإلكتروني وقوانينه" وقدم مقترحًا صينيًا باستخدام ميثاق الأمم المتحدة في "تحديد المبادئ الأساسية للأنشطة الإلكترونية."[10] نشرت صحيفة تشاينا ديلي *China Daily* الرسمية الصادرة باللغة الإنجليزية مقالات عديدة في الأعوام الماضية، واستند أكثرها إلى لقاءات مع مسؤولين صينيين ومحللين بمراكز الأبحاث، حيث كانت تهدف إلى إرسال الرسالة المطمئنة بأن الصين "مستعدة للعمل الجماعي بشأن الأمن الإلكتروني."[11]

أكد أساتذة جامعيون صينيون على تلك الآراء، مثل شين ييه (Shen Yi) من جامعة فودان، وأقروا بضرورة توصل الطرفين إلى "اتفاق بخصوص قواعد وقوانين الفضاء الإلكتروني من أجل التخلص من الأثر السلبي لحالة الشك."[12] وعلى النحو نفسه، أكد دونغ كينغلينغ (Dong Qingling) الأستاذ بجامعة الأعمال والاقتصاد الدولية في بكين أنه "يتعين على الصين والولايات المتحدة تسوية النزاعات وتأسيس أواصر الثقة في مجال الفضاء الإلكتروني."[13] ولربما يرجع السبب في هذا – وفق رأي ييه وينلي (Yi Wenli)، الباحث المساعد في مركز أبحاث تكنولوجيا المعلومات القومي – إلى أن تزايد الشك والريبة بين طرفي المحيط الهادئ يقلص مجال الحوار في شأن الأمن

---

[9] "مدونة قواعد السلوك الدولية لأمن المعلومات – منظور الصين لبناء فضاء إلكتروني سلمي وآمن ومفتوح وتعاوني"، وهو بيان أعد لمؤتمر منعقد في جنيف بضيافة معهد الأمم المتحدة لبحوث نزع السلاح، 10 فبراير/شباط 2014.

[10] ما شين مينغ (Ma Xinming)، "ما هو نوع نظام الإنترنت التي نحتاج إليه؟" المجلة الدورية الصينية للقانون الدولي، الطبعة 14، رقم 2، 2015، ص. 403-399.

[11] انظر أيضًا، على سبيل المثال، مقال وانغ شو (Wang Xu) بعنوان "الصين مستعدة للتعاون بخصوص الأمن الإلكتروني"، الصين يوميًا *China Daily*، 18 سبتمبر/أيلول 2015.

[12] مقال شين ييه (Shen Yi) بعنوان "الاستجابة لتحدي استراتيجية حرية الإنترنت المثيرة للإزعاج: تحليل التنافس والتعاون الصيني الأمريكي في مجال الفضاء الإلكتروني العالمي، Xi Zhong-Mei zai quanqiu xinxi kongjian de jingzheng yu hezuo"], *World Economics and Politics* [*Shijie jingji yu zhengzhi*], No. 2, 2012, pp. 69–79

[13] دراسة بعنوان "بناء الثقة من أجل الأمن الإلكتروني بين الصين والولايات المتحدة،" للكاتب دونغ كينغلينغ المنشورة بـ الدراسات الدولية بالصين، يوليو(تموز)/أغسطس (آب) 2014، ص 68-57.

الإلكتروني، حتى في مجالات المصلحة المشتركة، مما يشير إلى إمكانية إغلاق الباب أمام فرصة التفاوض على القواعد والقوانين.[14]

تتضح ضرورة المفاوضات المتواصلة والهادفة ذات الصفة الرسمية والمنتظمة في حالة رغبة الطرفين في تجنب الشك والأنشطة غير المرغوب بها في الفضاء الإلكتروني التي توجه علاقتهما نحو اتجاه سلبي. وبالنسبة لواضعي السياسات في الدولتين الواقعتين على جانبي المحيط الهادئ، يعد الفضاء الإلكتروني مجالاً جديدًا نسبيًا وسريع التطور، حيث تمحو التغيرات التكنولوجية التي توجهها الأسواق والأمن القومي الفوائد الاستراتيجية لتعزيز الاستقرار في المسافة التي تفصل بين الولايات المتحدة والصين. تتمحور خلافات الطرفين على الفضاء الإلكتروني حول خمس نقاط وهي: (1) شرعية استخدام الفضاء الإلكتروني للتجسس الاقتصادي أو الصناعي؛ (2) استخدامات الأمن القومي للفضاء الإلكتروني في أشكال أكثر تقليدية للتجسس وجمع المعلومات؛ (3) استخدام الفضاء الإلكتروني مستقبلاً في العمليات العسكرية؛ (4) الحقوق المفترضة للدول للتحكم في الوصول إلى المعلومات داخل حدودها (تشير الصين إلى هذا المبدأ باسم السيادة الإلكترونية)؛ (5) مسألة كيفية إدارة القواعد والأعراف الدولية والبنية الفعلية للإنترنت.

من منظور الولايات المتحدة، تمثلت الشكوى الأساسية في اختراقات الصين المتعددة والمتكررة لشبكات الشركات لسرقة الملكية الفكرية أو المعلومات التجارية الخاصة. في حين أن القيمة الإجمالية لهذه السرقة غير معروفة، يقدر أحد المراقبين وهو العقيد (المتقاعد) كيث أليكساندر (Keith Alexander)،[15] الرئيس السابق لوكالة الأمن القومي، تكلفة سرقة الصين للملكيات الفكرية من الولايات المتحدة بحوالي 300 مليار دولار سنويًا.[16] بعد سنوات من إبلاغ الولايات المتحدة الصين سرًا بوجهة

---

[14] مقال للكاتب بيه وينلي بعنوان "التباين بين الصين والولايات المتحدة والطريق نحو التعاون في الفضاء الإلكتروني/["Zhong-Mei zai Wangluo Kongjian de Fenqi yu Hezuo Lujing"]، العلاقات الدولية المعاصرة/[*Xiandai Guoji Guanxi*]، العدد 22، رقم 4، يوليو(تموز)/أغسطس (آب) 2012، ص 141-124.

[15] مقال للكاتب جيم غارامون بعنوان "رئيس شركة سايبركوم Cybercom يوضح تفاصيل حماية الفضاء الإلكتروني،" خدمات النشر للقوات الأمريكية، 23 سبتمبر/أيلول 2010.

[16] تقديرات مركز الدراسات الاستراتيجية والدولية (CSIS) لا تزيد عن عُشر هذه التقديرات (راجع تقرير CSIS بعنوان الأثر الاقتصادي للجرائم الإلكترونية والتجسس الإلكتروني، يوليو/تموز 2013)، ويمكن إجراء دراسة حالة بناءً على المنطق الاقتصادي وطبيعة التنمية الاقتصادية التي تثبت أن إجمالي الضرر الذي لحق بالولايات المتحدة يقل أيضًا عن هذه التقديرات.

نظرها في أن هذه الاختراقات لا تعد استخدامًا شرعيًا للأجهزة العسكرية والمخابراتية الخاصة بها - لكن دون فائدة، في عام 2014، اتخذت الولايات المتحدة خطوتها التالية بإدانة خمسة ضباط في الخدمة من جيش التحرير الشعبي في الصين بتهمة القرصنة، وهي خطوة دفعت الصين إلى تعليق مشاركتها في مجموعة العمل بين الولايات المتحدة والصين بشأن الفضاء الإلكتروني.[17]

وكانت المسألة الثانية التي تدعو للقلق هي الاختراق المتزايد لأنظمة الولايات المتحدة عبر الفضاء الإلكتروني لأغراض تجسس تقليدية تتعلق بالأمن القومي. وحتى يومنا هذا، لم تعلن الإدارات الأمريكية أن تلك الأنشطة تنتهك أي قوانين تتعلق بالاستخدام الملائم للفضاء الإلكتروني لأغراض التجسس. غير أن وتيرة وضخامة الاختراقات التي تم الكشف عنها مؤخرًا في أنظمة الحواسيب الأمريكية، وتشمل تحديدًا الكشف الذي تم في يونيو/حزيران 2015 عن اختراق مكتب إدارة شؤون الموظفين، دفع ببعض المحللين إلى الحديث عن ضرورة توضيح الظروف التي ينبغي في ظلها "توسيع رقعة مفهوم ما يُعرف 'بالهجوم الإلكتروني' ليشمل الاضطرابات الضخمة' التي رغم ذلك لا تسبب الأذى المادي للدولة المتضررة."[18] واقترح بعض المحللين وجود علاقة بين اختراقات شركات القطاع الخاص، مثل شركة أنثيم (Anthem) للخدمات الطبية، والهجمات على الهيئات الحكومية الأمريكية مثل مكتب إدارة شؤون الموظفين ووزارة الداخلية الأمريكية (التي تعرضت للقرصنة في أواخر عام 2014)، وذلك غالبًا بغرض تجميع قواعد بيانات هائلة للموظفين المدنيين الأمريكيين وجهات اتصالهم أو أقاربهم بالصين من أجل إمكانية مراقبتهم أو تجنيدهم.[19]

---

[17] مقال للكاتبين مايكل إس شميت وديفيد إي سانغر بعنوان "خمس ضباط بالجيش الصيني يواجهون اتهامات بشن هجمات إلكترونية،" المنشور بصيحفة نيويرك تايمز، 19 مايو/آيار 2014؛ مقال "الصين تطالب بإسقاط الاتهامات" للكاتبين شين وييهوا ولي شياوكون المنشور في صحيفة تشاينا ديلي 22 مايو/آيار 2014.

[18] مقال للكاتبة آشلي ديكس (Ashley Deeks) بعنوان "تالين تتكرر للمرة الثانية ونظرة للصين من عملية تالين،" مدونةلوفير، 31 مايو/أيار 2015.

[19] مقال للكاتبة إلين ناكاشيما (Ellen Nakashima) بعنوان "شركة أمن تتوصل لوجود علاقة بين الصين واختراق شركة أنثيم،" المنشور بصحيفة واشنطن بوست *Washington Post* 27 فبراير/شباط 2015a؛ ومقال للكاتبة إلين ناكاشيما (Ellen Nakashima) بعنوان "باستخدام سلسلة من الهجمات الشرسة، الصين تنشئ قاعدة بيانات بالأمريكيين،"واشنطن بوست *Washington Post* 5 يونيو/حزيران 2015c؛ ومقال للكاتب ستيفن براون بعنوان "مسؤول يؤكد بأن الاختراقات أضرت بأكثر من 25 ألف موظف بوكالة الأمن القومي،" المنشور بصحيفة واشنطن بوست *Washington Post* 23 أغسطس/آب 2014.

على صعيد آخر، تشعر الولايات المتحدة بالقلق حيال مسألة ثالثة وهي احتمال أن تكون الصين مستعدة لهدم البنى التحتية الأساسية للولايات المتحدة في حالة نشوب أزمة. وشهد مدير وكالة الأمن القومي الحالي، الأدميرال مايكل إس. روجرز (Michael S. Rogers)، على تهديد الصين لشبكة الكهرباء الأمريكية عبر الاختراقات التي خلّفت برمجيات مغروسة (يُشار إليها عادةً باسم الأبواب الخلفية) التي يمكن استخدامها للتدمير الشامل في حالة نشوب أزمة.[20] كما أن هناك مخاوف تجاه احتمالية أن تسيء كل من الولايات المتحدة والصين قراءة تصرفات وإشارات بعضهما البعض بخصوص الفضاء الإلكتروني في حالة الأزمات مما قد يؤدي إلى التصعيد. وبسبب طبيعة الفضاء الإلكتروني شبه المبهمة، من المحتمل أيضًا أن يسيء الطرفان فهم إشارات بعضهما البعض أو أن يظن الطرفان خطأ أن التصرفات التي يتخذها أي طرف ثالث على أنها صادرة من أحد منهما، خاصةً إذا قام طرف خبيث أو يعمل لمصلحته الذاتية بتوجيه الهجمات على الطرف الآخر عبر خوادم أمريكية أو صينية أثناء فترة عصيبة نسبيًا في العلاقات الثنائية. تشعر الولايات المتحدة والصين بالقلق تجاه الطريقة التي سيستخدم بها الطرف الآخر الهجمات الإلكترونية في حالة الحرب ومخاطر التصعيد التي قد يتسبب فيها مثل هذا الاستخدام.

كذلك، أعربت الولايات المتحدة عن مخاوفها تجاه معاملة الصين للشركات الأمريكية بذريعة حماية أمنها.[21]

وأخيرًا، انتقدت الولايات المتحدة الصين لقمعها حرية التعبير على الإنترنت. ولربما تصبح أنماط السلوك هي موضوع المفاوضات بين الولايات المتحدة والصين في المستقبل، مثل الحادثة التي وقعت أوائل عام 2015 حيث عملت هجمات الإغراق بسيل من البيانات (ما يعرف بحجب خدمة الموزع) على تعطيل موقع مشاركة البرمجيات GiTHub.[22]

---

[20] مقال كين ديلانيان (Ken Dilanian) بعنوان "مدير وكالة الأمن القومي يقول: بإمكان الصين تدمير شبكة كهرباء الولايات المتحدة،" المنشور بالأسوشيتد بريس Associated Press، 20 نوفمبر/تشرين الثاني 2014.

[21] مقال للكاتب بول موزور "القوانين الجديدة بالصين تثير حفيظة شركات التكنولوجيا الغربية بالصين،" المنشور بصحيفة نيويورك تايمز *New York Times* بتاريخ 29 يناير/كانون الثاني 2015. أجلت الصين تطبيق هذه القوانين منذ ذلك الحين.

[22] مقال لنيكول بيرلورث بعنوان "الصين تستخدم سلاح جديد قوي لتقييد الإنترنت، وفق التقارير" المنشور بصحيفة نيويورك تايمز *New York Times* 10 أبريل/نيسان 2015؛ ومقال بعنوان "الصين خلف الهجوم الإلكتروني على المواقع الإلكترونية الأمريكية، وفق التقارير" المنشور بصحيفة سان فرانسيسكو كرونيكل *San Francisco Chronicle* 8 مايو/آيار 2015.

أما بالنسبة للصين، فإنها تشجب اتهامات الولايات المتحدة لها بالقرصنة وتدعي بأنها هي ضحية للهجمات الإلكترونية الصادرة من الولايات المتحدة. ويشكو المسؤولون والمحللون الصينيون من القيود المفروضة من الولايات المتحدة على دخول شركات الاتصالات الصينية إلى الأسواق مثل شركة هواوي (Huawei) و شركة زد.تي.إي (ZTE Corporation). كما يستنكر المحللون الصينيون تمويل الولايات المتحدة لتكنولوجيا التحايل على الرقابة على الإنترنت ويؤيدون حق الدول في الرقابة على المعلومات المتاحة للأفراد داخل حدودها (وهو مفهوم يُعرف بـالسيادة الإكترونية). وكذلك يدين المراقبون الصينيون ما يصفونه "بالهيمنة" الأمريكية على الإنترنت ويشيرون إلى أن العديد من الموجهات والخوادم وكذلك البرامج المستخدمة لدعم البنية التحتية للإنترنت في الصين إما تصنعها أو تتحكم فيها الشركات الأمريكية.[23] ويشير المحللون الآخرون ومنهم جيانغ شونغ (Jiang Chong) مدير مركز أبحاث الأمن الاقتصادي التابع لمعاهد الصين للعلاقات الدولية المعاصرة إلى "المزايا الاحتكارية"[*longduan youshi*] للولايات المتحدة في مجالات المعايير التكنولوجية، والمرافق الأساسية، وموارد الملكية الفكرية، وتمييز اسم النطاق ويؤكد أن تلك المجالات تشكل نوعًا من "السيادة الإلكترونية"[*wangluo zhudaoquan*] أو حتى "الهيمنة الإلكترونية"[*wangluo baquan*].[24] وأخيرًا، ينادي العديد من المحللين الصينيين بأن ينتقل نظام اسم النطاق Domain Name System المستخدم لإنشاء مواقع الويب على الإنترنت - الذي تديره حاليًا شركة الإنترنت للأسماء والأرقام المخصصة واختصارها (آيكان) ICANN- إلى منظمة عالمية مثل الأمم المتحدة (ما يمنح الصين صوتًا في الإدارة العالمية للإنترنت).[25]

---

[23] انظر، على سبيل المثال مقالة جيو جي (Guo Ji) بعنوان "ينبغي ألا يتحول الفضاء الإلكتروني إلى وسيلة جديدة للهيمنة الأمريكية: لنبدأ من تفسير لواقعة بريزم-جيت" : [Wangluo buying chengwei Meiguo baquan xin gongju Cong 'Lingjingmen' shijian shuokai qu]," *Seeking Truth* [*Qiu Shi*], No. 15, 2013, pp. 57–59.

[24] Jiang Chong, "Cyber: The Invisible New Battlefront [Wangluo: Kanbujian de xin zhanxian]/" مقال للكاتب جيانغ شونغ بعنوان "الفضاء الإلكتروني: ساحة المعركة الجديدة الخفية/[Wangluo البحث عن الحقيقة/[*Qiu Shi*]، رقم 13، 2010، ص 55-53.

[25] مقال للكاتب يانغ جيان (Yang Jian)، بعنوان "طبيعة التناقضات في السياقات لاستخدام أمريكا لجملة 'المنهج العالمي للفضاء الإلكتروني [Meiguo 'Wangluo kongjian quanqiu gongyu shuo' de yujing maodun jiqi benzhi] المنشور بالاستبيان الدولي [*Guoji guancha*] *International Survey*، رقم 1، 2013، ص 52-46؛ ومقال للكاتب لو شوان ينغ (Lu Chuanying) بعنوان "محاولة لتحليل معضلة الحوكمة الدولية في الفضاء الإلكتروني/[Shixi dangqian

وحتى وقت قريب، كانت انتقادات الولايات المتحدة للصين أغلبها غير مباشرة، إذ كانت تشير ضمنيًا إلى الأنشطة الصينية دون تحديد الصين بعينها.[26] وقدمت نسخة تقرير شركة مانديانت (Mandiant) الصادرة في أوائل عام 2013 بشأن شركة قرصنة صينية تابعة لجيش التحرير الشعبي الصيني تبريرًا لإشارة المسؤولين الأمريكيين للصين دون سواها علانيةً.[27] وبعد مرور عدة أشهر، كانت قضية التجسس الإلكتروني الصيني على رأس مواضيع القمة بين الرئيس باراك أوباما والرئيس شي جين بينغ (التي عقدت في منتجع ساني لاندز في رانشو ميراج بولاية كاليفورنيا). تمثل هذه القمة ارتقاءً لمستوى المباحثات الرسمية بشأن الفضاء الإلكتروني بين البلدين. وعكست هذه المفاوضات رغبة الدولتين في التباحث، لكن مع استمرار الصين في نفي ممارستها لأي أنشطة تجسس إلكتروني، لم تثمر تلك المباحثات إلا قليلًا. ثم في مايو/آيار 2014، عندما فاجأت الولايات المتحدة الصين بإدانتها لخمسة ضباط بجيش التحرير الشعبي الصيني بسبب قيامهم بالتجسس الإلكتروني، ردت الصين بتعليق مفاوضات مجموعة العمل الرسمية بشأن الفضاء الإلكتروني. ولم تُعقد بعدها أي جلسات لمجموعة العمل بشأن الفضاء الإلكتروني، إلا أن الجانب الأمريكي أثار قضية الفضاء الإلكتروني مع الصين في جلسات قمة الحوار الاستراتيجي والاقتصادي (S&ED) التي عقدت في صيف 2015. ومباشرةً قبل قمة الصين والولايات المتحدة في سبتمبر/

---

wangluo kongjian quanqiu zhili kunjing]،" المنشور بدورية العلاقات الدولية المعاصرة *Contemporary* [*Xiandai guoji guanxi*] *International Relations* رقم 11، 2013، ص 54-48؛ ومقال للكتاب يانغ لي (Jiang Li) وجانغ شياولان (Zhang Xiaolan) وشو فيبياو (Xu Feibiao) بعنوان "معضلة الأمن الإلكتروني الدولية وطريقة حلها [uoji wangluo anquan hezuo de kunjing yu chulu] المنشور بدورية العلاقات الدولية المعاصرة *Contemporary* [*Xiandai guoji guanxi*] *International Relations* رقم 9، 2013، ص 58-52. يانغ (Yang) ولو (Lu) باحثان في معاهد شنغهاي للدراسات الدولية؛ أما جيانغ (Jiang) وجانغ (Zhang) وشو (Xu) فهم باحثون في معاهد الصين للعلاقات الدولية المعاصرة (CICIR) في بكين.

[26] وكان أبرز استثناء هو انتقاد الصين في يناير/كانون الثاني 2010 بسبب معاملتها لشركة جوجل Google: وهذا يعني أن اختراق القراصنة الصينيين لشبكة جوجل و رقابة الصين على محتويات جوجل دفع بشركة جوجل إلى الانتقال من الصين إلى هونغ كونغ. انتقدت وزيرة الخارجية الأمريكية هيلاري كلينتون (Hillary Clinton) سلوك الصين تجاه جوجل في أوائل 2010 وطالبت بتفسير. انظر إلى مقال سيسيليا كانغ (Cecilia Kang) بعنوان "هيلاري كلينتون تطالب بحرية الإنترنت، وتطالب الصين في التحقيق في الهجوم على جوجل،" المنشور بواشنطن بوست، 22 يناير/كانون الثاني 2010.

[27] Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*, March 2013. لاحظ وجود مناقشات مباشرة في موضوع التجسس الصيني قبل إصدار التقرير، مثل المباحثات الاستراتيجية والاقتصادية التي وقعت في وقت سابق. وأشارت وزيرة الخارجية كلينتون إلى تعرض شركة جوجل للقرصنة من الصين في عام 2010.

أيلول 2015، قام رئيس لجنة الشؤون السياسية والقانونية بالحزب الشيوعي الصيني مينغ جيانزو (Meng Jianzhu) بزيارة الولايات المتحدة للتنسيق بشأن قضايا الفضاء الإلكتروني بعد أن أشارت التسريبات الإعلامية إلى أن الولايات المتحدة تخطط لفرض عقوبات اقتصادية على الشركات الصينية، ما من شأنه أن يعيق مسار قمة الرئيسين شي وأوباما.[28] وفي أعقاب زيارة مينغ، أعلن الطرفان عن توصلهما لاتفاق في القمة المنعقدة بشأن الأمن الإلكتروني، الأمر الذي أثار دهشة العديد من المحللين، وحدد الاتفاق أنواعًا معينة من التجسس التجاري بأنه غير مقبول، وتعهد الطرفان بزيادة التعاون الثنائي. رغم أنها كانت خطوة أولى ناجحة، يؤكد الكثير من المحللين على أنها تستلزم متابعة كبيرة لكي تكون مجدية.[29]

الغرض من التقرير ومنهجيته

كان الدافع وراء هذا التقرير هو الرغبة في التوصل لفهم أفضل للعلاقات بين الولايات المتحدة والصين بخصوص قضية الأمن الإلكتروني الحرجة. للولايات المتحدة ثلاثة خيارات سياسية أساسية عند التعامل مع الصين بخصوص هذه القضية: التركيز مبدئيًا على تقوية الدفاعات الإلكترونية الأمريكية أو محاولة إقناع الصين بتغيير سلوكها عبر الوسائل الدبلوماسية أو المفاوضات أو كليهما بشأن القواعد والسلوكيات، أو إجبار الصين على تغيير ممارساتها الإلكترونية قسرًا.[30]

يعد تعزيز دفاعات الولايات المتحدة خيارًا سياسيًا رئيسيًا، كما أقر الباحثون ومحللو السياسات.[31] هذا الأمر واقع منذ سنين عدة، وينبغي بالتأكيد استمراره.

---

[28] مقال للكاتبين إريك بليتش وبين بلانشارد بعنوان "لقاء بين مسؤولين بالولايات المتحدة والصين لمباحثة قضايا الأمن الإلكتروني: البيت الأبيض،" المنشور برويترز Reuters، بتاريخ 12 سبتمبر/أيلول 2015.

[29] انظر، على سبيل المثال، مقال غريغ أوستين (Greg Austin) بعنوان "لا توجد حلول سهلة في الأمن الإلكتروني بين الولايات المتحدة والصين،" *East Asia Forum* 6 أكتوبر/تشرين الأول 2015. للاطلاع على المزيد من آراء المؤلفين بشأن هذه التطورات التي حدثت بينما كان هذا التقرير في طريقه للطباعة، راجع قسم الحواشي في هذا التقرير.

[30] يجوز الجمع بين جميع هذه الخيارات. فعلى سبيل المثال، قد تسعى الولايات المتحدة لإحراج الصين كي تغير سلوكها مع تقديم نوع من الترتيبات عن طريق التفاوض؛ وبالشكل نفسه، لربما تحاول الولايات المتحدة تعزيز دفاعاتها (الردع عن طريق الحجب) وفي الوقت نفسه الضغط على الصين للتفاوض.

[31] انظر على سبيل المثال مقال جيفري كار (Jeffrey Carr) بعنوان، "الهجمات الإلكترونية: لماذا يعد الثأر من الصين هو رد الفعل الخاطئ،" المنشور في مجلة ذا ديبلومات *The Diplomat* بتاريخ 6 أغسطس/آب 2015.

غير أن هذا النهج لا يسعى إلى التعامل مع مصدر الهجمات؛ إذ يُستحسن تقوية الدفاعات بالتأكيد، وبصرف النظر عن مصدر التهديد الإلكتروني. وسعيًا لعلاج قضية الفضاء الإلكتروني خلال العلاقة الثنائية، يتعين على الولايات المتحدة والصين إيجاد طريقة للتوصل إلى تسوية مؤقتة (أي اتفاق نتيجة للتفاوض) على مثل هذه القضايا. وعلى أساس هذه الاعتبارات، قررنا أن ننظر في الخيارات التي تتخطى مجرد تحسين الدفاعات الإلكترونية الأمريكية.

على نحو مماثل، لم نتدارس بطريقة منهجية خيار إجبار الصين على التوجه إلى طاولة المفاوضات. وبالطبع، يمكن أن تسعى الولايات المتحدة إلى تصعيد فرض التكاليف على الصين، من خلال مجموعة من ردود الأفعال التي قد تشمل مزيجًا من الإحراج العام والتهديدات،[32] أو إدانة القراصنة الصينيين على نحو فردي،[33] أو فرض العقوبات على الشركات الصينية[34] أو حتى شن حملة من الهجمات الإلكترونية المدمرة، وتجلب جميع هذه الخيارات مخاطر كبرى، ما يزيد من آمال إقناع الصين بالنظر إلى المفاوضات على أنها طريقة لتقليل حدة الضرر وتقليص الفرص أمام المزيد من التدهور في العلاقات.[35] لم يكن النهج المستند على الإجبار بأي حال الخيار الأول لإدارة أوباما، لكن بعدما شهدت الولايات المتحدة فشل المبادرات قليلة التكلفة وقليلة المخاطر في جلب الصين إلى طاولة المفاوضات، اتضح أنها على مدار العام 2014-2015 توصلت إلى ضرورة زيادة الضغط على الصين للتوصل إلى نتائج. تحدث الرئيس أوباما عن قضية الفضاء الإلكتروني مع الصين في خطابه أمام موظفي وكالة الأمن القومي في 11 سبتمبر/أيلول 2015 قائلًا: "يمكننا اختيار جعل هذا الميدان تنافسيًا –وأضمن لكم أننا سنفوز إن اضطررنا لذلك- أو يمكننا التوصل إلى اتفاق نقول

---

[32] "أوباما يلوح بهاجس حرب إلكترونية مستقبلية قبل زيارة شي جين بينغ، ويتعهد بخسارة الصين،" منشور بصحيفة ساوث تشاينا مورنينغ بوست *South China Morning Post*، 12سبتمبر/أيلول 2015.

[33] مقال إلين ناكاشيما (Ellen Nakashima) بعنوان "إدانة المخترقين بجيش التحرير الشعبي الصيني جزء من استراتيجية أمريكية أشمل لتحجيم التجسس الإلكتروني الصيني،" المنشور بصحيفة الواشنطن بوست *Washington Post*، 22 مايو/آيار 2014.

[34] مقال للكاتبة إلين ناكاشيما (Ellen Nakashima) بعنوان "الولايات المتحدة في طريقها لفرض عقوبات على الصين بشأن التجسس الاقتصادي،" المنشور بصحيفة الواشنطن بوست *Washington Post*، 30 أغسطس/آب 2015c.

[35] تناقش ماسترو ضرورة تقبل المخاطر الكبرى عند مواجهة إصرار الصين. انظر مقال أوريانا سكايلار ماسترو (Oriana Skylar Mastro) بعنوان "أسباب استمرار الإصرار الصيني،" واشنطن الفصلية *Washington Quarterly*، النسخة 37، رقم 4، شتاء 2015، ص 170-151.

من خلاله إن التنافس لن يخدم مصلحة أحد؛ دعونا نمهد الطريق بالتوصل إلى مبادئ أساسية تحكم كيفية عملنا".[36]

غير أن هذا النهج يحمل خطر تصعيد النزاع حتى إلى العالم الفعلي أو الإضرار بشدة بجهود الولايات المتحدة الرامية إلى اجتذاب التعاون الصيني في مجالات أخرى، مثل تناول قضية التغير المناخي، أو منع انتشار تكنولوجيا أسلحة الدمار الشامل أو تحقيق الاستقرار في الاقتصاد العالمي أو مكافحة التطرف العنيف. ومن غير الواضح ما إذا كانت الصين ستصدق أنه يجري اتخاذ إجراءات كتلك بغرض إجبارها على المفاوضات أم أنها لن ترى فيها سوى تصعيد لما يمكن للبعض في الصين أن يراه كحرب باردة دائرة فعليًا (حتى وإن كانت غير معترف بها) أو "منافسة صامتة"، للعلاقة بين الصين والولايات المتحدة، على حد وصف أحد مقاطع الفيديو الصادرة حديثًا عن جامعة الدفاع الوطني التابعة لجيش التحرير الصيني.[37] وقد تُفسر بعض أشكال الهجمات الإلكترونية (ضد ما يُعرف بالجدار الناري العظيم، على سبيل المثال) على أنها محاولات للاعتداء على سيادة الدولة، أو حتى لتقليص حكم الحزب الشيوعي الصيني، والسعي إلى تغيير النظام الحاكم.[38] وأخيرًا، وعلى مستوى عملي، لم نعتقد أنه يمكننا إيجاد ما يكفي من البيانات لتقييم وقائع هذا المنهج؛ إذ لا تسلط المنشورات الصينية الضوء كثيرًا على هذه القضية، ومن المفترض ألا يكون المحاورون الصينيون على استعداد لتوفير البيانات المفيدة، التي يمكنها المساهمة في تقييم مسار عمل كهذا. رغم درايتنا بهذا الخيار ودراستنا له لفترة من الفترات، لم نتناول في هذا البحث ذلك المسار بشكل منهجي.

بدلًا من ذلك، كان هدفنا الأول هو تقييم احتمالات أن تتوصل الولايات المتحدة والصين إلى اتفاق عبر المفاوضات أو إلى إيجاد طريقة أخرى للاتفاق على الأعراف والسلوكيات المتعلقة بالفضاء الإلكتروني. وكما أسلفنا، يسعى هذا التقرير إلى الإجابة عن سؤالين أثارهما إلغاء مجموعة العمل بين الولايات المتحدة والصين بخصوص الفضاء الإلكتروني وهما: ما هو المطلوب لإعادة أي شكل من أشكال المفاوضات

---

[36] مقال للكاتب ديفيد جاكسون (David Jackson) بعنوان "أوباما ورئيس الصين شي يعقدان اجتماعات مكثفة بشأن الأمن الإلكتروني والجيش،" المنشور بصحيفة يو إس إيه توداي *USA Today*، 21 سبتمبر/أيلول 2015.

[37] بيرليز 2013.

[38] مقال لجي لينفي (Zhi Linfei) بعنوان "تعليق: على الولايات المتحدة التفكير مليًا قبل الثأر من الصين بسبب اتهامات بالاختراق لا أساس لها من الصحة،" المنشور بصحيفة شينخوا Xinhua، 3 أغسطس/آب 2015.

الرسمية بين الولايات المتحدة والصين فيما يتعلق بالفضاء الإلكتروني؟ وفي حالة استئناف المفاوضات، ما هي المقايضات التي يمكن إجراؤها بين الولايات المتحدة والصين بخصوص السلوك في الفضاء الإلكتروني؟ وفي سياق معالجة هذين السؤالين، نتناول أيضًا بعض الموضوعات (مثل موقف الردع الأمريكي فيما يتعلق بالفضاء الإلكتروني) التي لا تعد بالضرورة جزءًا من أي صفقات، ولكن من شأنها التأثير في التوصل إلى تفاهم بين البلدين.

تتشكل منهجيتنا من عدة مكونات. أولًا، درسنا الأبحاث غير المباشرة ذات الصلة الخاصة بموضوع منظور الصين للأمن الإلكتروني وأثر الأمن الإلكتروني على العلاقات بين الولايات المتحدة والصين، لنثري فهمنا لوضع القضية في المرحلة التي بدأنا فيها بحثنا. كما عقدنا مناقشات مع خبراء مختصين من الولايات المتحدة لجمع الموارد من خبراء بارزين بالشأن الصيني أو خبراء السياسات الإلكترونية الضليعين بالجانب الفني، أو كما هو الحال في بعض الحالات، من لديهم إلمام بالأمرين. واستخدمنا أيضًا تقارير أساسية مفتوحة المصدر حول هذه المسألة من قنوات إعلامية رائدة وتبادلنا وجهات النظر مع زملاء متخصصين.

ثانيًا، سعينا إلى فهم مواقف الصين عبر تحليل ما كتبه الخبراء الأكاديميون والمحللون العاملون في مراكز الأبحاث التابعة للوزارات الصينية. ورغم أن هذه المصادر لا تكون دائمًا جازمة، إلا إنها تمكننا من توصيف المعالم العامة لمنظور الصين بشأن القضايا المتعلقة بالفضاء الإلكتروني. كذلك، ونظرًا لكون الفضاء الإلكتروني قضية حساسة نسبيًا في الصين، قلما كتب عنها المحللون الصينيون بأسلوب يختلف كثيرًا عن سياسات الحكومة، وفق ما أظهرته الأبحاث التي أجراها الخبير في الشؤون الصينية مايكل سوين (Michael Swaine). وهذا يعني أن الفجوة بين وجهات النظر الرسمية وغير الرسمية، وماينتج عنه من مخاطر الخلط بينهما، هي فجوة صغيرة نسبيًا.[39]

ثالثًا، درسنا تاريخ المفاوضات غير الرسمية حول الفضاء الإلكتروني بين الولايات المتحدة والصين (وتحديدًا المباحثات التي بدأت عام 2009 بين مركز الأبحاث الأمريكي "مركز الدراسات الاستراتيجية والدولية" و معاهد الصين للعلاقات الدولية المعاصرة). تشارك الباحثان الأساسيان لهذه الدراسة معًا في الجولات التسع من الحوار

---

[39] مايكل دي سوين (Michael D. Swaine) بعنوان "آراء الصين بشأن الأمن الإلكتروني في العلاقات الخارجية،" دورية مراقب قيادة الصين *China Leadership Monitor* رقم 42 خريف 2013.

بين مركز الدراسات الاستراتيجية والدولية ومعاهد الصين للعلاقات الدولية المعاصرة، ما قدم مصدرًا قويًا لوجهات النظر والخبرات لاستمداد المعلومات منه.

رابعًا، في مايو/آيار 2015، سافرنا إلى بكين وأجرينا حوارات مع أكثر من 30 فردًا، من ضمنهم أكاديميون ومحللون في مراكز الأبحاث وضباط في الجيش ومسؤولون حكوميون من الصين. محاورونا هم من المتخصصين في مجالات كثيرة من القضايا المتعلقة مباشرة بالعلاقات بين الصين والولايات المتحدة بخصوص الفضاء الإلكتروني، ومن ضمن هؤلاء، خبراء مهتمون تحديدًا بالعلاقات بين الصين والولايات المتحدة والسياسات الإلكترونية، والخبراء المعنيون بالحد من الأسلحة، والخبراء الاستراتيجيون العسكريون، والمسؤولون الحكوميون المعنيون بقضية الأمن الإلكتروني والمحللون المختصون باستراتيجية التنمية الاقتصادية الصينية. كما استفدنا من الفرصة لتبادل وجهات النظر مع خبراء الأمن الإلكتروني الصينيين الزائرين الذين مروا بواشنطن، وكذلك مع لو وي (Lu Wei) رئيس هيئة الفضاء الإلكتروني في الصين، عندما كان في زيارة إلى الولايات المتحدة في ديسمبر/كانون الأول 2014 وألقى خطابًا عامًا في جامعة جورج واشنطن.[40] في هذا التقرير، سنشير إلى بعض المتحاورين من أصحاب المناصب الحكومية بالمحاورين رفيعي المستوى ونشير إلى من سواهم بالمشاركين في الحوار.

تنظيم التقرير الحالي

الفصل الثاني وعنوانه "التوصل إلى اتفاق"، يضع الدعائم لفهم موقف الجانبين تجاه قضايا الأمن الإلكتروني، وذلك من خلال تحديد نمطين نموذجيين يتم التمييز بينهما عبر إدراك البلدان المختلف للأعراف والسلطة، ودور ومصالح الدول. وإليكم ماتوصلنا إليه؛ ينظر أتباع الردع الأحمر إلى الأعراف على أنها انعكاس لتوازن القوى الكامنة ومصالح الدولة، بينما يرى أتباع الردع الأزرق القواعد على أنها أقرب إلى القوانين والخطوط الحمراء الحيادية المتفق عليها التي تضمن المصلحة العامة لجميع الأطراف في النظام الدولي. وستوضح الفصول التالية أن هذه الرؤى المختلفة لطبيعة ودور الأعراف تحمل إشارات مهمة عن إدراك كل طرف لتصرفات وسلوك الطرف الآخر فيما يخص الفضاء الإلكتروني.

---

[40] مقال بعنوان "رئيس الفضاء الإلكتروني الصيني يناقش إمكانية بناء الثقة المشتركة مع الولايات المتحدة،" *GW Today*، 3 ديسمبر/كانون أول 2014.

أما الفصل الثالث وعنوانه "التوصل إلى الوضع الحالي" فيدرس المسائل التي تفرق بين الولايات المتحدة والصين فيما يتعلق بالفضاء الإلكتروني: من حيث سماتها الأساسية، وتصوير الولايات المتحدة لهذه القضايا، ورؤية الصين لها. يعتمد الفصل على مراجعتنا للمراجع الغربية ذات الصلة من المصادر غير المباشرة وعلى تحليلنا للمؤلفات الصينية عن الأمن الفضائي، ونتائج المحاولات السابقة للتوصل إلى إحراز تقدم في مجال الفضاء الإلكتروني من خلال المباحثات غير الرسمية بين مركز الدراسات الاستراتيجية والدولية، ومعاهد الصين للعلاقات الدولية المعاصرة، ومجموعة العمل الرسمية بين الولايات المتحدة والصين بشأن الفضاء الإلكتروني.

ويقوم الفصل الرابع، بعنوان "التوصل إلى اتفاق"، على لقاءات أجريناها مع محاورين رفيعي المستوى ومشاركين في الحوار من الصين. في بعض الحالات، نعرض مباشرةً ما سمعناه. وفي حالات أخرى، نستخدم ما لدينا من مواد لننظر في مناهج ومواقف حوارية بديلة (مثل المباحثات الثنائية في مقابل المباحثات المتعددة الأطراف، والمباحثات التزامنية في مقابل اللاتزامنية).

يلخص الفصل الخامس، وعنوانه "الخاتمة"، نتائج الأبحاث ويدرس الخيارات من أجل تحقيق أهداف سياسات الأمن الإلكتروني الأمريكي في مواجهة الصين.

التوصل إلى اتفاق

حاولنا جاهدين، أثناء إجراء هذه الدراسة، فهم بعض الاختلافات الجوهرية في أسلوب تناول الولايات المتحدة والصين للقواعد والمعايير. وحتى نصل إلى هذه الغاية، أعددنا مجموعة إرشادية من الأنماط النموذجية. الردع الأحمر هو نمط نموذجي ينطبق على عناصر كثيرة من نظرة الصين لدور القواعد ودور الردع في ضمان التزام الأطراف الأخرى بهذه القواعد. الردع الأزرق هو نمط نموذجي ينطبق على عناصر كثيرة من نظرة الولايات المتحدة لدور القواعد ودور الردع في ضمان التزام الأطراف الأخرى بهذه القواعد. رغم أننا نورد الأمثلة من سلوك الصين لوصف الردع الأحمر وأمثلة من سلوك الولايات المتحدة لوصف الردع الأزرق، لا نجزم بأن سلوك الصين يتوافق دائمًا مع الردع الأحمر، ولا أن سلوك الولايات المتحدة يتوافق دائمًا مع الردع الأزرق. ولنعرض الموضوع بإيجاز، بقدر التزام الصين بالردع الأحمر، نرى بأن قادتها يؤكدون على أن النظام الدولي الحالي مؤسَّس على توزيع للقوى والمصالح بشكل يخدم الولايات المتحدة والغرب، وأن القواعد التي تشكل النظام الدولي تعكس مصالح الولايات المتحدة، وهي القوة المهيمنة التي أسست النظام.

وفي المقابل، بقدر التزام الولايات المتحدة بالردع الأزرق، يرى المسؤولون الأمريكيون أن النظام الدولي مبني على مجموعة من الممارسات الليبرالية والشاملة والعادلة، التي بمرور الوقت، اتخذت شكل مجموعة القوانين والأعراف التي تعمل، بشكل كبير، على موازنة وحماية مصالح جميع الأطراف الفاعلة في النظام العالمي. رغم أن الاختلافات بين هذين النمطين النموذجيين ليست مطلقة بأي شكل من الأشكال– إذ يدرك المفكرون الصينيون فائدة القانون (وعادةً ما تستخدم الحكومة الصينية اللغة المستخدمة في ميثاق الأمم المتحدة)، وتشك قلة من الأمريكيين في أن القانون يرتكز على أساس القوة – إلا أن الاختلافات في تأكيد ذلك كبيرة جدًا.

في هذا الفصل، ندرس أولًا طبيعة تلك الاختلافات ومصدرها. وللقيام بذلك، نعرِّف القواعد بأنها ما يحدد الخطوط التي تفرق بين نمطين من السلوكيات وهما: النمط المرغوب فيه والنمط المحظور أو غير المشروع. ثم نستخدم مفاهيم التدويل (أو *guoji huayu quan*)، والردع والإجبار لوصف طريقة تطبيق القواعد ودعمها. ونختم النقاش بدراسة كيف أن هذه الاختلافات بين وجهات النظر الأمريكية والصينية حول تطبيق القواعد تنطبق على نظرة البلدين لطبيعة علاقاتهما في الفضاء الإلكتروني.

أبعاد وآثار الآراء المتباينة بشأن الردع

يغلب على فلسفة الردع الأزرق اتخاذ النظام الدولي القائم كنقطة بداية له والسعي للحفاظ على هذا النظام وحمايته والعمل على تحسينه ليصل إلى أفضل صوره. تمارس الدول التي تعتمد على نموذج الردع الأزرق، مثل الولايات المتحدة، نفوذًا معياريًا وفكريًا وتعريفيًا، تظهره من خلال العلاقات الثنائية وعبر المنظمات الدولية، لتكوّن توافقًا شاملاً حول السلوكيات المقبولة وغير المقبولة في المجتمع الدولي. ولدعم دعم هذه المطالب المعيارية القائمة على القوانين، يركز الردع الأزرق في الأساس على وصف السلوك من منظور شرعيته أو عدم شرعيته المعيارية، وكخطوة ثانوية فقط، ينزع إلى الإشارة إلى القوة المادية للقوات التي تدعم هذه القواعد. وتتوافق هذه الرؤية للقواعد، جزئيًا مع امتلاك القدرة الفعلية على فرض تكاليف باهظة على جميع الأطراف الفاعلة في النظام الدولي تقريبًا (كما تفعل الولايات المتحدة) ولكنها تختار كسب الدعم لقواها عبر فرض بعض القيود على نفسها لتكسب انضمام الجهات الفاعلة الأضعف للنظام.[1]

يتوافق الردع الأزرق مع صورة العالم المكون من النظراء، حيث تتحول الاعتراضات على سلوك أي دولة أخرى إلى اتهامات بانتهاك هذه الدولة الأخرى للقوانين المقبولة عمومًا المفروضة على نظام عالمي من دونها تعم فيه الفوضى. لا يعمل الردع الأزرق عن طريق السلطة التعسفية بل من خلال نظام قائم على التهديد يعززه عقاب مدعوم من جهة فردية وأحيانًا أكثر من جهة، ويدار بأسلوب تطغى عليه الصبغة القانونية. فتجاوز النقاط المحظورة، أي خرق القانون مثلًا يستلزم العقاب في

[1] G. John Ikenberry, *After Victory: Institutions, Strategic Restraint, and the Rebuilding of Order After Major Wars*, Princeton, N.J.: Princeton University Press, 2000.

حالة الرغبة في الحفاظ على القواعد، سواء كانت الدولة المعرضة للعقاب دولة حليفة أو حتى إن كانت دولة ثالثة على الحياد (مثلما حدث في الكويت في أغسطس/آب 1990).

ومن ثم، يمزج هذا المنهج بين مسألة "ما هي الأفعال التي تشكل عملًا عدائيًا ويجب معاقبتها" ومسألة "إن كان العقاب المفروض ضد هذه الأفعال يصب في مصلحة دولة ما".[2] وما يتضمنه هذا السؤال هو ضرورة توافق أي خط محظور متفق عليه مع المفهوم الأوسع عن ماهية الخطوط المحظورة التي قد تكون مناسبة لجميع الأطراف للرد عليها. فالقانون الساري على أحد الخطوط ينبغي أن يسري على جميعها. غير أن أحد أسباب اتباع الردع الأزرق للرأي أو الخطاب الذي يدعم منهجية الردع ذات الصبغة القانونية هو نفوذه الهائل على نص هذا القانون (وفي اللحظات الحرجة يمكنه أن يعفي نفسه من العقاب). هكذا إذًا يكون الالتزام مشروطًا وليس مطلقًا، ولا تتمتع الدول الأقل قوة بهذه الرفاهية.[3]

ينصب تركيز الردع الأحمر أكثر على العلاقة بين الأفكار ومصالح أصحاب النفوذ هؤلاء، والعلاقة بين نفوذ أحد الأطراف الفاعلة والأطراف القوية الأخرى في النظام. كما يتضمن، على نحو نموذجي، فرضية تعارض المصالح بين الأطراف المتنوعة في النظام ، في أغلب الحالات. وبالفعل، يميل نهج الصين حيال الردع إلى افتراض أن أقوى طرف في النظام سيسعى إلى إخفاء الاختلافات بين مصالحها ومصالح الأطراف الأخرى الأضعف، في أغلب الحالات، وذلك باستخدام لغة معيارية توحي بوجود نسق سلوكي شرعي واحد يخدم مصالح جميع الأطراف في النظام، وتروج وعيًا زائفًا هدفه إرباك أو إجبار الأطراف الأضعف على قبول شرعية وضعيتها الأدنى منزلة عبر حثها على تصديق أو تقبل المعايير التي لا تخدم مصالحها حقًا. يقطن الردع الأحمر عالمًا لا تحدده أطراف فاعلة من النظراء بقدر ما يحدده التسلسل الهرمي، حيث تتواصل الدول مع بعضها لما لديها من مستويات مختلفة من المصلحة في دعم قواعد معينة. ونظرًا لأن تلك تعد انعكاسات لعلاقات القوى الكامنة والمصالح أكثر منها لقوانين حيادية تضمن استقرار النظام، ينظر الردع الأحمر إلى الأعراف بقدر كبير من الشك،

---

[2] القانون الدولي لا يذكر "الأعمال العدائية" لكنه يذكر "استخدام القوة" "والهجوم المسلح". لكننا لاحظنا طرح التحليلات غير الرسمية للحرب الإلكترونية السؤال التالي"هل يعد ذلك عملًا عدائيًا؟" لاقتراح أن بعض الأعمال في الفضاء الإلكتروني تستدعي، بل وحتى تدفع لرد عسكري.

[3] قد ترغب الولايات المتحدة، على سبيل المثال، في الالتزام بأحد القوانين التي لا تخدم مصالحها، وذلك كوسيلة لدفع الآخرين إلى الالتزام بقوانين أخرى لا تصب في مصالحهم دائمًا.

ويسعى أتباعه إلى حساب المكاسب والخسائر بدلًا من الأفعال الصائبة والخاطئة. ولا يفترض أن القواعد التي يقوم عليها النظام الدولي الأشمل هي بالضرورة جيدة في حد ذاتها كما يتم وضعها حاليًا. وبالتالي، يألف المفكرون الصينيون كثيرًا ترابط القوى الكلي (بما في ذلك النفوذ الدبلوماسي والقوة الاقتصادية، على سبيل المثال) بين القوى الرائدة في النظام الدولي. وبسبب ذلك، لا يظهرون قدرًا كبيرًا من الاهتمام أو الرغبة في الرد على انتهاكات القواعد، بافتراض أن القواعد تعكس أساسًا مصالح القوى المهيمنة ولا تعكس مصالح المجتمع الدولي ككل. ومن عواقب هذه الآراء أن بعض المفاهيم مثل مصداقية النظام الدولي تكون أقل أهمية، بما أن النظام بأكمله لا يُنظر إليه على أنه يحظى بقدر كبير من الأهمية. بل يُعتد مباشرة بمصالح الطرف الفاعل المحدد فيما يتعلق بمدى تأثير أي تصرف بميزان القوى بين البلدين.

عمليًا، رغم اعتراف الصين ببعض المزايا في حكم القانون، تكررت شكواها بأن صياغة الكثير من القوانين والقواعد التي تدير النظام الدولي تمت في فترة كانت الصين فيها منهكة القوى أو ضعيفة استراتيجيًا. وبما أن القانون لطالما كان ولا يزال يتأثر بتوزيع القوى، ينبغي على الأعراف والقواعد الجديدة أن تعكس قوة الصين الجديدة والكبرى داخل النظام الدولي. ولاحظت الصين أن الولايات المتحدة هي الدولة الوحيدة التي لا يمكن فرض العقوبات عليها (عمليًا).

ترتكز نماذج الردع الزرقاء والحمراء على المصالح المتنافسة والتصورات حول السلوك الذي ينبغي أن تتبعه الدول. ينبغي ألا تشير الاختلافات إلى وجود صدام، إذ يعتمد الكثير على استعداد كل طرف للتخلي عن الإجراءات التي يشعر بأن له الحق في اتخاذها بسبب اعتراضات الطرف الآخر. غير أنه من المرجح أن تزداد احتمالات سوء التفاهم إلى الحد الذي تظن فيه الولايات المتحدة أن الصين تتصرف بتهكم (لأنها تفضل النفوذ على القوانين) وتظن الصين أن الولايات المتحدة تتصرف على نحو زائف (لأنها تستخدم القوانين لإخفاء النفوذ).

مصادر الخلاف

يعكس الردع الأزرق تجربة الولايات المتحدة في الحرب الباردة، حيث كان بإمكان كل جانب تدمير الجانب الآخر - بصرف النظر عن من كانت لديه القوة التدميرية الأكبر في متناول يده. لم يكن هناك مجال للشك في أن الهجوم النووي سيجلب هجومًا نوويًا

مضادًا، غير أن الأسئلة الصعبة انطوت على ظروف أخرى قد يتم استخدام الأسلحة النووية فيها. ما تبقى هو تحديد الطريقة التي تضع فيها الدول الخطوط المحظورة الخاصة بها وكيفية إقناعها أعداءها (وطمأنتها أصدقاءها) أنها ستستخدم فعلًا الأسلحة النووية في المواقف التي هددت (أو تعهدت) باستخدامها. رغم المساعي التحليلية لدراسة مسألة الحد من الحرب النووية فور نشوبها، انخفضت الثقة بأن الحد من الحرب سيأخذ مجراه في الوقت المناسب (أي قبل قتل الملايين)، إن تم الحد منها بالأساس. زادت تلك المخاوف من التأكيد على أنه لم يستخدم أي سلاح نووي أبدًا.

في المقابل، يتوافق الردع الأحمر مع التقييمات التي أجراها قادة الصين على تجارب بلدهم خلال ما وصفوه بأنه "قرن من الذل"، الذي وقع بين 1840 و1949، عندما سيطرت القوى الأجنبية على سلالة تشينغ (Qing) التي حكمت قبل سقوطها عام 1911، وبعدها انهارت الصين ما بين عصيان مدني وحرب في الفترة ما بين 1912 و1949. وأثناء "قرن الذل"، لم يكن لسلالة تشينغ ولا جمهورية الصين التي تلتها وسيلة لدرء نهبها من الأطراف الخارجية المتقدمة اقتصاديًا سواء من أوروبا أو روسيا أو اليابان. وعندما وصل الحزب الشيوعي الصيني إلى الحكم، كان هدفه هو بناء قوة الدولة وبالتالي الإمساك بزمام مصير الصين – وبنمو قوتها، تكتسب ما يكفي من الاحترام من الخارج لتكسب الإذعان لمصالحها الخاصة (حتى لو كانت تكلفة ذلك كبيرة على مصالح جيرانها).

تشكّل المفاهيم المتنافسة في المجتمع أساسًا عميقًا للاختلافات. في الولايات المتحدة، يعد الفرد المستقل هو الوحدة الأساسية للنظام الاجتماعي، ويدرك هذا الفرد تمامًا حقه في اتخاذ القرارات بما يتفق مع القيود التي تنشأ من تعامله مع الآخرين. تصاغ هذه القيود في شكل قانون.

لكن في الصين في المقابل، غطى النظام الشيوعي الشمولي على الفكر الاجتماعي الأكثر تقليدية للكونفوشيوسية-الشرعوية، ومنحت هذه الأنظمة الثلاثة الأولوية لنفوذ الدولة والمجتمع على حساب الفرد. إضافة إلى ذلك، تزعم هذه التعاليم أن السلطة الشرعية للحكومة ينبغي ألا تسمح بوجود أي عوائق رسمية باتجاه المواطنين، وهو مفهوم برز بوضوح في مبدأ "دكتاتورية الشعب الديمقراطية"، وأعربت الحكومة الصينية مؤخرًا عن رأيها بأن مبدأ السلطة الدستورية أو فكرة تحجيم الحكومة بالقانون

تمثل تهديدًا لنظام الحكم.[4] وفي داخل الإطار الاجتماعي الكونفوشي يُمنح الأفراد درجة معينة من السلطة على الآخرين بناء على وضعهم في المجتمع. يُتوقع استيعاب هذه العلاقات داخليًا، ويؤدي هذا الاستيعاب بدوره إلى تقليل ضرورة الاستخدام الصريح للقوة لنيل الطاعة.

أظهرت الأبحاث السابقة عن الفكر العسكري الصيني أن كلمة الردع أو كما تُعرف بالصينية [*weishe*] ليست كلمة أصيلة في اللغة الصينية وتُترجم إلى ما هو أقرب لمزيج من كلمة الردع بمعناها المستخدم في اللغات الغربية مع إضافة بعض دلالات لكلمة الإكراه أو الإجبار.[5] لا تنبع هذه الاختلافات من قصور الترجمة بقدر نشأتها من الظروف التاريخية المختلفة التي عاشتها المجتمعات الصينية والغربية. يعكسُ الردعُ الأزرق تجاربَ الولايات المتحدة في الحرب الباردة وتجارب أوروبا مع مفهوم ميزان القوى. ويعكس الردع الأحمر تجربة الصين المختلفة مع الحرب الباردة، حيث وجدت أن الردع مبدأ مفروض للدفاع عن نظام تعتبره نظامًا غير شرعي وغير مرغوب فيه ومفروض على الصين بتكاليف باهظة لمصالح الدولة.[6]

يستهدف الردع الأزرق الاستقرار، مما يتوافق مع احتياجات دولة في وضعها الراهن. ويستهدف الردع الأحمر فكرة مواجهة الهيمنة في حال ضعف الدولة تحت مسمى المبادئ العامة، ثم تتحول الدولة إلى دولة مهيمنة عندما تبلغ ما يكفي من القوة، لهذا دائمًا ما توضع المصالح في الاعتبار عندما تتخذ البلدان الأخرى اختياراتها. أو كما صاغها رئيس الخارجية الصيني السابق يانغ جيه تشي (Yang Jiechi) في عام 2010: "الصين دولة كبيرة...وغيرها من البلدان هي بلدان صغيرة وهذا هو الواقع."[7]

---

[4] مقال فون وينتربوتوم (Vaughan Winterbottom) بعنوان "في الصين، كلمة الدستورية كلمة بذيئة،" المنشور بصحيفة ذا إنتربريتر *The Interpreter* بتاريخ 28 يناير/كانون الثاني 2014؛ ومقال للكاتب كريس باكلي بعنوان "هجوم الصين على الأفكار الغربية" المنشور بصحيفة نيويورك تايمز *New York Times*، 19 أغسطس/آب 2013.

[5] دراسة لجو مكرينولدز (Joe McReynolds) بعنوان "التفكير الصيني بشأن الردع الإلكتروني،" في دورية تأثير جيش التحرير الصيني على صنع السياسات الأمنية الوطنية في الصين لمحرريها فيليب سي سوندرز وأندرو سكوبيل، ستانفورد، كاليفورنيا: مطابع جامعة ستانفورد، 2015.

[6] مقال للكاتب دين شينغ بعنوان "آراء الصين بشأن الردع" المنشورة بدورية القوات المشتركة الربع سنوية *Joint Forces Quarterly*، رقم 60، ربيع 2011، ص 94-92.

[7] "أسنان التنين الجديدة،" المنشور بصحيفة ذا إكونوميست *The Economist*، 7 أبريل/نيسان 2012.

عناصر الاختلاف

من وجهة نظر الردع الأزرق، الردع أمر إما موجود أو غير موجود. نظريًا، قد يكون الردع موجودًا لدى الجميع في نفس الوقت إذا لم تتعدَّ أي دولة على الخطوط المحظورة للدول الأخرى خوفًا من العواقب المترتبة على ذلك. وإن تداعى الردع، قد يضطر المحافظون على الردع إلى إعادة تحديد أو إعادة تعريف خطوطهم المحظورة مع دعم موقفهم بالإشارات و/أو الإجراءات ذات التكلفة الباهظة. وقد تتضمن الإشارة المناورة بعناصر القوات (مثل تحريك السفن والطائرات)، لكن دون استخدام القوة نفسها بالضرورة. يولي الردع الأزرق قدرًا كبيرًا من الاهتمام إلى الخطوط المحظورة. ينبغي أن تكون هذه الخطوط شديدة الوضوح حتى تتمكن الأطراف الأخرى من الحكم على السلوك المتعلق بهذه الخطوط المحظورة على نحو موثوق به – لا من حيث ما يحظر على الآخرين فعله فحسب، بل ما يمكن أن يفكر به الآخرون من الإفلات من العقاب. يفترض الردع الأزرق أن إبلاغ الآخرين بوضوح بالأمور التي ستدافع عنها الدولة يقلل من احتمال نشوب حرب تنشب عن طريق الخطأ أو سوء التقدير.

يتخلى الردع الأحمر عن الخطوط المحظورة لصالح درجة من الغموض الاستراتيجي هدفها تضخيم نفوذ الجهة الأضعف عن طريق توسيع مجال الريبة تجاه أنماط الأفعال التي قد تستدعي رد الفعل. ونظريًا، يؤدي عدم وضوح النقاط إن تم تجاوزها، إلى النزاع، ويزيد من تعقيد الأمور أمام القوى الأخرى مع إعطاء الدولة الأضعف في نفس الوقت (مثل الصين) المرونة الاستراتيجية المطلوبة للامتناع عن اتخاذ فعل معين إذا قررت أن هذا الفعل قد يدمر مصالحها، لكنها تفتقر إلى القوة اللازمة لمعاقبة الطرف الذي ارتكب الفعل. يشجع هذا النهج البلدان الأخرى على أن تأخذ في اعتبارها آراء الدولة القوية بخصوص ما يشكل الخطوط المحظورة تحديدًا، ويشجعها على التدبر قبل إجراء أي تصرف، وعلى دراسة مخاطر النزاع الذي قد ينشأ بسبب تصرفاتها على مدى نطاق أوسع بخلاف ما قد يكون عليه الحال إذا عبرت تلك الدولة عن مصالحها بشكل أوضح.

وعمليًا، لم ترسم الصين خطوطًا محظورة واضحة على نحو نمطي بقدر ما عبرت عن غضبها المتزايد تجاه تصرفات الآخرين المبالغ فيها وفق وجهة نظرها. وهذا يعني أن الردع الصيني تم بأثر رجعي وضمني وتناظري بشكل نسبي (مستوى الغضب دليل على مبالغة الطرف الآخر في فعله). وعلى عكس ذلك، سعى الردع الأمريكي ليكون مرتقبًا نسبيًا (أي معلنًا عنه من البداية) وصريحًا ورقميًا (إما أن

تتخطى الخطوط المحظورة أو لا تتخطاها). إضافة إلى ذلك، بما أن الردع الأحمر هو استراتيجية القوة الأضعف ولكن الساخطة، فإنه لا يتضمن فقط عوامل الإكراه بل يتضمن كذلك الجهود المطلوبة لتكوين التصورات بين الجمهور الغربي بأن هذه الدولة تتحمل نسبة عالية من تقبل المخاطر بسبب ظنها بأن الردع يتضمن المقدرة والاستعداد للمجازفة بالحرب.[8] وعلى نقيض ذلك، ينصب اهتمام الردع الأزرق على تجنب احتمالية نشوب النزاع العرضي أو غير المقصود ويسعى إلى إعادة الوضع إلى الاستقرار الذي كان قبل الأزمة.

لدى الردع الأحمر خاصية مميزة وهي تذكير الآخرين بمراكزهم في النظام الهرمي الخاص بتوزيع القوى الدولية. ولطالما ذكرت الصين الدول الأخرى بضرورة احترام المصالح الصينية وقوتها. واستغلت الصين حربها ضد الهند عام 1962 وغزوها لفيتنام عام 1979 لتذكير جيرانها بما في وسعها أن تفعله (ولن تتوانى عن فعله) في حال تهديد مصالحها. وكانت لضربات مدافعها على الموانئ الشمالية والجنوبية في تايوان عام 1996 نفس الأولويات (إلى أن تدخلت الولايات المتحدة لتفرض نفوذها).

وإذا لاحت الحرب في الأفق، يشير خطاب الصين إلى ضرورة استخدام القوة لإجبار الآخرين على منح الصين الاحترام الذي تستحقه. وغرض الحرب هو استعراض أسس هذا الاحترام (أي "لقد طلبنا منكم احترام مصالحنا، والآن سوف نجبركم على ذلك"). ولهذا السبب، رأت الصين أن عليها أن تحسب ميزان القوى بدقة قبل أن تستعرض قوتها. وعلى نقيض ذلك، يرى المحللون الأمريكيون أن الحرب تنشأ من عدم القدرة على الإعلان عن الخطوط المحظورة و/أو عدم القدرة على الإعلان عن مصداقية تهديداتها. فغرض القوة هو تعزيز تلك النوايا (أي، "لقد طلبنا منكم ألا تفعلوا هذا الأمر، والآن علينا أن نستخدم العقاب لنوضح وجهة نظرنا").

من وجهة نظر الولايات المتحدة، كان من المهم أن تبقي احتمالات العقاب أمامها، وتحديدًا إذا رغبت الدولة في الحفاظ على مستوى من الردع بعد العقاب المبدئي. بالتالي، ينبغي تدريج العقاب في كل حالة يُتوقع فيها أن يفلت الطرف الآخر من التطبيق الفوري للعقاب. وبالنسبة للصين، تقل أهمية تدريج العقاب، لأن الهدف من استخدام القوة ليس تعديل سلوك البلدان الأخرى، لكن للتأكيد على قوة الصين،

---

[8] Cheng, 2011. يناقش مقال ماسترو المنشور عام 2015 جهود الصين لاستخدام المناورة بالمخاطر ولتكوين انطباع بوجود درجات كبيرة من قبول المخاطر من أجل توسيع قدرتها على تكوين القرارات الخاصة بسياسات الحكومات الأجنبية.

وهكذا يُتوقع من البلدان الأضعف أن تعدل من سلوكها احترامًا للصين. ومن جهة أخرى، تدرك الدول الأقوى أن الصين لن تخضع بخنوع رغم التفاوت في معدلات قوتها النسبية.

إذا كان الردع الأزرق يتعامل مع الإجبار على أنه أمر مختلف عن الردع، حتى وإن كان الردع الأحمر يراهما وجهين لعملة واحدة، فهذا لأن الردع الأزرق هو أقرب إلى نموذج تطبيق القانون الذي يتناسب مع القوة المؤسسة للنظام والقائمة بذاتها، بينما يرتكز الردع الأحمر أكثر على الافتراضات حول طبيعة القوة والخوف والنظام. لا يوقع الردع الأزرق العقاب إلا على الأخطاء التي يتم ارتكابها. وإذا نجح الردع، فلن يجرؤ أحد على تخطي الحدود. وخطاب الإجبار – الذي يتطلب من الدولة أن تتصرف بشكل ما وإلا وقع عليها العقاب – لا يلائم نموذج تخطي الحدود بهذه السهولة، لأنه خطأ إغفال، وهو أمر مختلف تمامًا. وتضع هذه المقارنة استقلالية الطرف الآخر في الحسبان. وقد تدعي الدول التي لم تتخط الخطوط المحظورة أنها لم تتعرض للإكراه – بل ببساطة لم يكن في نيتها تخطي الخطوط المحظورة موضوع النقاش في المقام الأول. وفي المقابل، تجد الدول المعاقبة لعدم تنفيذها لأمر ما نفسها مجبرة على فعله تحت الضغط، ستظهر، على الأرجح، وكأنها تتعرض للإكراه. يرتكز الردع الأحمر على الإذعان لرغبة دولة أخرى، بغض النظر عن القضية. ومسألة استخدام القوة لمنع دولة أخرى من اتخاذ خطوة إلى الأمام أو لإجبارها على الرجوع خطوة إلى الوراء هي مسألة ثانوية. لكن ما يهم هو الحد الذي تُفرض عنده إرادة الدولة على الدول الأخرى. ومع فرض الدولة لإرادتها، تُمنح أهمية أقل لمفهوم حقوق الأطراف الفاعلة في اتخاذ قراراتها باستقلالية، وفي الواقع، يفضل الردع الأحمر أن تنظر الدولة الأخرى (إن لم يكن بالضرورة الأطراف الأخرى) إلى الخضوع بهذا المنظور تحديدًا.

ينظر فكر الردع الأزرق إلى الاستقرار الدولي على أنه نابع من الالتزام العالمي بمجموعة من القواعد تتعلق بما يمكن أن تفعله دولة في أخرى، ويُطبق الفكر الأزرق بالإجراءات التي تُتخذ ضد من ينتهك القواعد. ويجد الردع الأحمر الاستقرار في الإقرار الدولي بوجود تسلسل عالمي للقوى (بمعنى توزيع القوى العالمي أو التسلسل الهرمي) ليستلزم نمط من الاحترام. يرتكز كل من نوعي الردع على الحظر وعلى سلطة تنفيذه، غير أن الردع الأزرق يؤكد على الحظر، بينما يؤكد الردع الأحمر على السلطة.

القانون والمساواة

ينجذب الردع الأحمر للخطابات التي تؤكد على استقامة الدول الأضعف التي تتلاعب في عالم من الدول القوية (ذات ماض إمبريالي). غير أن استراتيجية الخطاب القائم على مناهضة الهيمنة ستقع في مأزق إذا اكتسبت الدولة ما يكفي من القوة لتتحول بنفسها إلى دولة مهيمنة. وكثيرًا ما تعتمد المؤشرات مثل السيادة والهيمنة على المواقف عند التطبيق بكل حال، وبالتالي، إذا تغير الموقف، تتغير كذلك مصالح الدولة غير أن فهمها للطريقة التي يتم بل ويجب ممارسة اللعبة بها لا يتغير. وبسبب صعوبة هذه التغيرات تحديدًا، يجب أن يتحلى الردع الأحمر بوعي أكبر عند المشاركة في العمليات النفسية (وربما حتى بإدراك أعمق) من الردع الأزرق. وهكذا يكون عمل الردع الأزرق أسهل، طالما أن ما دامت والقواعد التي يؤيدها تتحمل سقوط المنادي بها من وضع الهيمنة أو صعوده إليها.

وهكذا يشكل موقف الردع الأحمر تجاه القانون تناقضات محتملة. فمن جهة، يعد الإصرار على حكم القانون في المجالات المشتركة، مثل الفضاء الإلكتروني، طريقة جيدة لتحجيم سلوك الآخرين، لكن عند تطبيق القانون على الذات، سيكون الجواب المتعارف عليه هو الاختباء وراء مزاعم السيادة (أي قدرة الدولة على العمل بقوانينها) والمناداة بالثقة المتبادلة. ومن جهة أخرى، إذا تحولت الدولة إلى قوة مهيمنة بالفعل، قد تكتشف أن هناك بعض القوانين والأعراف الدولية التي لا يمكن إعادة تشكيلها بما يناسب مصالحها. ومن ثم، قد تتحول الخطابات الكلامية المسبقة لمفهوم القوانين والأعراف الدولية إلى قيود ما كانت لتظهر في عالم يتحدد فيه السلوك المقبول في المقام الأول من قِبل من يمتلكون السلطة.

تميل الصين والولايات المتحدة –كل على حدة- إلى استخدام مفهوم "المساواة" على نحو مختلف. وتؤمن الولايات المتحدة أنها تتعامل مع الدول الأخرى على قدم المساواة لأنهم يتساوون أمام القانون والأعراف الدولية. وفي المقابل، تشكو الصين من أن الولايات المتحدة لا تتعامل معها على قدم المساواة لأنها لا تحظى بالاحترام الكافي من الولايات المتحدة لها كدولة ذات قوة مماثلة لها (وهي ليست كذلك).[9]

يتأقلم الردع الأزرق مع التحالفات بسهولة بسبب سهولة توسيع مجال التطبيق الأحادي للقواعد العالمية على نظام تطبيق ذي جوانب متعددة. وتكاد الولايات

[9] لقاءات مختلفة، بكين، مايو/آيار 2015.

المتحدة تجزم أن التحالفات تتشكَّل على قدم المساواة وأن التحالفات تعمل بموجب مبادئ التصويت (حتى وإن أدرك الجميع من هو صاحب السلطة الفعلي داخل التحالف). لا يتأقلم الردع الأحمر بهذه السهولة مع التحالفات لأن عالمه لا يتشكل حقيقةً من أقران صوريين أو حتى فعليين، فكل منهم إما أن يكون في مرتبة أعلى أو أدنى نسبة إلى بعضهم البعض. قد يكون للصين دول تشترك معها في المصالح العامة أو حتى في الحلفاء الرسميين. وفي تلك العلاقات، إذا كانت الصين دولة قوية، يُنظر إلى الدول المنحازة لها بالضرورة على أنها دول متوسلة حبيسة علاقات غير متكافئة. وبالتالي، من المستبعد أن تكون الدول المنحازة حليفة لبعضها البعض، حيث لا تربطها الرغبة في الدفاع عن قيم مشتركة بقدر ما تربطها التبعية المشتركة للصين.

تطبيق مناهج ردع مختلفة بشأن الفضاء الإلكتروني

ينعكس الفرق بين نموذجي الردع الأحمر والأزرق في الجدل الدائر حاليًا حول الفضاء الإلكتروني. ولتوضيح هذه النقطة، يجب النظر في مفاهيم الهيمنة، والإسناد، والتصعيد، والاستقرار، والقواعد كما يمكن أن يتم تطبيقها في الفضاء الإلكتروني وكما تنعكس في المناهج الأمريكية والصينية.

الهيمنة

تبقى الصين شديدة القلق، أو ربما حتى شديدة الهوس، بالهيمنة في الفضاء الإلكتروني – أي قدرة بعض الدول على تنفيذ ما تريده دائمًا فيما يتعلق بالفضاء الخارجي، بينما تُجبر الدول الأخرى على الالتزام بالقواعد التي وضعتها القوى المهيمنة. ولا يتحدث المسؤولون والخبراء الأمريكيون بلغة الهيمنة (ربما حتى لا يفكرون فيها) ولكن يفترضون أنه إذا التزمت الدول بالقوانين العادلة والمعقولة (مصدر هذه القوانين لا علاقة له بموضوع النقاش) ستتمكن من تحقيق أهدافها المشروعة في الفضاء الإلكتروني وفي العالم الفعلي أيضًا.

هل يمكن أن تصبح الصين قوة مهيمنة في الفضاء الإلكتروني يومًا ما؟ ما الذي يميز الولايات المتحدة حتى جعل منها قوة مهيمنة في الفضاء الإلكتروني، من وجهة نظر المحللين الصينيين؟ إذا كانت ميزة الولايات المتحدة هي إمكانياتها الوطنية الأصيلة (مثل التعليم ورأس المال)، فسيكون طريق الصين لانتزاع الهيمنة الأمريكية مباشرًا وشرعيًا وهو: المزيد من الإنفاق على التعليم والمزيد من الدعم للإبداع. بل يبدو أن المفكرين

الصينيين يؤمنون بأن الولايات المتحدة تملك مزايا غير عادلة في الفضاء الإلكتروني نتيجة لاختراعها التكنولوجيا ذات الصلة التي صنعت الإنترنت – وهي ميزة نالتها عن جدارة ولكن احتفظت بها بشكل غير عادل. ويثير غضب الصين كذلك شركات إدارة الإنترنت التي يوجد مقرها في الولايات المتحدة، مثل هيئة الإنترنت للأسماء والأرقام المخصصة آيكان (وهي شركة غير ربحية تعمل على إدارة جوانب محددة لتسجيل اسم النطاق على الإنترنت) وإلى حد أقل، فريق عمل هندسة الإنترنت (وهي منظمة ذات عضوية مفتوحة تدعم معايير الإنترنت الشائعة والطوعية).

تقاوم الولايات المتحدة إعادة هيكلة هذه المنظمات في الاتجاه الذي يرعى مصالح الصين لأنها ترى أن قوانين الصين المفضلة للفضاء الإلكتروني ستأتي على حساب حرية الإنترنت. أما الصين، فهي ترى أن حرية الإنترنت عنصر أساسي للهيمنة الأمريكية وتهديد صريح لحكم الحزب الشيوعي الصيني. ولتعزل نفسها بشكل أفضل عن التهديد المتصور للتخريب المدعوم من الولايات المتحدة والنابع من الإنترنت، أعربت الصين عن رغبتها في إنشاء اتصال بكابلات الألياف البصرية من آسيا إلى أوروبا مباشرةً لتجنب إرسال حركة نقل البيانات عبر الإنترنت على الخوادم الموجودة في الولايات المتحدة (حيث يخشى المحللون الصينيون من إمكانية اعتراضها أو حجبها في حالة نشوب النزاع).

وبالمثل، ترغب الصين في الاستفادة من سوقها الداخلية لتدعم انتشار المعايير الفنية مع علامة "صنع في الصين" المميزة ليصب ذلك في مصلحة الشركات الصينية. وبالتالي تبذل الصين جهودًا حثيثة لتزيح ما تطلق عليه لقب المحاربين الحراس الثمانية المدافعين عن هيمنة الأمريكية للإنترنت (وهي شركات سيسكو Cisco، و أي بي إم IBM وغوغل Google وكوالكوم Qualcomm وإنتيل Intel، وآبل Apple وأوراكل Oracle ومايكروسوفت Microsoft).[10] و رغم نجاح الشركات الصينية في إحراز تقدم كبير في سوق الأجهزة الإلكترونية (مثل موجهات هواوي Huawei، وهواتف زد.تي.إي ZTE، وهواتف شاومي النقالة Xiaomi)، إلا أن شركات الصين لم تتمتع بنفس القدر من النجاح في سوق البرمجيات. إذ يتطلب مجال البرمجيات القدرة على اختراع أو إعادة ابتكار أشياء جديدة لتشغل الأجهزة وأجهزة الكمبيوتر. كما يستفيد من تأثيرات الشبكة (أي، يضع قائد الأمس الاتفاقيات التي تجذب الناس لتتلاءم مع

[10] مقال كارلوس تيجادا (Carlos Tejada) بعنوان "مايكروسوفت المحاربون الحماة ومخاوف الصين بشأن الفضاء الإلكتروني،" بصحيفة وول ستريت جورنال *Wall Street Journal*، 29 يوليو/آذار 2014.

القائد الحالي، ما يجعل قائد الأمس هو قائد المستقبل). ولا تعد القدرة على الابتكار (على نقيض إجراء تحسينات بسيطة في التصميم الحالي) ولا القدرة على الاستفادة من النجاح السوقي المسبق، ميزة نسبية للصين.

وتقابل الصين مشكلة أخرى في الفضاء الإلكتروني وهي أنه: بينما قد تطمح إلى أن تكون قوة مهيمنة في شرق آسيا في العالم الفعلي، ليس هناك مغزى من أن تكون القوة المهيمنة في شرق آسيا في الفضاء الإلكتروني. فما هو قدر الهيمنة الذي تبتغي تحقيقه في الفضاء الإلكتروني؟ هل يكفي إبطال كل المزايا التي تحصدها الولايات المتحدة من كونها القوة المهيمنة العالمية في الفضاء الإلكتروني، أم ينبغي عليها أن تسعى لتكوين نوع من الاكتفاء الذاتي الإقليمي في الفضاء الإلكتروني؟

الإسناد في مقابل ارتباط القوى

إن الثقة في القدرة على تحديد من قام بشن هجمة إلكترونية هي مسألة هامة جدًا في نهج تطبيق القانون الذي يختص به الردع الأزرق، حتى أن بعض المحللين يتناقشون في ضرورة تطبيق معايير إثبات الذنب التي تتجاوز مجرد الشك قبل إنزال العقاب. وتقل أهمية الثقة في الإسناد عند الردع الأحمر، الذي يهتم أكثر بالقدرة على الانتقام والسيادة على من يريد الانتقام منهم.

من وجهة نظر الردع الأحمر، لا يكون السؤال هو "هل يمكننا إثبات أن الدولة (أ) ارتكبت هذا الأمر؟" بل "هل نستطيع إنزال العقاب على المعتدي المزعوم؟ وإن استطعنا ذلك، من سيتصدر القائمة؟ وفي مقابل ذلك، وحتى إن كان النصر غير محتمل، هل بوسعنا تحمل عدم التراجع إذا شكّل الضرر الناتج عن تعرضنا للهجوم بنجاح انطباعًا بالضعف؟" وفي ظل هذه الظروف، لا يتمثل المقياس السليم لتقييم متغيرات الانتقام لدى الردع الأحمر في درجة الثقة في استهداف المعتدي الفعلي بدقة، ولكن بالأحرى في تقييم تفاوت القوى النسبي والقدرة على الاستفادة من رد الفعل الانتقامي واستعادة السمعة. ومن ثم، من المرجح بشكل أكبر أن يتحرك الردع الأحمر كرد فعل لنمط الهجمات الذي يغير ميزان القوى أو يلوح بتغيير وشيك في ميزان القوى، وبالتالي ينبغي التصدي له. وعلى عكس ذلك، يغلب على الردع الأزرق الانتقام من اعتداء واحد فقط، ولا سيما إذا هدد ذلك الاعتداء سيادة القانون في الفضاء الإلكتروني إذا لم يُقابل بالعقاب.

وتبقى الولايات المتحدة في حالة غضب بسبب رفض الصين القطعي للإقرار بالهجمات الإلكترونية التي شنتها، رغم كثرة الأدلة على قيامها بذلك. فالصين دولة بلا

قوانين، في نظر الولايات المتحدة. وفي نظر الصين، تعد مساعي الولايات المتحدة لانتزاع اعتراف من الصين بمثابة حيلة لإجبار الصين على الخضوع لهيمنة الولايات المتحدة في الفضاء الإلكتروني.

التصعيد

إن كبح نزوع الطرف الآخر إلى التصعيد في الفضاء الإلكتروني أثناء النزاع يثير قضايا مماثلة لقضايا ردع الهجوم الأولي. والفارق الرئيسي هو أنه أثناء النزاع، غالبًا ما تكون معايير الإسناد أقل من مثيلتها فيما يخص الردع أثناء وقت السلم. وبالنسبة للردع الأزرق، فإن القدرة والاستعداد على التصرف سريعًا في حالة خرق هذه الحدود أمران أساسيان، كي لا يُرى التعدي الذي غُض الطرف عنه اليوم على أنه المستوى الجديد المعتاد من الهجمات الإلكترونية "المقبولة" (في سياق النزاع الأعم والأشمل).

ويفترض الردع الأحمر أن النزاع في الفضاء الإلكتروني هو أحد أوجه الصراع الأعم الذي هو أحد الأوجه الدائمة الوجود في المجتمع الدولي، حتى لو كان التقليل من قيمة هذه الصراعات أو نفي وجودها تمامًا مفيدًا في بعض الأحيان. وقد ترغب هذه الدولة كذلك في الحد من مجال النزاع ومحاولة إقناع الآخرين بعدم وجود مثل هذا النزاع لحثهم على تقليل حذرهم، أو لحماية سمعتها أو تقليل احتمال مواجهتها للانتقام (أو مزيج من هذه الدوافع الثلاثة). وفي العموم، يسعى الردع الأحمر إلى ضبط مستوى النزاع إلى الحد الذي يصب في مصلحته. وهكذا تقل احتمالية استخدام الردع الأحمر لنهج العصا والجزرة (الترغيب والترهيب) في محاولة لتنظيم طبيعة الهجمات الإلكترونية ذاتها التي يشنها الردع الأزرق. وطالما أن أحد الأطراف لا يمانع كثيرًا الانتهاكات الفردية للقواعد المفترضة، لا يحتمل أن تؤدي المواجهة بين الدولتين إلى تصعيد فوضوي، لأن كل طرف سيحاول أن يناظر (أو يتغلب على) انتهاكات الآخرين لإقناع الطرف الآخر بعدم تخطي حدوده. يتوافق هذا النمط السلوكي مع طبيعة الهجمات الإلكترونية، وتحديدًا تبعيتها لأشكال أخرى من النزاع ويتوافق مع صعوبة تحديد أية هجمات تعدت أية حدود بدقة.

قد تستدعي الواقعة الواحدة ردود فعل مختلفة من الطرفين، رغم ذلك. قد يتصرف الردع الأزرق بعنف تجاه فعل أجراه الردع الأحمر يستهدف توسيع نطاق الحرب الإلكترونية المقبولة (على سبيل المثال، عبر وضع أهداف جديدة أو إدخال الفساد في الأنظمة التي لم تتعرض لشيء إلا للأعطال في السابق). قد يباغت رد الفعل هذا التقييم الذاتي للردع الأحمر الذي يذهب إلى أن التصرف لم يظهر فرقًا في علاقات

القوى (أي أنه لم يغير خطاب النزاع أو العلاقة بين البلدين). وقد يتصرف الردع الأحمر بعنف تجاه هجوم شنه الردع الأزرق من شأنه تغيير علاقات القوى (أي مثلًا إضعاف الاستقرار الداخلي للردع الأحمر أو إضرار العلاقات بينه وبين البلدان الأخرى) وبالتالي يباغت الردع الأزرق الذي ظن أنه لم يكن يهاجم أي أهداف محظورة حتى هذه اللحظة (أو استخدم أساليب الهجوم الإلكتروني التي كانت تعد ممنوعة). وتؤدي الاختلافات الجوهرية فيما يعتبره كل طرف عملًا تصعيديًا إلى تصعيد من جانب كل طرف لأنه ظن أن الطرف الآخر بدأ في التصعيد بينما لم يكن التصعيد في نية أي من الطرفين.

الاستقرار

يرغب الطرفان في استقرار الفضاء الإلكتروني (أي غياب الظروف التي تشعل الهجمات الإلكترونية أو الحروب الحركية التي تبدأ بالهجمات الإلكترونية الفعلية أو المفترضة). لكن ربما يسعى كل طرف إلى الاستقرار بطريقته. أقرت الولايات المتحدة أن وضع الحدود والحفاظ عليها المقترن، بالضرورة، بإصرار الولايات المتحدة المفهوم على إنفاذ هذه الحدود هو ما يرسي الاستقرار. ولكن ما لم تعط الدول المعتدين المحتملين فرصة تفسير الشك، فإن ما يبدو على أنه هجوم إلكتروني – بينما قد يكون حادثة أو تقييمًا خاطئًا بأن واقعة التجسس الإلكتروني تشير في حقيقتها إلى هجوم إلكتروني وشيك - قد يشعل فتيل النزاع في عالم يستعد فيه كل طرف للانتقام من تجاوزات الآخرين.[11] وتشير الصين إلى أن التسلسل الهرمي المفهوم جيدًا للقوة يخلق توافقًا في الآراء بشأن نتائج تحدي النظام القائم، إذ لا يوجد سبب يدفع أي طرف فاعل في النظام إلى الاعتقاد بأنه يمكنه الاستفادة في نهاية المطاف من تصاعد مثل هذا التحدي. ونظريًا، قد يؤدي هذا النهج إلى زيادة الاضطرابات في وقت انتقال الهيمنة من دولة (التي لا تزال تصر على امتيازاتها) إلى أخرى (التي تتحدى الامتيازات). ومع ذلك، ما دامت الأنشطة في الفضاء الإلكتروني تعد مجموعة فرعية لمجموعة مؤشرات القوى الواسعة، لن تهم الاضطرابات التي تواجه فقط النظام القائم في الفضاء الإلكتروني عند حساب علاقات القوى الأعم.

---

[11] فعلى سبيل المثال، ما بدا على أن كوريا الشمالية دست البرمجيات الخبيثة في شبكات محطات الطاقة النووية بكوريا الجنوبية اتضح أنه برمجيات خبيثة عشوائية منتشرة على الإنترنت واقتحمت الشبكات الداخلية (لم تتأثر مفاتيح التحكم في المحطة النووية)؛ وانظر إلى مقال ميونغ تشو (Meeyoung Cho) بعنوان "إزالة 'دودة ' منخفضة المخاطر من محطة نووية تم اختراقها بكوريا الجنوبية ،" وكالة رويترز Reuters، 30 ديسمبر/كانون الأول 2014.

الإشارات

وتظهر المشكلات أيضًا إذا سعت الولايات المتحدة إلى قراءة إشارات الصين وأغفلت (أو قررت ألا تقر) بأن الصين تنظر إلى الردع من منطلق إطارها الخاص – والعكس صحيح. وقد تفسر الولايات المتحدة تصرفات الصين بأنها تحاول اختراق القواعد أو تؤسس قواعد مختلفة للسلوك الدولي، وقد تفسر الصين تصرفات الولايات المتحدة بأنها تجبر الصين على الخضوع لمركز القوى المرغوب للولايات المتحدة. ولربما تعتبر الولايات المتحدة إدانة الضباط الخمسة بجيش التحرير الشعبى الصينى في مايو/آيار 2014 إشارة بأنه لا يمكن للأفراد الذين يتصرفون بما يخالف قانون الولايات المتحدة الإفلات من العقاب على تصرفهم هذا. ومن جهة أخرى، قد يفسر الصينيون الإدانات بأنها محاولة من الولايات المتحدة لاستعراض قوتها خارج أراضيها ومن ثم الاعتداء على السيادة الصينية – وكان إنهاء الصين للمباحثات الرسمية حول الأمن الإلكتروني طريقتها في الرد على ذلك.[12]

وبالمثل، ناشدت الولايات المتحدة الصين بتضييق الخناق على استخدام كوريا الشمالية للإنترنت لتكون إشارة إلى كوريا الشمالية بأن الهجمات المدمرة، (أو على الأقل شديدة التخريب) ضد الشركات العالمية، تتجاوز حدود الممارسات المقبولة. لكن الصين، كما تشير التقارير، عزفت عن الضغط على كوريا الشمالية. وقد تنظر قيادة الصين إلى مشاركة كوريا الشمالية في اختراق شركة سوني Sony على أنها جزء صغير جدًا من علاقة أوسع نطاقًا – بينما قد يعطى أي إجراء تتخذه الصين شأنًا كبيرًا وينظر إليه كإشارة إلى أن الصين قد رضخت لضغوط الولايات المتحدة.

الفكرة الأعم هي أن الردع الأزرق يرد على الانتهاكات بينما يركز على علاقة القوى الأشمل بين الدول. ويعد خلق سابقة لمعاقبة الهجمات الإلكترونية أحد العوامل الكبيرة، وربما حتى الغالبة، في رغبة الولايات المتحدة في معاقبة كوريا الشمالية ، بغض النظر عن الطرف الذي شنها. وقال القائد العسكري بالقيادة الإلكترونية الأمريكية (USCYBERCOM)، الأدميرال مايكل إس. روجرز (Michael S. Rogers) إن "قضية سوني مهمة بالنسبة لي لأن العالم كله يشاهد كيف أننا كأمة سنتصرف تجاه

[12] وبالطبع، يحتمل أيضًا أن الولايات المتحدة لم تجد نتيجة للاعتراضات المرسلة على نحو خاص إلى جانب الصيني بشأن الاختراقات الإلكترونية وبالتالي سعت إلى فرض عقوبة على تصرفات الصين. وبتوجيه الإدانة المذكورة أعلاه، لربما شعر الصينيون ببساطة بتحد لمصالحهم وهيبتهم فسعوا إلى الرد بطريقة تهدف لدعم موقفهم وإعادة تشكيل صورتهم على أنهم ضحايا أبرياء.

هذا الأمر." وأضاف "إن لم نذكر الجاني باسمه هنا، فسوف يشجع ذلك الآخرين على التفكير 'بأن ذلك لا يمثل أحد المحظورات للولايات المتحدة.'"[13] فمقاومة الصين لا تعنى كثيرًا بالتغاضي عن الهجمات الإلكترونية بقدر ما تقلق بشأن علاقتها مع كوريا الشمالية والولايات المتحدة. بالنظر إلى الدول الأخرى، تجنح الولايات المتحدة إلى التحديد، بينما تجنح الصين إلى التعميم، وبالنظر إلى معايير السلوك، تجنح الولايات المتحدة إلى التعميم، بينما تجنح الصين إلى التحديد.

الخلاصة

ارتكز الردع بين الولايات المتحدة والاتحاد السوفيتي على مدى فترة كبيرة من الحرب الباردة، على الأقل على المستوى النووي، على التطابق النسبي للقدرات والتفاهم المتبادل بخصوص ما يعنيه الردع. كان للطرفين فكرة عامة عما ستكون عليه الخطوط المحظورة للطرف الآخر وفكرة عامة لما سيكون عليه رد فعل الطرف الآخر في حال تجاوز تلك الخطوط.

وقد لا يسري هذا الأمر في العالم المكون من نماذج ردع مختلفة اختلافًا جذريًا. من وجهة نظر الردع الأزرق، يعد تجاوز الحدود تصرفًا بحد ذاته، ويعرِّض الإخفاق في ملاحظة هذا التجاوز والرد عليه سيادة القانون للخطر. ومن وجهة نظر الردع الأحمر، تصبح الحدود منطقة واسعة، ويعتمد الرد، كليًا، على غزو هذه المنطقة على السياق الذي يحدث فيه هذا التعدي وعلى ما يعنيه هذا التعدي بخصوص فهم الطرف الآخر لعلاقات القوى النسبية. ولا تستحق التجاوزات الرد عليها إلا إذا أظهرت أن تصورات دولة ما عن دولة أخرى تتطلب التصويب، ولا يمكن تحديد ذلك دون اعتبار أحداث أخرى – قد لا يكون لها علاقة بالفضاء الإلكتروني. وفعلًا، تعتمد حسابات الولايات المتحدة بخصوص الرد أو عدمه على أحداث لا تتعلق بآخر طرف تخطى حدوده. وفي حالة شركة سوني، لابد أن الولايات المتحدة وضعت في حسبانها عمل قرصنة سابق على شركة لاس فيغاس ساندز Las Vegas Sands Corporation (منسوب إلى إيران إلى حد كبير) وتوصلت إلى ضرورة التصرف بشكل ما بشأن مسألة سيادة القانون في الفضاء الإلكتروني. من المرجح أن تربط الصين بين الأحداث التي تقع في الفضاء

---

[13] سام فريتسيل (Sam Frizell) "مدير وكالة الأمن القومي متحدثًا بشأن اختراق شركة سوني: 'العالم بأكمله يراقبنا'،" بمجلة التايم *Time*، 8 يناير/كانون الثاني 2015.

الإلكتروني بالسياق الأعم لتصرفات الدولة الأخرى، بينما تنظر الولايات المتحدة على الأغلب إلى الأحداث في الفضاء الإلكترني في سياق هذا المجال. وعندما نحاول تفسير سبب ضرورة عقاب كوريا الشمالية للاعتداء على سوني – وهي سياسة اعتمدها رئيس الولايات المتحدة – سنرى أن قائد القيادة الإلكترونية الأمريكية يؤيد الانتقام لأن العالم يشاهد كيف سنتصرف تجاه الاعتداء – لكننا لا نرى أن رئيس قيادة المحيط الهادئ الأمريكية يذهب إلى إن ذلك كان يشكل عنصرًا أساسيًا في علاقة الولايات المتحدة مع كوريا الشمالية.

إن العالم الذي تتحكم فيه القوى الرئيسية في النظام الدولي بنموذجي ردع متباينين بشكل بكبير، يتطلب فهم كل طرف للردع من منظور الطرف الآخر. إن التوصل إلى الآلية العقلية المرنة اللازمة لتحقيق ذلك لا يعد أمرًا صعبًا فحسب بل يفترض أيضًا ألا ينظر كل طرف للطرف الآخر بعين الخصومة فقط.

التوصل إلى الوضع الحالي

تأثرت العلاقة بين الولايات المتحدة والصين كثيرًا بما تظن كل دولة أن الدولة الأخرى تقوم به ضدها فيما يتعلق بالفضاء الإلكتروني. وفي هذا الفصل، نستعرض تاريخ علاقة البلدين في الفضاء الإلكتروني ونصف منظور كل دولة لأنشطة الدولة الأخرى. ومن أجل ذلك، نستمد معلوماتنا من التقارير الإعلامية مفتوحة المصدر وكذلك مؤلفات الخبراء المختصين من الولايات المتحدة والصين بشأن الأمن الإلكتروني. كما نعتمد على مشاركتنا في تسع جولات من المباحثات غير الرسمية بشأن الأمن الإلكتروني بين مركز الدراسات الاستراتيجية والدولية ومعاهد الصين للعلاقات الدولية المعاصرة.

نبدأ بعرض تصورات الولايات المتحدة للصين بشأن الأمن الإلكتروني بالتفصيل. يلعب امتعاض الولايات المتحدة من سلوك الصين في الفضاء الإلكتروني دورًا كبيرًا في رأيها الإجمالي بالصين، بينما تلعب مخاوف الصين تجاه سلوك الولايات المتحدة في الفضاء الإلكتروني دورًا أقل تأثيرًا في نظرتها الكلية للولايات المتحدة. وحسب ما قاله لنا أحد المتحاورين الصينيين "قد تعتبر الولايات المتحدة الأمن الإلكتروني من أولوياتها الخمس مع الصين، لكن بالنسبة لنا، فقد يأتي من بين أهم عشر أو حتى عشرين قضية بيننا وبينكم."[1]

كانت الصراعات الأولى حول الفضاء الإلكتروني بين الولايات المتحدة والصين أمورًا فردية بحتة. وبعد الأحداث التي وقعت في العالم الفعلي، مثل تفجير سفارة الصين في بلغراد عام 1999 وحادثة الطائرة من طراز EP-3 بالقرب من جزيرة هاينان في 2001، اجتهد القراصنة من الطرفين في تشويه المواقع الإلكترونية في الدولة الأخرى. زادت العواقب قليلًا عن كونها مجرد مضايقات خفيفة، لكنها عملت

[1] مقابلة في بكين، مايو/آيار 2015.

على تكوين وتعزيز انطباع لدى الولايات المتحدة بأن الصين استخدمت الخوادم الوكيلة (البروكسي) في المقام الأول لشن الهجمات الإلكترونية سواء الصغيرة أو الكبيرة. وبمرور الوقت، توصلت التقييمات الأمريكية المختصة إلى أن عمليات الصين في الفضاء الإلكتروني، سواء كانت قد استخدمت "المناضلين الإلكترونيين" الوطنيين في البداية أم لم تستخدمهم، قد تطورت حتى أخذت شكل عملية أكثر مركزية إلى حد كبير، وتولت المنظمات العسكرية والاستخباراتية أعمال القيادة والتحكم.[2]

التجسس الإلكتروني في الصين

مع استثمار كل من الولايات المتحدة والصين في الأنظمة الشبكية (كما يسميها الصينيون *xinxihua* أو *informatization*)، مارس الطرفان التجسس الإلكتروني ضد بعضهما البعض (وضد أطراف أخرى) لأغراض كثيرة. ويرجع أحد الأسباب إلى احتفاظ الولايات المتحدة بهيمنتها وسيطرتها الفعالة على القراصنة التابعين لها، والذين حافظوا على الأمن التشغيلي بمعايير عالية جدًا، فكل ما هو معروف عن القرصنة التي أجرتها الولايات المتحدة والصين يأتي من الإلمام بالقرصنة الصينية.

تصاعدت مشكلة الولايات المتحدة مع أنشطة الصين في الفضاء الإلكتروني على مدى عدة أعوام، وبدأت في أوائل العقد الأول من القرن الحالي. من ضمن الهجمات المنسوبة إلى الصين، الاختراقات المعروفة باسم تيتان رين في معامل وزارة الطاقة ما بين 2003 و2005، بالإضافة إلى الهجمات اللاحقة التي استهدفت المؤسسات الدفاعية مثل كلية الحرب البحرية وكلية الدفاع الوطني.[3] أدت هذه الهجمات إلى إيقاف التشغيل لفترة طويلة حتى يتأكد المسؤولون عن الإشراف أن جميع الأنظمة خضعت للتنظيف الدقيق وأنه لا خطورة من كشف البيانات السرية. وأدت الهجمات

---

[2] Brian Krekel, George Bakos, and Christopher Barnett, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, Washington, D.C.: لجنة استعراض الاقتصاد والأمن بين الولايات المتحدة والصين، 2009؛ انظر أيضًا مانديانت 2013 ومقال نايجل إنكستر (Nigel Inkster) بعنوان "الاستخبارات الصينية في عصر الفضاء الإلكتروني،" *Survival*, المجلد 55، رقم 1، فبراير/شباط – مارس/آذار 2013، ص 66-45.

[3] مقال نيثان ثورنبور (Nathan Thornburgh) بعنوان "خفايا الهجوم الاختراقي الصين،" التايم *Time*، 25 أغسطس/آب 2005.

على وزارة التجارة الأمريكية (التي تتعامل مع ضوابط التصدير والاستيراد) إلى تغيير الموظفين لجميع أجهزتهم لإعادة السيطرة على أنظمتهم. وضرب اختراق آخر وزارة الخارجية.[4] واستهدفت إحدى الهجمات الجريئة جدًا، والتي كُشف عنها عام 2007، الأجهزة في وزارة الدفاع، بما في ذلك الكمبيوتر الشخصي لوزير الدفاع.[5] إضافة إلى ذلك، أثناء خوض عضوي مجلس الشيوخ جون ماكين (John McCain) وباراك أوباما الانتخابات الرئاسية، تم إبلاغهما أن القراصنة الصينيين اخترقوا أنظمة الكمبيوتر في مقرات حملتيهما الانتخابيتين.[6]

وتعززت سمعة الصين بأنها طرف قوي في الفضاء الإلكتروني مع اختراق برنامج مقاتلات لوكهيد مارتن إف-35 لايتنيغ II الذي كان هدفه سحب بيانات بحجم عدة تيرابايتات.[7] ويشاع أن القراصنة استولوا على بيانات غير سرية فقط، ولم يكن أغلبها مفيدًا، لأن المعلومات حول المقاتلة من طراز إف-35 كانت محدودة. وفي الواقع، تعلمت الصين، على الأرجح، الكثير عن صناعة الطائرات النفاثة المتطورة بواسطة معدات الهندسة العكسية التي حصلت عليها من روسيا. وربما تعلمت الصين أيضًا ما يتعلق بدمج الأنظمة بشكل عام، لكن يبقى هذا الأمر مجرد تخمين. وتصر الشائعات على احتمال حصول الصين على معلومات تعادل بيانات فائقة السرية مع مجموعة البيانات غير السرية المسروقة. وفي أواخر 2009، اكتشفت غوغل Google أنها تعرضت أيضًا للهجوم (عبر سرقة مستودع الشيفرات التابع لها على وجه الخصوص) من أفراد تسللوا إليها عبر خادم في تايوان في اتجاه الصين، وأطلق الباحثون الذين اكتشفوا حادثة الاختراق هذه لقب "العملية أورورا" عليها. وكان العنصر الجديد في الهجوم على غوغل هو استعداد الشركة لمناقشة الموضوع، وإقناع الحكومة الأمريكية بإثارة الحادثة كقضية دولية مع الصين. وكانت شركة غوغل تقع تحت ضغط من

---

[4] كرستين لاغوريو (Christine Lagorio) "اختراق أجهزة كمبيوتر وزارة الخارجية،" وكالة أخبار سي بي إس CBS News، بتاريخ 11 يوليو/تموز 2006.

[5] انظر إلى تقرير مركز الدراسات الاستراتيجية والدولية (CSIS) بعنوان "أحداث الفضاء الإلكتروني البارزة منذ 2006،" 10 مارس/آذار 2014.

[6] تقرير بريندان ساسو (Brendan Sasso): "اختراق الصين لحملتي أوباما وماكين في 2008،" صحيفة ذا هيل *The Hill*، 7 يونيو/حزيران 2013.

[7] مقال لشيبان غورمان (Siobhan Gorman) وأوغاست كول (August Cole) ويوتشي دريزان (Yochi Dreazen) بعنوان "جواسيس الكمبيوتر يتسللون إلى مشروع طيارة محاربة،" ذا وال ستريت جورنال *Wall Street Journal*، 21 أبريل/نيسان 2009.

الحكومة الصينية بسبب مقاومة مطالب لفرض رقابة على نتائج البحث مع رغبتها في المنافسة في السوق الصينية ضد شركة بايدو Baidu، وهو محرك بحث منافس، وأعلنت غوغل في الوقت نفسه أنها ستوقف خدمتها الداخلية في الصين وستنقل مستخدميها في الصين إلى موقعها في هونغ كونغ. وهذا يعني أن نتائج البحث في الصين لن تخضع لرقابة غوغل، رغم أن المستخدمين سيكون عليهم المرور سور الصين "الناري" العظيم Firewall عند إجراء البحث. وأوضحت سلسلة هجمات أخرى، تعرف باسم شادي رات Shady RAT كما أطلق عليها الباحثون الذين قاموا باكتشافها في شركة مكافي McAfee، مدى اجتهاد القراصنة الصينيين. وجد الباحثون خادمًا يحتوي على ملفات مسروقة من 74 شركة مخترقة، وكان جميعها مخزنًا بشكل مؤقت لاسترجاعها في وقت لاحق.[8] وكانت أغلب الشركات - وليس جميعها - في الولايات المتحدة، وتنوع مجال أعمالها بين الصناعة والعقارات التجارية.

في عام 2011، تم اختراق شركة آر إس أيه RSA التي تبيع أنظمة التوثيق متعدد العوامل. يُشاع أن المخترقين تمكنوا من اقتحام الأنظمة التي احتفظت بخوادم توثيق شركة RSA، ما مكنهم من اقتحام الأنظمة التي كانت تحميها منتجات RSA. وبعد مرور عدة أشهر على الهجوم، استخدم المخترقون معلومات مجمعة من الهجوم لاستهداف شركة لوكهيد مارتن Lockheed Martin، إلا أنه تم إحباط الهجوم على ما يبدو.[9]

وفي عام 2011، نُفذ هجوم إلكتروني ضد شركات النفط من أجل تحديد طريقة تقييمها لبعض بقع النفط والعطاءات التي كانوا يستعدون لها.[10] وقد تكون هذه المعلومات ذات قيمة هائلة لشركات النفط المتنافسة، إذ تتمكن حينها من تحديد قيمة

---

[8] استولى المخترقون على الملفات، ثم أرسلوها إلى خادم آخر لتجميعها، ثم استلموها في مرحلة لاحقة (أي "أرسلوها بالبريد إلى الوطن"). قد يكون تم تخزين الملفات على الخادم مؤقتًا استعدادًا لإرسالها لاحقًا. على الأرجح، لم يكتشف الملفات أصحابها الأصليون ولكن عن طريق طرف ثالث متخصص في البحث عن هذه الملفات، لم يُجرَ هذا التحري بإيعاز من جميع المنظمات التي وصلت ملفاتها إلى الخادم. لكن ربما سددت إحدى هذه المنظمات ثمن هذا التحري.

[9] مقال لماثيو جيه شوارتس (Matthew J. Schwartz) بعنوان "لوكهيد مارتن تعاني من هجوم إلكتروني عنيف،" المنشور بمجلة إنفورميشن ويك دارك ريدنغ *InformationWeek Dark Reading*، 30 مايو/آيار 2011.

[10] خدمات مكافي فاوندستون المهنية ومعامل مكافي، الهجمات الإلكترونية العالمية على الطاقة: "تنين الليل" مستندات حكومية، سانتا كلارا، كاليفورنيا: شركة مكافي، 10 فبراير/شباط 2011. انظر أيضًا مستند كتبه ديميتري ألبيروفيتش (Dmitri Alperovich)، عنوانه الكشف عن العملية شادي رات *(الجرذ المتخفي)*، مستندات حكومية، سانتا كلارا، كاليفورنيا: شركة مكافي، 3 أغسطس/آب 2011

حقوق التنقيب وكيف تزيد قليلًا على كبرى شركات النفط عند عرض هذه الملكيات للإيجار. وأثبتت شركات المحاماة، مصادفة، أنها تعد أهداف سهلة لهذه الاختراقات لأنها تحتفظ ببيانات ثرية لكنها بطبيعة الحال ليست من ضمن الشركات واسعة الخبرة بالكمبيوتر (وليست بالضخامة التي تمكنها من الحصول على موظفين تكنولوجيا معلومات متمكنين).[11]

اشتدت الاختراقات الصينية حتى أن رئيس إدارة الأمن الإلكتروني التابع لمكتب التحقيقات الفيدرالي شون هنري (Shaun Henry) قال "هناك نوعان من الشركات: الشركات التي تعرضت للاختراق والشركات التي لا تعرف أنها تعرضت للاختراق."[12]

ولكن لسخرية القدر، يبدو أن الصين تعاني من المهارات المحدودة.[13] فلم تكن محاولات إخفاء أثر اختراق البرمجيات الخبيثة أو سحب البيانات فعالة بالقدر الكافي. فحقيقة أن الملفات التي وجدت على خوادم وسيطة لم تكن مشفرة تعني أنه من يجد هذه الملفات يمكنه قراءتها وتخمين مصدرها وإبلاغ الضحايا، ما يمكنهم من وقف الضرر الناتج عنها. أي شخص يستخدم الطريقة نفسها لاختراق 33 شركة، على طراز عملية أورورا، يخاطر بانهيار جهوده الاختراقية بأكملها عند اكتشاف الاختراق الأول. في عام 2012، نشرت وكالة الأمن القومي تقديرات تفيد بمسؤولية أكثر من عشر جماعات في الصين عن معظم عمليات الاختراق التهديدية المتقدمة.[14] لم يُتخذ أي إجراء فعال ضد المخترقين، ولعل هذا هو السبب وراء عدم بذل مجهود كبير في إخفاء آثارهم.

---

[11] مقال مايكل أيه رايلي (Michael A. Riley) وصوفيا بيرسون (Sophia Pearson) بعنوان "مخترقون صينيون يستهدفون شركات المحاماة للحصول على بيانات تخص التعاقدات السرية،" المنشور بصحيفة بلومبرغ Bloomberg، 31 يناير/كانون الثاني 2012.

[12] مقال بعنوان "شركة نيسان أحدث شركة تتعرض للاختراق،" للكاتبة نيكول بيرلروث المنشور بصحيفة نيويورك تايمز *New York Times*، بتاريخ 24 أبريل/نيسان 2012.

[13] ديفيد كرافيتس، "رئيس مكتب التحقيقات الفيدرالية يصف المخترقين الصينيين باللصوص السكارى" موقع آرس تكنيكا *Ars Technica* 6 أكتوبر/تشرين الأول 2014. ويُذكر أن الرئيس شي طالب بمهارات أفضل بعد شكاوى الرئيس أوباما أثناء قمة ساني لاندز في يونيو/حزيران 2013.

[14] "اثنتا عشرة مجموعة اختراق صينية هي مسؤولة عن الهجمات على الولايات المتحدة،" من وكالة أنباء الأمن الداخلي Homeland Security News Wire، 16 ديسمبر/كانون أول 2011. أشارت تقديرات لاحقة إلى 20 مجموعة، انظر مقال داني يادرون (Danny Yadron)، وجيمس تي آريدي (James T. Areddy) وبول موزور (Paul Mozur) بعنوان "عمق وتنوع اختراقات الصين، على حد تأكيدات الخبراء" ذا وول ستريت جورنال *Wall Street Journal*، 29 مايو/آيار 2014.

بينما تدعي الصحافة الصينية أن اتهامات الولايات المتحدة لها بالتجسس الإلكتروني لا تتعدى كونها تلفيقات دعمها "مفهوم الحرب الباردة" الأمريكي الذي عفا عليه الزمن،[15] ليست الولايات المتحدة الدولة الوحيدة التي تتصور أنها تتعرض لاختراقات إلكترونية متواصلة من القراصنة الصينيين. وردت اتهامات من ألمانيا (وتحدثت رئيسة الوزراء أنجيلا ميركل (Angela Merkel) بهذا الشأن شخصيًا مع نظرائها الصينيين)،[16] والمملكة المتحدة[17] (التي حذرت الشركات علنًا من هذه التهديدات)، وفرنسا[18] وكندا[19] وأستراليا[20] وإسرائيل[21] وتايوان[22] واليابان[23] ورابطة دول جنوب شرق آسيا[24] والهند.[25]

---

[15] "تشاينا فويس (صوت الصين): إلقاء عقلية الحرب الباردة على الأمن الإلكتروني الصيني،" المنشور بصحيفة شينخوا Xinhua، 22 أبريل/نيسان 2014.

[16] "تقرير الجاسوسية: زيارة ميركل للصين أفسدتها مزاعم بالاختراق،" شبيغل الإلكترونية، 27 أغسطس/آب 2012. انظر أيضًا "هجوم المخترقين الصينيين على الحكومة والشركات الألمانية" وانت تشاينا تايمز *Want China Times*، 26 فبراير/شباط 2013.

[17] مركز الدراسات الإستراتيجية والدولية، 2014.

[18] إليوت سيفتون (Eliot Sefton)، "الصين اخترقت وزارة فرنسية للحصول على بيانات بشأن مجموعة العشرين" المنشور بصحيفة ذا ويك *The Week*، 8 مارس/آذار 2011.

[19] "اختراق الجواسيس الصينيين لمجلس الأبحاث الوطني الكندي" من موقع البي بي سي BBC، 29 يوليو/أذار 2014.

[20] مقال للكاتب روب تايلور (Rob Taylor) بعنوان "سرقة المخترقين الصينيين لخطط المقر الرئيسي لمبنى المخابرات الأسترالي: تقرير،" رويترز، 27 مايو/آيار 2013؛ والكاتب ديلان ويلش (Dylan Welch) بعنوان "اختراق القراصنة الصينيين للمؤسسات الإعلامية الأسترالية قبيل اجتماع مجموعة العشرين،" المؤسسة الإعلامية الأسترالية Australian Broadcasting Corporation، 13 نوفمبر/تشرين الثاني 2014.

[21] مقال لجو ميلر (Joe Miller) بعنوان "تسلل المخترقين الصينيين إلى شركات القبة الحديدية الإسرائيلية شبكة البي بي سي BBC، 31 يوليو/تموز 2014.

[22] مقال لشانون تيسي (Shannon Tiezzi) بعنوان "شكاوى من تايوان بسبب هجمات إلكترونية شديدة من الصين،" من مجلة ذا ديبلومات *The Diplomat*، 15 أغسطس/آب 2014.

[23] مقال لمونامي يوي (Monami Yui) وشينغو كاواموتو (Shingo Kawamoto) بعنوان "اتهامات لمجرمين صينيين بسرقة بنك باليابان إلكترونيًا" Bloomberg، 17 ديسمبر/كانون الأول 2014.

[24] مقال لتيم كولبان (Tim Culpan) بعنوان "هجوم إلكتروني تجسسي لمدة عقد يخترق أهدافًا جنوب شرق آسيوية،" Bloomberg، 12 أبريل/نيسان 2015.

[25] مقال لجون ماركوف وديفيد باربوزا بعنوان "الباحثون يتقفون أثر سرقة البيانات ويتبينون أنها تنبع من المتسللين بالصين،" نيويورك تايمز *New York Times*، 5 أبريل/نيسان 2010.

وأخيرًا، يتفق التجسس الإلكتروني مع النهج الأشمل للصين نحو جمع المعلومات والاستحواذ على الملكية الفكرية القيمة من الناحية الاستراتيجية. وأدين عدد كبير من الأفراد الصينيين في الخارج بسبب عمليات تجسس فعلية أو عمليات سرقة الملكيات الفكرية أو معلومات تخص الملكية التجارية.[26] على سبيل المثال، أوضحت التقديرات أن هناك نسخة واحدة فقط من بين كل عشر نسخ من نظام تشغيل "مايكروسوفت ويندوز" Microsoft Windows استخدمت في الصين في بداية عام 2011 كانت أصلية، ويفترض أن النسخ غير القانونية أكثر عرضة للاختراق من غيرها، وهي حقيقة توضح مدى هشاشة البنية التحتية للصين في وجه الهجمات الإلكترونية من الدول الأخرى.[27] كثيرًا ما تتأخر طلبات لاستيراد المنتجات في الصين أو بدء التصنيع في الصين بسبب مطالب بتقديم قدر كبير من ملكية الشركات الفكرية للشركات المحلية قبل حصولها على إذن للدخول في السوق الصينية. اتهم أيضًا عدد كبير من المحللين الأجانب الصين بالتلاعب بمعايير تكنولوجيا المعلومات للإبقاء على مزاياها في السوق المحلية ولمنح الشركات الصينية الصدارة في اقتحام الأسواق الخارجية.

من ضمن المخاوف الأمريكية الأخرى استهداف المخترقين الصينيين للبنية التحتية الحيوية الأمريكية في محاولة لاستغلال المجتمع والاقتصاد الأمريكي كرهينة في حالة نشوب مواجهة كبرى بين الدولتين. في عام 2011، على سبيل المثال، حاول مسؤول بوزارة الدفاع الأمريكية التوضيح للصين أن اختراقها لأنظمة خطوط أنابيب الغاز الطبيعي يعد خطًا أحمر للولايات المتحدة.[28] كما أن اختراق شركة تيلفينت

---

[26] على سبيل المثال، مقال يوديت باتاشارجي (Yudhijit Bhattacharjee) بعنوان "نوع جديد من الجواسيس: كيف تستولي الصين على الأسرار التكنولوجية الأمريكية،" المنشور بجريدة ذا نيويوركر *New Yorker* بتاريخ 5 مايو/آيار 2014 (عن العمليات ضد شركة بوينج) ومقال كارين غولو (Karen Gullo) بعنوان "إدانة رجل من سكان كاليفورنيا بسرقة أسرار صناعية تخص شركة دوبون" المنشور بجريدة بلومبرج بيزنس *Bloomberg Business* بتاريخ 5 مارس/آذار 2014 (عن العمليات ضد شركة دوبون).

[27] في بحث أجري برعاية شركة مايكروسوفت، يقول جانتز (Gantz) وآخرون أن النسخ غير القانونية هي أكثر عرضة للبرمجيات الخبيثة (لكن يجب الرجوع للمصدر). انظر بحث جون إف. جانتز (John F. Gantz) وآخرون بعنوان "العالم الخطير للبرمجيات المزيفة والمقرصنة *The Dangerous World of Counterfeit and Pirated Software*: كيف أنه في وسع البرمجيات المقرصنة أن تعرض الأمن الإلكتروني للمستهلكين والشركات والدول للخطر...وكذلك تكاليفها التالية على الوقت والمال فرامنغهام، ماساتشوستس: شركة البيانات الدولية International Data Corporation 2013.

[28] مقال لمارك كلايتون (Mark Clayton) بعنوان "حصري: الهجمات الإلكترونية تعرض خطوط الغاز الطبيعي للتخريب،" المنشور بشبكة كريستشان ساينس مونيتور *Christian Science Monitor*، 27 فبراير/شباط 2013.

Telvent، وهي الشركة الكندية التي تمد قطاع الغاز الطبيعي الأمريكي بأنظمة التحكم، قد لامس وترًا حساسًا.[29]

في عام 2013، اعتبر مدير الاستخبارات الوطنية الهجوم الإلكتروني الواسع النطاق على البنية التحتية الحيوية للدولة (وكانت شبكة الكهرباء أهم جزء منها) أكبر تهديد قصير المدى على أمن الدولة.[30] وفي العام التالي، أقر مدير وكالة الأمن القومي، الأدميرال مايكل إس. روجرز، بإمكانية أن تقوم الصين، وربما غيرها من الدول، بإلحاق الضرر بشبكة الكهرباء الأمريكية.[31]

استراتيجية الولايات المتحدة الدولية للفضاء الإلكتروني لعام 2011

تصف استراتيجية الولايات المتحدة الدولية للفضاء الإلكتروني لعام 2011 عالمًا ترغب الولايات المتحدة في رؤيته لكن من الواضح أنه يتطلب توقف وتجنب الأطراف الأخرى، وتحديدًا الصين، عن بعض السلوكيات. إذ تناشد المجتمع الدولي بتكوين إجماع رأي بخصوص مبادئ السلوك المسؤول في الفضاء الإلكتروني، وتستشهد بمعاهدة بودابست بشأن الجرائم الإلكترونية (التي تلزم الموقعين عليها بدعم الجهود الدولية لحل الجرائم الإلكترونية، بما فيها التجسس الإلكتروني) كمثال على ما تراه نهجًا نافعًا. وأكدت الاستراتيجية على أن إحدى قواعد السلوك المسؤول هي: "على الدول تحديد ومقاضاة المجرمين الإلكترونيين...والتأكيد على أن القوانين والممارسات

---

[29] مقال لبريان كريبز (Brian Krebs) بعنوان "اتهام القراصنة الصينيين بالتسلل إلى شركة صناعات الطاقة تيلفينت Telvent،" من مدونة تقارير كريبز عن الأمن *Krebs on Security*، 12 سبتمبر/أيلول 2012.

[30] الصفحة الأولى من جيمس أر. كلابر (James R. Clapper) "بيان السجل: تقييم المخاطر العالمية على جماعة الاستخبارات الأمريكية،" واشنطن العاصمة: صرح مدير الاستخبارات الوطنية في 26 فبراير/شباط 2015

> نعتقد بأن هناك احتمال بعيد بتعرض أنظمة البنية التحتية الحيوية للولايات المتحدة لهجمات إلكترونية كبيرة خلال العامين المقبلين من شأنها تعريض الخدمات للتعطل لفترات طويلة وعلى نطاق واسع مثل انقطاع الكهرباء في المنطقة.... رغم ذلك، تستطيع الأطراف الفاعلة محدودة التطور ولكن شديدة الحماس أن تصل إلى الشبكات الأمريكية ذات الحماية الضعيفة التي تتحكم في الوظائف الأساسية مثل توليد الكهرباء، على مدى العامين التاليين، لكن قدرتها على الاستفادة القصوى من هذا الوصول لإحداث الأعطال الشديدة القوة والمنهجية ستكون محدودة على الأغلب. وفي الوقت نفسه، هناك خطر أن تتسبب الهجمات غير المتطورة بعواقب وخيمة نظرًا للتكوينات والأخطاء غير المتوقعة في النظام، أو قد يمتد الضعف الموجود في عقدة واحدة ليفسد الأجزاء الأخرى من النظام الشبكي.

[31] Dilanian, 2014.

تحجب الملاذات الآمنة عن المجرمين، والتعاون مع التحقيقات الجنائية الدولية دون تأخير،" وبالإضافة إلى ذلك "على الدول إدراك وتحمل مسئوليتها لحماية البنى التحتية المعلوماتية وتأمين الأنظمة المحلية ضد الدمار أو سوء الاستخدام."[32] يجب أن تضمن الدول أن المخترقين لا يستخدمون شبكاتها لشن هجمات على أنظمة الدول الأخرى – في ضوء احتجاجات الصين بأن أطرافًا أخرى دائمًا ما تستغل شبكات الصين غير المؤمنة للهجوم على أهداف غربية – والتأكد من تأمين الدول لشبكاتها بحيث يستحيل شن هذه الهجمات العابرة.

وانصب رد فعل الصين على إصدار الاستراتيجية جزئيًا على مخاوفها بشأن الكيفية التي تقترحها الولايات المتحدة للرد على الهجمات الإلكترونية. ويرد في الاستراتيجية في الصفحة رقم 10 الآتي: "بالتوافق مع ميثاق الأمم المتحدة، تمتلك الدول الحق الأصيل في الدفاع عن النفس الذي قد تدفعه الأعمال العدائية في الفضاء الإلكتروني،" ويُستكمل الحديث في هذه النقطة في الصفحة رقم 14:

> عند الضرورة، سترد الولايات المتحدة على الأعمال العدائية في الفضاء الإلكتروني بنفس الطريقة التي ترد بها على أي تهديد تواجهه بلادنا. تتمتع كل الدول بالحق الأصيل في الدفاع عن النفس، وندرك بأن بعض الأعمال العدائية التي ارتكبت عبر الفضاء الإلكتروني قد تفرض بعض الإجراءات بموجب الالتزامات بيننا وبين شركائنا في المعاهدات العسكرية. ونحتفظ بالحق في استخدام جميع الوسائل اللازمة – الدبلوماسية، والمعلوماتية، والعسكرية، والاقتصادية – بما يلائم ويتفق مع القانون الدولي المعمول به، من أجل الدفاع عن وطننا وحلفائنا وشركائنا ومصالحنا. وفي تلك الأثناء، سنستنفد جميع الخيارات قبل خيار القوة العسكرية على قدر استطاعتنا، سنجري تقييمًا دقيقًا لتكاليف ومخاطر اتخاذ إجراء في مقابل تكاليف عدم اتخاذ إجراء، وسنتصرف بطريقة تعكس قيمنا وتعزز شرعيتنا، وسنطلب الدعم الدولي الواسع كلما كان ذلك ممكنًا.

---

[32] البيت الأبيض، الاستراتيجية الدولية بشأن الفضاء الإلكتروني: الرخاء والأمن والصراحة في عالم مترابط إلكترونيًا، واشنطن العاصمة، مايو/آيار 2011، ص 10.

تفاعلت الصين مع هذه الفقرة تحديدًا ولابد أنها وصلتها تصريحات أحد القادة العسكريين الأمريكين الذي لم يكشف عن اسمه: "إذا عطلتم شبكة الكهرباء الخاصة بنا، لربما نضع قذيفة في مدخنة من مداخنكم."[33]

مانديانت وسنودن وجيش التحرير الشعبي الصيني 5

جاء وابل من الأحداث غير المتوقعة ليعيد ترتيب المواجهة بين الولايات المتحدة والصين بشأن الفضاء الإلكتروني بين العامين 2013 و2014.

وصدر في فبراير/شباط 2013 تقرير شركة مانديانت (Mandiant) وهي شركة أمن إلكتروني متخصصة في التحريات الجنائية (اشترتها شركة فاير آي FireEye لاحقًا)، الذي قدم أدلة وفيرة على تورط مجموعة واحدة على الأقل، وهي الوحدة 61398، التابعة لجيش التحرير الشعبي الصيني في أكثر من 100 اختراق مختلف لـ 20 قطاع مختلف من الاقتصاد الأمريكي بدأت في 2006.[34] وكانت هذه هي القضية العلنية الأولي التي تم الربط فيها بين التجسس الإلكتروني ذي الدوافع الاقتصادية وبين الصين، وليس فقط الصين نفسها بل الحكومة الصينية أيضًا (لا المخترقين الأفراد).[35] ومنذ ذلك الوقت، تم التعرف على مجموعات اختراق أخرى، وأغلبها له علاقة إما بجيش التحرير الشعبي الصيني أو وزارة أمن الدولة الصينية.[36] وأدى التطوير الذي شهدته قدرة الولايات المتحدة الإسنادية (في القطاعين العام والخاص) منذ منتصف

---

[33] انظر، على سبيل المثال، آدم سيجال (Adam Segal) "ردود فعل الصين على الاستراتيجية الدولية للفضاء الإلكتروني،" مجلس العلاقات الخارجية Council on Foreign Relations، 23 مايو/آيار 2011؛ شو وا (Zhou Wa) "تنظيم الإنترنت هو مسألة سيادية: وزير الخارجية، "تشاينا ديلي *China Daily*، 20 مايو/آيار 2011؛ وشيبان غورمان (Siobhan Gorman) وجوليان إي بارنز (Julian E. Barnes) "المعركة الإلكترونية: عمل عسكري،"وال ستريت جورنال *Wall Street Journal*، 31 مايو/آيار 2011.

[34] مانديانت، 2013.

[35] يمكن الاستدلال على أهمية هذا التمييز من الجدال الذي يخوض فيه المسئولون الصينيون دائمًا: لدينا 600 مليون صيني على الإنترنت ولا يمكننا مراقبتهم جميعًا. ويفترض أن الصينيين لن يشيروا إلى عدم إمكانية مراقبة موظفي جيش التحرير الشعبي الصيني.

[36] انظر مثلًا تقرير نوفيتا (Novetta) بعنوان "ائتلاف الأمن الإلكتروني يصدر تقريره الكامل حول المنع الموسع لجهود التجسس التي ترعاها الدولة الصينية،" واشنطن، 28 أكتوبر/تشرين الأول 2014 (يبدو أن شركة سيمانتك Symantec تتحدث عن مشروع إلدرود بروجيكت Elderwood Project بلقبه الفرعي *Axiom*).

2012 على الأقل إلى زيادة التوترات بين المسؤولين الأمريكيين ونظرائهم الصينيين بشأن قضية التجسس الإلكتروني ذي الدوافع الاقتصادية.[37] كانت هذه القضية على رأس المباحثات في قمة ساني لاندز في يونيو/حزيران 2013. وبعد القمة، ناقش المستشار بوكالة الأمن القومي توماس إي. دونيلون (Thomas E. Donilon) هذه القضية بمزيد من التفصيل في خطاب مهم له، وذهب وزير المالية جاك ليو (Jack Lew) إلى الصين في مهمة رسمية للتأكيد على هذه القضية.[38]

لكن في عشية القمة، سافر إدوارد سنودن - المسؤول السابق بوكالة الأمن القومي الأميركية من هونولولو إلى هونغ كونغ، حيث مكث لعدة أيام قبل السفر جوًا إلى روسيا. وبعد وصوله إلى هونغ كونغ، بدأ سنودن في نشر وثائق ادعى أنها تكشف تفاصيل مهمة عن إمكانيات وكالة الأمن القومي في الفضاء الإلكتروني وأنشطتها السابقة. وأكدت هذه الوثائق تصورات المحللين الصينيين بأن الولايات المتحدة تمتلك إمكانيات تجسس إلكتروني متطورة وأنها كانت تستخدمها بتوسع لاختراق نظم العلومات للدول الخارجية بما فيها عدة أهداف في الصين.[39]

كانت هذه الكشوفات فرصة لابتهاج المسؤولين الحكوميين الصينيين.[40] ووصفت إحدى التعليقات في وكالة أنباء شينخوا الأحداث بأن "الولايات المتحدة التي كانت تلعب دور الضحية البريئة للهجمات الإلكترونية لفترة طويلة، تبين أنها الشرير الأكبر في عصرنا."[41] أعاقت ادعاءات سنودن جهود الولايات المتحدة لحشد الضغط ضد الصين والدول الأخرى لتحدد معالم الاختلاف بين التجسس التقليدي ضد أهداف تخص الأمن القومي والتجسس الإلكتروني ذي الدوافع الاقتصادية ضد المصالح التجارية للقطاع الخاص.

---

37 ناكاشيما 2014

38 مقال لمارك لاندر (Mark Landler) وديفيد إي سانغر (David E. Sanger) بعنوان "الولايات المتحدة تطالب الصين بقطع الهجمات الإلكترونية وقبول القوانين،" صحيفة نيويورك تايمز *New York Times* 12 مارس/آذار 2013.

39 مقال لتي بينغ شين (Te-Ping Chen) بعنوان "سنودن يدعي باختراق الولايات المتحدة للصين،" ذا وال ستريت جورنال *Wall Street Journal* 23 يونيو/حزيران 2013.

40 مقال بعنوان "راقب من يتصنت عليك،" ذا إيكونوميست *Economist*، 15 يونيو/حزيران 2013.

41 شين 2013. انظر أيضًا مقال لانا لام (Lana Lam) "سنودن يصرح: استهدفت وكالة الأمن القومي جامعة تسينغ-هوا بالصين بهجمات اختراقية مكثفة،" *South China Morning Post* بتاريخ 22 يونيو/حزيران 2013.

ومع التقدم الطفيف في قضية الفضاء الإلكتروني الناتج عن جهود المفاوضات المباشرة، تغير اتجاه سياسة الولايات المتحدة تجاه اختراقات الصين الإلكترونية. في مايو/آيار 2014، أدانت وزارة العدل الأمريكية خمسة ضباط بجيش التحرير الشعبي الصيني لاختراقهم شركات القطاع الخاص بالإضافة إلى شركة يونايتد ستيلورکرز (United Steelworkers).[42] ووفق البيانات الصحفية الصادرة بشأن الإدانات،[43] تعرضت ست مؤسسات للاختراق، ووقعت البيانات التالية في قبضة المخترقين:

- من شركة وستنغهاوس Westinghouse: مواصفات فنية ومواصفات تصميم تخص خطوط الأنابيب ورسائل بالبريد الإلكتروني تتعلق بإنشاء مرفق في الصين لشركة تملكها الدولة.
- من شركة سولار ورلد Solar World: معلومات تخص تدفق النقد، وأساليب التصنيع، ومعلومات عن خطوط الإنتاج، والتكاليف، والمراسلات القائمة على مبدأ سرية المعلومات بين المحامي وموكله والمتعلقة بالتقاضي التجاري المستمر.
- من شركة يو إس ستيل U.S. Steel: معلومات على الخوادم، ربما ترتبط بقضية تجارية ضد شركات الصلب الصينية.
- من شركة إيه تي آي ATI: معلومات تخص بيانات اعتماد الشبكة، وربما ترتبط شركة مشتركة ونزاع تجاري مع شركة صينية مملوكة للدولة.
- من شركة آلكوا Alcoa: رسائل بريد إلكتروني، بما في ذلك مباحثات داخلية بخصوص شراكة ما مع شركة صينية مملوكة للدولة
- من شركة يونايتد ستيلورکرز United Steelworkers: رسائل بريد إلكتروني خاصة باستراتيجيات متعلقة بالنزاعات التجارية المعلقة.

---

[42] دون اتهامات تتعلق بجرائم الحرب، من النادر جدًا إدانة دولة للضباط العسكريين في دولة أخرى بسبب جرائم ارتكبت في البلد الأم للمتهمين. و لا يميز القانون الأمريكي الذي بموجبه تمت إدانة هؤلاء الضباط، وهو قانون إساءة استخدام الحواسيب والتحايل بها لعام 1986، بين الاختراق غير المصرح به للأنظمة التجارية و الاختراق غير المصرح به لأنظمة الأمن القومي. وهكذا، لن يختلف السند القانوني الأمريكي كثيرًا في إدانة ضباط آخرين في جيش التحرير الصيني، على سبيل المثال، لاقتحامهم أجهزة الكمبيوتر بوزارة الدفاع.

[43] إدارة الشؤون العامة بوزارة العدل الأمريكية: "إدانة الولايات المتحدة لخمسة مخترقين عسكريين صينيين بسبب التجسس الإلكتروني ضد الشركات الأمريكية وشركة تابعة لوزارة العمل من أجل الحصول على مكاسب تجارية،" واشنطن 19 مايو/آيار 2014.

لاحظ أن جميع المؤسسات المخترقة كانت تتعامل مع الجانب الصيني سواء بصفتها شريكًا تجاريًا أو طرفًا في النزاع التجاري. باستثناء الإشارة إلى "أساليب التصنيع" بشركة سولار ورلد Solar World،[44] لم ترد دلائل كبيرة على سرقة الملكية الفكرية.[45]

أبدت الصين استياءها فورًا من الإدانات وانسحبت من مباحثات مجموعة العمل الرسمية التي بدأت في العام الأسبق. وزاد من غضبها صدور الأمر التنفيذي بتاريخ 1 أبريل/نيسان 2015 الذي نص على: "تجميد ممتلكات بعض الأشخاص المتورطين في أنشطة هامة غير مشروعة باستخدام الفضاء الإلكتروني."[46]

المباحثات غير الرسمية بين معاهد الصين للعلاقات الدولية المعاصرة ومركز الدراسات الاستراتيجية والدولية

في عام 2009، اقترحت الصين الشروع في مفاوضات غير رسمية بشأن الفضاء الإلكتروني مع مجموعة من المتخصصين الأمريكيين البارزين، سعيًا لمواجهة تزايد شكاوى الولايات المتحدة بشأن التجسس الإلكتروني.[47] اشتمل الجانب الصيني على مسؤولين من معاهد الصين للعلاقات الدولية المعاصرة، وشملت الوفود عددًا متزايدًا

---

[44] قد تشير المعلومات عن خطوط الأنابيب المتعلقة بخطوط أنابيب شركة وستنغهاوس إلى وجود ملكية فكرية، لكن ربما استولت عليها الصين سعيًا منها لفهم أساس التكلفة لعطاءات وستنغهاوس وبالتالي لتجد سعرًا أفضل لعرضه مقابل خدمات وستنغهاوس.

[45] ربما يعتقد مسؤولو الحكومة الأمريكية أن الكشف عن سرقة الملكية الفكرية سيكون أكثر ضررًا من الكشف عن سرقة معلومات تخص الملكية التجارية (ولكن لا يتضح كيف سيتعامل هذا الخيار مع عملية الاكتشاف إذا وصلت الإدانات إلى حد المحاكمة). كان هناك اقتراحات بمعاملة التجسس الإلكتروني ذي الدوافع الاقتصادية على أنه قضية تجارية. وقعت الصين على اتفاقية الجوانب التجارية لحقوق الملكية الفكرية التابعة لمنظمة التجارة العالمية. تحظّر الاتفاقية على الدول سرقة الملكية الفكرية لكنها لم توضح الكثير بشأن الاستفادة من سرقة بيانات الملكية التجارية. وإذا كان الجانب الصيني مهتمًا أكثر بالملكية التجارية حقًا، فسوف يصعب تحديد ما إذا كانت تصرفاته قد انتهكت اتفاقية الجوانب التجارية لحقوق الملكية الفكرية.

[46] انظر إلى خطاب باراك أوباما "الأمر التنفيذي - تجميد مملتكات بعض الأشخاص المتورطين في أنشطة هامة غير مشروعة باستخدام الفضاء الإلكتروني" واشنطن العاصمة: البيت الأبيض، 1 أبريل/نيسان 2015. يبدو أن الصين تعاملت مع الأمر التنفيذي كما لو كان صادرًا ضدها تحديدًا، رغم أنه عبر كذلك عن عقوبات الولايات المتحدة على بعض الكوريين الشماليين بعد اختراق شركة سوني.

[47] عقدت الولايات المتحدة مفاوضات أكثر رسمية مع الروس، وكان أحد نتائجها هو الاتفاق على "خط ساخن" فيما يتعلق بالفضاء الإلكتروني، كي يسعهما مناقشة الأحداث التي تتعلق بالدولتين قبل أن تتحول إلى أزمات معقدة.

من المسؤولين الحكوميين على مر الوقت. وترأس الجانب الأمريكي مركز الدراسات الاستراتيجية والدولية، لكنه جمع مشاركين من مختلف أنحاء واشنطن العاصمة، ومن داخل مراكز الأبحاث، بالإضافة إلى مجموعة كبيرة مشاركة من المسؤولين الحكوميين، بمرور الوقت، إلى الحد الذي ينبغي النظر فيه إلى المباحثات على أنها شبه رسمية (Track 1.5) أو أنها خليط من الاجتماعات الرسمية وغير الرسمية. وحتى كتابة هذا التقرير، انعقدت تسع جلسات من الحوار، بدأت في ديسمبر/كانون أول 2009 في واشنطن العاصمة وتناوبت بين الربيع والصيف في بكين وأوائل الشتاء في واشنطن. وتلى الاجتماع الثامن (مايو/آيار 2013) فترة توقف بسبب بداية ونهاية المباحثات الرسمية بين البلدين. وعقد اجتماع تاسع في واشنطن في فبراير/شباط 2015.

وكان أبرز ما يميز الجلسات التسع في مجملها هو الاستمرارية لا التغيير الذي أدت إليه –لأن المواقف التي جاء بها المحاورون الأمريكيون والصينيون منذ ست سنوات هي نفسها التي يؤيدونها اليوم، في الجزء الأكبر منها. ومن ضمن التغييرات التي تمت ملاحظتها بالنسبة للطرف الصيني هي تقلص مخاوفهم بشأن عدم إمكانيتهم مواكبة التحديات التي فرضتها الإنترنت على المجتمع الصيني. وفي المقابل، نادرًا ما تربط الصين بين شكواها من دعم الولايات المتحدة المزعوم للمواد المتعلقة بالمعارضة على الإنترنت وشكاوى الولايات المتحدة بشأن الأنشطة الصينية غير المرغوب فيها في الفضاء الإلكتروني. واستمرت تأكيدات الصين على السيادة في عالم المعلومات أثناء المفاوضات. ومن ضمن الأفكار البارزة الأخرى كان إدراك الصين لسيطرة الولايات المتحدة على الفضاء الإلكتروني واستمرارها في السيطرة عليه، وبالتالي ينبغي ألا تقلق الولايات المتحدة بشأن هذا المجال بقدر قلق الآخرين. وترى الصين أن شكوى الولايات المتحدة من الهجمات الإلكترونية لا مبرر لها، بسبب الوضع الذي تتمتع به. واستدل الممثلون الصينيون على اعتماد بلدهم على الإمكانيات الأمريكية بمواقف عديدة: تستضيف الولايات المتحدة أنظمة بطاقات الائتمان وحجوزات الطيران الخاصة بهم؛ اعتمدت اتصالاتهم الطارئة على شركة أمريكية؛ اعتمدت مكاتبهم على شركة مايكروسوفت التي لم تُنسَ إجراءاتها عام 2008 (عندما أدى تحديث في النظام

ويرجع التقدم السريع مع روسيا (على الأقل حتى عام 2014) إلى الاستفادة من المفاوضات الثنائية الرسمية على مدى 50 عامًا، ما أنتج وعيًا واضحًا عن الطريقة التي يتعامل بها الطرفان. لم يُصنع بعد هذا التاريخ مع الصين.

إلى تعتيم العديد من الشاشات في الصين[48]) وعام 2012 (عندما أقنعت محكمة أمريكية بإغلاق الموقع الإلكتروني الصيني 3322.org). وأعرب المشاركون الصينيون عن قناعاتهم بأن الشركات، مثل مايكروسوفت، كانت تعمل على تجميع كميات كبيرة من البيانات الشخصية الخاصة بمستخدمي الإنترنت في الصين وأن هذه المعلومات يمكن للحكومة الأمريكية الحصول عليها بمذكرة قضائية أو بوسيلة أخرى.

وكان المشاركون الصينيون في هذه المناقشات على درجة كبيرة من الوعي بالصعوبات التي تواجهها الصين في الحفاظ على الإنترنت قيد التشغيل في مواجهة مواطن الخلل، (حتى أن أحد المشاركين ذكر انقطاع خدمات نظام اسم النطاق في 17 محافظة في مرحلة أو أخرى) و"حقيقة" أن الولايات المتحدة تتحكم في جميع نطاقات المستوى الأعلى (.gov ، .org، .com، و .edu وغيرها).[49] لم تجد الصين مبررًا لقلق الولايات المتحدة بشأن تأمين سلاسل التوريد، إلا كدليل على الكيفية التي يمكن أن تتبعها لإدارة المخاطر.

أبدى المشاركون الصينيون قلقهم كذلك من الدودة الخبيثة ستوكسنت Stuxnet (على الأقل في أعقاب حادثتها مباشرة) ومن تأسيس القيادة الإلكترونية الأمريكية (USCYBERCOM)، التي رأوا أنها دليل على رغبة الولايات المتحدة في عسكرة الفضاء الإلكتروني، بينما تمت الإشارة إلى غياب نظير صيني معلن عنه على أنه دليل على نوايا الصين السلمية. وامتدت هذه الشكوك إلى تصورهم (الذي تخلوا عنه حاليًا) بأن مناورات عاصفة الحواسب (Cyber Storm) التابعة لوزارة الأمن الداخلي كانت تحضيرات للاستعداد جيدًا في مواجهة الحرب الإلكترونية التي ترعاها الولايات المتحدة.[50] وعم شك مماثل نحو ادعاء الولايات المتحدة لحقها في الرد على الهجوم الإلكتروني، ويرجع سبب ذلك إلى أن الصين لا تثق في ادعاءات الولايات المتحدة بالإسناد، لأن الصينيين أنفسهم لا يمكنهم إتقان الإسناد، رغم أنهم يرغبون في تحسين قدراتهم في ذلك المجال كما هو واضح.

---

[48] مقال لتوماس كلابيرن بعنوان "غضب القراصنة الصينيين بسبب الفشل الذريع لشركة مايكروسوفت" من موقع إنفورميشن ويك *Information Week*، 23 أكتوبر/تشرين الأول 2008.

[49] تخلط الصين بين مقر هذه النطاقات في الولايات المتحدة والنطاقات التي تتحكم فيها الحكومة الأمريكية.

[50] إدارة الأمن القومي الأمريكية تقرير بعنوان "عاصفة إلكترونية: تأمين الفضاء الإلكتروني،" صفحة ويب 1 ديسمبر/ كانون الأول 2015.

نزعت الصين إلى النظر إلى مشكلة الحرب الإلكترونية من منظور التحكم في السلاح، وطرحت أسئلة مثل، "ما هو السلاح الإلكتروني؟" و"هل ينبغي حظر الأسلحة التي لا يمكنها التمييز بين الأهداف العسكرية والمدنية؟" و"هل يمكن خلق فضاء إلكتروني يعادل المواد الدالة (وهي مواد إرشادية تزرع في المواد الكيميائية المتفجرة لتعريفها من حيث المصدر أو الأصل)؟"

وأخيرًا، رغم تفهم الصين لمخاوف الولايات المتحدة بشأن تجسس الصين الإلكتروني ذي الدوافع الاقتصادية، إلا إنها رفضت أن تناقش مدى شرعية التجسس الإلكتروني ذي الدوافع الاقتصادية من عدمه في عالم يعتبر فيه التجسس الإلكتروني المتعلق بالأمن القومي أمرًا تجريه الدول الآن بشكل روتيني. وناقش العديد من المشاركين في الحوار ضرورة وجود الثقة المتبادلة، وقالوا إنه يتعين على الولايات المتحدة أن تظهر أنها تعتبر الصين محل ثقة وتتصرف بموجب ذلك، وأكدوا على ضرورة عدم اتهام الصين بالجرائم الإلكترونية.[51]

[51] إن مصطلح تبادل الثقة الذي يكرره دائمًا المحللون الصينيون على مدى سياقات متنوعة، غالبًا ما يتسبب في إرباك المحللين الأمريكيين. وفق آراء كيان ينجي (Qian Yingyi) وجيا كينغو (Jia Qingguo) وباي تشونغن (Bai Chong'en) ووانغ جيسي (Wang Jisi)، يعني مصطلح تبادل الثقة الاستراتيجية في العلاقات بين الولايات المتحدة والصين إدراك الطرفين الأغراض الاستراتيجية للطرف الآخر مع التحلي بالتوقعات الطيبة تجاه مواقف وتصرفات الطرف الآخر بخصوص قضايا المصالح الحيوية. لا يعني بناء الثقة الاستراتيجية المتبادلة نفي كل من الصين والولايات المتحدة وجود تعارض مصالح وخلافات أيديولوجية بينهما. على العكس، فهو يعني أن كلًا من الطرفين سيسعى جاهدًا إلى تقليل أثر النزاعات والاختلافات على العلاقات الثنائية وتكوين تفاعلات سليمة على المدى الطويل بناءً على اتفاقهما على على أن المصالح المشتركة بينهما أكبر من الخلافات. انظر دراسة أجراها كيان ينجي Qian Yingyi وجيا كينغو Jia Qingguo وباي تشونغن Bai Chong'en ووانغ جيسي Wang Jisi، بعنوان "بناء الثقة المتبادلة بين الصين والولايات المتحدة،" الواردة في دورية حررها شاو بين هونغ (Shao Binhong) بعنوان العالم في 2020 وفق منظور الصين: مباحثات النخبة السياسة الخارجية الصينية بشأن التوجهات في السياسات الخارجية لايدن، هولندا: Koninklijke Brill NV 2014، ص 291-277.

ما الذي يمكن أن تقدمه الولايات المتحدة لتثني الصين عن التجسس الإلكتروني ذي الدوافع الاقتصادية؟

كان رد الصين العلني على الاتهامات المختلفة بممارستها التجسس الإلكتروني هو النفي التام.[52] تعكس ملاحظات نائب الوزير ونائب مدير مكتب الدولة لمعلومات الإنترنت كيان شياوكيان (Qian Xiaoqian) على نحو كبير موقف الصين عند اتهامها بالتجسس الإلكتروني:

> معارضتنا لجميع أشكال الاختراق واضحة وثابتة... وفي الآونة الأخيرة، بدأ الناس في ترويج نظرية عن تهديد الإنترنت الصيني، التي تعد مجرد امتداد لنظرية "التهديد الصيني" القديمة ولا أساس لكلتيهما من الصحة.[53]

إضافة إلى ذلك، يعرب العديد من الصينيين عن إيمانهم بأن الولايات المتحدة تمارس التجسس الإلكتروني ذي الدوافع الاقتصادية، حتى إن لم يكن لديهم أي دليل محدد يرتكزون عليه، وأن المسؤولين الصينيين والصين نفسها ضحايا للجرائم الإلكترونية النابعة من الولايات المتحدة. ومؤخرًا، وصفت الصين الاتهامات الموجهة إليها باختراق مكتب إدارة شؤون الموظفين بأنها

> اتهامات باطلة [من شأنها] بالتأكيد الإضرار بالثقة المتبادلة بين القوتين الكبيرتين في العالم اليوم [والتي وجهت]...دون أي دليل [لأنه] لا يمكن تقفي أثر الهجمات الإلكترونية، إذ تشن عادةً عبر الحدود دون تحديد هوية الفاعل.[54]

بغياب أي تغيير في آراء الصين حول مصداقية ادعاءات الإسناد، يستحيل على الأرجح إجبار الصين على الاعتراف بتورطها في أي حادثة تجسس إلكتروني، بغض النظر عن

---

[52] "لا تعترف بشيء وانكر كل شيء،" كما نشرته مجلة ذا إيكونوميست *The Economist*، بتاريخ 8 يونيو/حزيران 2013.

[53] انظر مقال كريستوفر بودن بعنوان "الولايات المتحدة تدعي أن القرصنة تقوض مصالح الصين،" شبكة بايونير بريس *Pioneer Press*، 9 أبريل/نيسان 2013. انظر أيضًا مقال "مسؤول كبير يحث على الثقة المتبادلة بين الصين والولايات المتحدة بشأن الأمن الإلكتروني،" المنشور بشينخوا Xinhua، 10 أبريل/نيسان 2013.

[54] على سبيل المثال، مقال جو جانكينغ (Zhu Junqing) بعنوان " تعليق: خطأ الولايات المتحدة في حق الصين بشأن الخروقات الإلكترونية تضر بالثقة المتبادلة،" المنشور بوكالة شينخوا الإخبارية Xinhua، 6 يونيو/حزيران 2015.

تكرار مطالب المسؤولين الأمريكيين بالاعتراف أو الاعتذار أو أي تغيير في سلوك نظرائهم الصينيين.

بافتراض أن الولايات المتحدة كانت على استعداد للقيام بما هو أكثر من مجرد الحوار (أو إدانة الأفراد الذين يستحيل تقديم أنفسهم أمام المحكمة). ما الذي ستطلبه الولايات المتحدة من الصين لتقوم به؟ ما نسبة نجاح الولايات المتحدة؟ ما هي المخاطر المتخذة أثناء المحاولة (أو عند النجاح)؟

إذا تمكنت الولايات المتحدة من إرساء القواعد التي تميز التجسس الإلكتروني ذي الدوافع الاقتصادية من نظيره ذي الأهداف الخاصة بالأمن القومي، سيتعين عليها أن تقر بأن الكثير مما يثير مخاوف الولايات المتحدة بشأن التجسس الإلكتروني الخاص بالصين (مثل اختراقها لمكتب إدارة شؤون الموظفين) لا يقل شرعية عن التجسس الإلكتروني الأمريكي باعتبار أنه يستهدف أهدافًا تقليدية لدى الدولة. وعلى نحو مماثل، فإن اقتحام الصين المزعوم لعمليات إنتاج مقاتلات لوكهيد مارتن إف-35[55] وهجومها على شركة RSA (بهدف اختراق أهداف على شاكلة لوكهيد مارتن)، واختراقاتها السابقة لوكالات حكومية أمريكية، قد تدخل جميعها ضمن التعريف واسع النطاق لأنواع التجسس التي يتم تنفيذها باسم الأمن القومي والتي تراها الولايات المتحدة شرعية (وإن كانت غير مرغوبة، بالتأكيد، عندما تجد نفسها هي الهدف مع قطاعها الدفاعي – الصناعي).

وأحد التحديات هو أن ما يشكل الأمن القومي للصين قد لا تراه الولايات المتحدة كذلك بالضرورة. يبدو أن الصين مارست التجسس الإلكتروني ضد جريدة نيويورك تايمز *New York Times* لقيام أحد الصحفيين بها بكتابة مقال عن عائلة رئيس الوزراء السابق وين جياباو (Wen Jiabao) وجمعها لثروة هائلة غير معلومة المصدر.[56] بالنسبة لدولة تخشى الغضب الشعبي بسبب فساد المسؤولين، قد تشكل هذه الاتهامات تهديدًا للأمن القومي، لكن بالنسبة للولايات المتحدة وحسب التعديل الأول من الدستور لا يعد هذا الأمر قضية أمن قومي.[57]

---

[55] غورمان وكول ودريزن (Gorman, Cole, and Dreazen)، 2009

[56] مقال لنيكول بيرلروث بعنوان "المقرصنون بالصين هاجموا صحيفة التايمز لمدة الأربعة شهور الماضية،" نيويورك تايمز *New York Times* 31 يناير/كانون الثاني 2013.

[57] تتعامل الصين مع أي أمر ينعكس سلبًا على سمعة الحزب الحاكم على أنه تهديد لاستقرار النظام، وبالتالي تعتبره قضية أمن قومي. لا تعتبر الولايات المتحدة هذا النهج للخطاب السياسي مشروعًا أو يتوافق مع قواعد حقوق الإنسان.

من العقبات الأخرى أمام من تجسس الصين الإلكتروني ذي الدوافع الاقتصادية ترى الصين أن حجم ونطاق المكاسب المحتملة قد يفوقان العقوبات التي ربما تسعى الولايات المتحدة لفرضها على الصين لاستمرارها في ممارسة التجسس الإلكتروني ذي الدوافع الاقتصادية. قد يكون هناك مستقبل تستنتج فيه الولايات المتحدة والصين أن كلًا منهما سيكون أفضل حالاً إذا لم يشرع أي منهما في التجسس الإلكتروني ذي الدوافع الاقتصادية. إذ لن تضطر أي دولة حينها إلى الإنفاق الكبير على الدفاع الإلكتروني، وستكون عوائد الجهود المبذولة لإنتاج الملكيات الفكرية أكبر، لأن الطرفين سيحصلان على ملكيات خاصة لما قاما بإنتاجه (وفي بعض الأحيان، ابتكاره). وعلينا تصور صفقة تحسن من حال كل من الولايات المتحدة والصين. وإن كان الأمر كذلك، فلا يكون هناك تسويات (أو وفقًا لخبراء الاقتصاد مجموعة من التكاليف الجانبية) التي تحسن من حال الطرفين. ويعني ذلك أن إصدار القرار يتطلب مواجهة، تحاول من خلالها الولايات المتحدة إقناع الصين بنبذ التجسس الإلكتروني ذي الدوافع الاقتصادية وإلا تواجه العواقب. ومن ثم، فالاستراتيجية الحالية هي (حتى كتابة هذا التقرير) الإلحاح الدبلوماسي مع عواقب بسيطة.

ما تتضمنه هذه المواجهات هو أن استمرار التجسس الإلكتروني ذي الدوافع الاقتصادية يهدد الصداقة مع الولايات المتحدة، وهو أمر تفترض حكومة الولايات المتحدة أن قيمته للصين أكبر من قيمة المكاسب الصينية من التجسس الإلكتروني ذي الدوافع الاقتصادية. ومن المفترض أن تكلفة قطع الولايات المتحدة لأواصر صداقتها مع الصين هو أن الصين ترد بالمثل. وفي نهاية المطاف، السؤال المهم هو: أي دولة تحتاج الأخرى أكثر؟ لاحظ أحد المندوبين الصينيين، في جلسة المباحثات التاسعة بين مركز الدراسات الاستراتيجية والدولية ومعاهد الصين للعلاقات الدولية المعاصرة، إلى أن الولايات المتحدة بفضل قوتها ومركزها هي الدولة الوحيدة التي لا يمكن فرض العقوبات عليها (عمليًا). وسيكشف المستقبل النقاب عن الوقت الذي سيبقى فيه هذا الوضع على ما هو عليه في وجه التوجهات الاقتصادية وغيرها.

هل يمكن التوصل إلى اتفاق؟

أجرينا سلسلة من الاجتماعات في بكين مع مسؤولين في الوكالات الحكومية المختصين في إدارة قضية الفضاء الإلكتروني، وضباط في الخدمة وضباط متقاعدين بجيش التحرير الشعبي الذين ينصب عملهم على الأمن الإلكتروني، والخبراء من مراكز الأبحاث الحكومية، والخبراء الأكاديميين، من أجل دراسة الخيارات أمام تطوير التعاون وتقليص الشك مع الصين بشأن قضايا الأمن الإلكتروني. كانت مقابلاتنا شبه منظمة، بمعنى أننا طرحنا عددًا قليلًا من الأسئلة الثابتة: ما المطلوب لاستئناف المفاوضات (المتوقفة في وقت إجرائنا للمناقشات)؟ ما الذي ستجنيه هذه المفاوضات؟ ما المطلوب للحفاظ على زخم هذه المباحثات؟ ما الذي تود الصين رؤيته من الولايات المتحدة في هذه المفاوضات؟ وكانت هذه الأسئلة بمثابة مقدمات لنقاش أوسع (وفي بعض الحالات القليلة، تحدث محاورونا أولاً). يستعرض هذا الفصل نتائج البحث التي توصلنا إليها ويستعرض ما كشفت عنه هذه المحادثات عن الطريقة التي التي يمكن للولايات المتحدة أن تتبعها لتحقيق تعاون أكبر مع الصين بشأن الفضاء الإلكتروني.

الخلفية

الخلاف بين الولايات المتحدة والصين بخصوص تصرفات كل منهما في الفضاء الإلكتروني هو خلاف غير متماثل من حيث الأولويات والمسائل التي تثير القلق. ترغب الولايات المتحدة أن تكف الصين عن اختراقاتها لشبكات الشركات التجارية، ويود الصينيون مجرد التخلص من هذه المشكلة. فيما يخص هذا الاختلاف في الأولويات، يذكر أحد المتحاورين الذين تحدثنا معهم، وهو خبير في العلاقات الأمريكية الصينية، أنه رغم اعتبار الفضاء

الإلكتروني من ضمن أهم خمس قضايا تشغل الولايات المتحدة، إلا إنه لم يدخل حتى ضمن أهم عشر قضايا بالنسبة للصين على الأرجح. وأشار متحاور آخر أنه لم يشهد قط أي قضية تقفز إلى قمة جدول أعمال المناقشات بشأن السياسات الثنائية الأمريكية الصينية مثل الفضاء الإلكتروني، وهو أمر يبدو أنه قد باغت القيادة الصينية، على حد قول مراقب ثالث. وعلق متحاور رابع بأنه رغم إدراك الطرفين هشاشة البنى التحتية الأساسية، تم التعبير عن هذه المخاوف على نحو أكثر تكرارًا وصخبًا في الولايات المتحدة.

يدرك المتحاورون الصينيون أن الفضاء الإلكتروني قضية تثير القلاقل في العلاقات بين الدولتين وأنها تقلص الثقة الاستراتيجية (على حد تعبير الصينيين). وانخفاض الثقة الاستراتيجية قد يضع العراقيل بدوره أمام حل المشكلات الأخرى (مثل التجارة والبيئة والقضايا الجيو استراتيجية). وقد يزيد كذلك من احتمالات نشوب النزاع في المستقبل، سواء بشكل عرضي أو مقصود. حتى وإن ساد الظن بأن القليل من النزاعات التي تحدث في الفضاء الإلكتروني تُحدث اختلافًا كبيرًا مقارنة بالنزاعات التي تحدث في العالم الفعلي (مثل قضية بحر الصين الجنوبي)، فإن حل المشكلات في هذا المجال سيكون له تداعيات خارجه والعكس صحيح.

وكما ذكرنا، للولايات المتحدة ما لايقل عن ثلاث قضايا متعلقة بالفضاء الإلكتروني مع الصين: التجسس الإلكتروني ذو الدوافع الاقتصادية، التهديد المحتمل للبنية التحتية الحيوية للولايات المتحدة، والخطر المتبادل لسوء الفهم الاستراتيجي. ويبدو أن ذلك يستدعي ضرورة المفاوضات والضمانات المتبادلة والتفاهم المشترك، على التوالي.

ونبدأ بتقييم مناخ المفاوضات ثم نستعرض مجالات التفاوض المحتملة.

المفاوضات الرسمية

تماشيًا مع التصريحات السابقة الرسمية وغير الرسمية، أكد المتحاورون الصينيون تكرارًا وبقوة أحيانًا أنه لا يمكن استئناف المفاوضات الرسمية ما دام الضباط الخمسة في جيش التحرير الصيني قيد الاتهام. وقد بدا الغضب الشديد على كثير من المتحاورين بسبب إدانة الولايات المتحدة لهؤلاء الضباط العسكريين الصينيين بسبب القرصنة. وقال متحاور رفيع المستوى تحدثنا معه إنه إذا أرادت الولايات المتحدة تحقيق تقدم "عليها أن تركع على ركبتيها وتتوسل من أجل الصفح عنها مثلما فعل [رئيس وزراء ألمانيا الأسبق فيلي برانت (Willy Brandt)" وأكد أن هذا التصرف

"سوف يكسب ود الشعب الصيني."[1] وتحدث مطولًا متحاور آخر رفيع المستوى وأكد بأن هذه الإدانة تناقض القانون الدولي والممارسات الدولية، إذ إنه لا يمكن تفسير التجسس الإلكتروني بأي حال من الأحوال على أنه جريمة حرب. وأعرب المحاورون الصينيون تكرارًا عن اهتمامهم بمعرفة ما إذا كان سيتم إلغاء الإدانات أو التراجع عنها.[2]

من الصعب تخيل عودة الصين إلى المفاوضات الرسمية دون حل موضوع الإدانات، ويصعب أكثر تخيل تنازل الولايات المتحدة عن الاتهامات لمجرد أن الصين طلبت منها ذلك.[3] إلا أن بعض المتحاورين بمراكز الأبحاث التابعة للحكومة والجيش، بعد أن أعربوا عن آرائهم بخصوص طبيعة الإدانات غير المبررة، يرجحون وجود طريقة لاستئناف المفاوضات الرسمية حتى وإن رفضت الولايات المتحدة إسقاط الاتهامات. ومن ضمن الأفكار التي اقترحها أحد المحاورين أن يتم ببساطة وضع آلية حوار رسمية جديدة بشأن الفضاء الإلكتروني، بحيث يُطلق عليها اسم آخر بخلاف "مجموعة العمل المختصة بالفضاء الإلكتروني" ويتم إدراجها في منتدى آخر بخلاف حوار الأمن الاستراتيجي التابع للحوار الاستراتيجي والاقتصادي. ورأى أحد المشاركين أن نقل مكان النقاش من الحوار الاستراتيجي والاقتصادي بين الولايات المتحدة والصين إلى منتدى آخر يسمح باستئناف المباحثات دون الإخلال بإصرار الصين على وقف المباحثات حتى تحل قضية الإدانات. وبما أن آلية الحوار الجديدة هذه لا تتعلق بإدانة ضباط جيش التحرير الشعبي، يمكنها أن تبدأ دون الاضطرار إلى انتظار حل مسألة الإدانات.

غير أننا لمسنا شعورًا طاغيًا في الصين بأن المفاوضات الرسمية لا تقدم سوى الفرصة لكل طرف لعرض وجهة نظره للطرف الآخر. وقال اثنان من المتحاورين رفيعي المستوى أن أفضل نهج بموجب الظروف الحالية هو عقد مجموعة عمل دائمة أو مستمرة (في مقابل مجموعة العمل الثنائية). بحيث تخدم مجموعة العمل هذه أغراضًا متنوعة وهي: التفكير في المقترحات (بعضها يستلزم معلومات فنية كبيرة) قبل أي مفاوضات رسمية بين الطرفين، لتخرج بمجموعة مشتركة من معايير السلوك في الفضاء الإلكتروني لاستبدال دليل تالين Tallinn وبيان الصين وروسيا المشترك بشأن الفضاء الإلكتروني الذي أصدرته منظمة شنغهاي للتعاون، أو حتى للنظر في

---

[1] حوار أجري في بكين في 2015.

[2] حوار أجري في بكين في 2015.

[3] تفاعل عدد قليل من المشاركين في الحوار على نحو مماثل تجاه الأمر التنفيذي (أوباما 2015). بعبارة أخرى، كان ذلك موجهًا ضد الصين، وكان عدوانيًا بكل تأكيد وكان عقبة أمام استئناف المفاوضات.

ادعاءات الاختراقات الإلكترونية من جانب كل طرف والتوصل إلى تقييم مشترك لوقائع الحالة الموضوعية وتعيين الإسناد.[4]

يمكن اتخاذ المفاوضات غير الرسمية كوسيلة للخروج بأفكار، ولا سيما الأفكار التي تعتمد على ما إذا كانت بعض أنماط التكنولوجيا ستقدم ما تدعيه أو أن بعض أنواع السياسات ستحقق الأهداف المرجوة. قد يكون من الصعب جدًا التحقق من الامتثال، على سبيل المثال، في الفضاء الإلكتروني، وربما كان أصعب حتى مما هو عليه الحال في العالم الفعلي (مثل مراقبة البرنامج النووي للدولة الأخرى). ولا يمكن الخوض في كل هذه القضايا في المباحثات الرسمية الدورية وحدها. لكن فكرة أن المجموعات غير الرسمية ستطرح أمرًا تتفق عليه الحكومات بالتزكية هو أمر غير منطقي كذلك. ينبغي على جميع المفاوضات غير الرسمية بشأن الأمن في الفضاء الإلكتروني العودة إلى المفاوضات الرسمية إذا رغبت في تحقيق تأثير قوي ودائم.

ذكر الكثير من المشاركين في الحوار أهمية صياغة إما مذكرة تفاهم أو مجموعة تدابير لبناء الثقة، وأعربوا عن أملهم – الذي تحقق بعدها - بتوقيع هذه الاتفاقات أو الإعلان عنها في قمة سبتمبر/أيلول 2015. وبدا أن هناك تركيزًا أكبر على القيام بإجراء يبرز قدرة التوافق بين الصين والولايات المتحدة بدلًا من السعي إلى تحقيق أي أمر بعينه بحلول ذلك التاريخ.

التجسس الإلكتروني ذو الدوافع الاقتصادية

إن موقف الصين الرسمي لاتهامات الولايات المتحدة بممارسة الصين للتجسس الإلكتروني ذي الدوافع الاقتصادية هو النفي القطعي المقترن بالتأكيدات بأن الإسناد الدقيق والحاسم هو أمر مستحيل بالضرورة في الفضاء الإلكتروني.[5] وأقر العديد من المتحاورين أن عناوين بروتوكول الإنترنت (IP) التي يوجد مقرها بالصين والمرتبطة بالهجمات الواردة لا تشكل أي إثبات لهوية من يرتكبها وأن هذه الاتهامات تعكس

[4] غير أن إحدى الصعوبات قد تتمثل في أن وثيقة منظمة شانغهاي للتعاون تشير إلى السلوكيات وقت السلم، بينما يشير دليل تالين إلى السلوكيات وقت الحرب.

[5] وأعرب، رغم ذلك، بعض الخبراء المتخصصين الذين حاورناهم، عن رأيهم بأن الشكوك الصينية بشأن إمكانية الإسناد لا تتعدى كونها مواضيع للنقاش، وأكدوا على أن الجانب الصيني يدرك تمامًا ليس فقط إمكانية بل وأيضًا سهولة تحقيق الإسناد في كثير من الحالات، نظرًا للطبيعة غير المتقنة لعدد من الاختراقات الإلكترونية الصينية. حوارات مع خبراء أمريكيين بالأمن الإلكتروني، واشنطن العاصمة، يونيو/حزيران 2015.

الخطاب المعادي للصين. أكد الرئيس تشي بنفسه على ذلك في أوائل 2015، وفق رأي أكثر من مشارك.[6]

وبالتالي فوجئنا بأن محاورًا واحدًا فقط، وهو مشارك في الحوار رفيع المستوى، نفى نفيًا قاطعًا أن الصين تمارس التجسس الإلكتروني ذا الدوافع الاقتصادية؛[7] وبدا أن اثنين من المشتركين اعترفا ضمنًا بممارسة التجسس الإلكتروني ذي الدوافع الاقتصادية عندما ذكرا أن الادعاءات الأمريكية بأن سرقة بروتوكول الإنترنت تسببت في النمو الاقتصادي للصين هو أمر مبالغ فيه بشكل كبير. وتحدث آخرون بشكل عام عن صعوبة الإسناد، غير أن الكثير منهم وضعوا صعوبة ممارسة الصين للإسناد في الاعتبار (وأشار بعضهم صراحةً إلى سوء مستوى الإسناد الذي كانت تقوم به الصين)، بينما تحدث الآخرون عن الإسناد بشكل عام. وفي المقابل، عندما لفتنا نظرهم إلى أن الولايات المتحدة تعترض على التجسس الإلكتروني ذي الدوافع الاقتصادية النابع من الصين، لم يردوا على ذلك (باستثناء المحاور رفيع المستوى السابق ذكره). ولم يزعم أحد أن الولايات المتحدة نفسها كانت تمارس التجسس الإلكتروني ذا الدوافع الاقتصادية.

وثمة مسألة أخرى ذات صلة وهي ما إذا كان المشاركون معنا في الحوار من الصين قد رأوا أن التجسس الإلكتروني ذا الدوافع الاقتصادية أقل شرعية من التجسس الإلكتروني الذي يُمارَس لأغراض تقليدية تخص الأمن القومي. وفي المقابلات، شرحنا وجهة النظر الأمريكية: وهي أن الولايات المتحدة تعتبر التجسس الإلكتروني ذا الدوافع الاقتصادية بغيضًا على وجه الخصوص وتريد للصين أن تتوقف عنه. عزف أغلب المشاركين في الحوار عن الاعتراض على هذه العبارة، بل أنه بدا على اثنين منهم أنهم يتفقون معها. غير أن أحد المحاورين رفيعي المستوى اعترض تمامًا وقال إن التجسس الإلكتروني لأغراض الأمن القومي كان مقبولًا بمستوى أدنى من التجسس الإلكتروني ذي الدوافع الاقتصادية.

ولكي نكون منصفين، فإن فكرة أن التجسس الإلكتروني ذي الدوافع الاقتصادية أقل شرعية من التجسس الإلكتروني لأغراض الأمن القومي غير مستمدة من القانون الدولي ولا تشكل مقترحًا يقبله الجميع. وفي حين لا تمارس الولايات المتحدة التجسس الإلكتروني ذا الدوافع الاقتصادية، لا تبدو الصين الدولة الوحيدة التي تعتبره

---

[6] حوار أجري في بكين، مايو/آيار 2015.

[7] للأسف، كان هذا المشارك أكثر ميلًا للاتفاق مع الموقف الأمريكي في أن التجسس الإلكتروني ذا الدوافع الاقتصادية أقل شرعية من التجسس الإلكتروني لأغراض الأمن القومي.

نوعًا مشروعًا من التجسس.[8] ولكن لا توجد دولة أخرى تعتبر محط شكاوى التجسس الإلكتروني ذي الدوافع الاقتصادية بقدر الصين. وكذلك لم تشكُ الولايات المتحدة تحديدًا من التجسس الإلكتروني ذي الدوافع الاقتصادية الذي مارسته الدول الأخرى إلى الحد الذي ذكرت فيه الصين بالاسم بخصوص هذا السلوك. لعل الصين تعتبر التجسس الإلكتروني ذا الدوافع الاقتصادية نوعًا جذابًا ومشروعًا من التجسس نظرًا للتشابك الوثيق بين إدارة الدولة الصينية للسياسة والاقتصاد. ويتوافق النظام السياسي والاقتصادي الأمريكي أكثر مع تصنيف التجسس إلى النوع الموجه ضد الأهداف العامة (المشروع) والنوع الموجه ضد الأهداف الخاصة (غير مشروع)، أكثر من توافق نظام الصين مع هذا التصنيف.

ماذا تريد الصين؟

نطرح الآن هذا السؤال: ماذا تريد الصين من الولايات المتحدة في مقابل موافقتها على وضع قواعد معينة فيما يتعلق بالفضاء الإلكتروني، وبالأخص، قاعدة مجدية وقابلة للتنفيذ ضد التجسس الإلكتروني ذي الدوافع الاقتصادية؟

ما أثار اهتمامنا هو العناء الذي وجده جميع المحاورين المشاركين معنا تقريبًا للتعبير عن أي شيء محدد أو جوهري رأوا أن الصين تريده كتنازل من الولايات المتحدة في المفاوضات بشأن الأمن الإلكتروني. كما أننا لم نحصل على انطباع بأن عدم قدرتهم على تحديد مجموعة من المطالب كان بسبب امتلاكهم قائمة ما زالوا يعملون على ترتيب أولوياتها، أو حتى مجموعة من الطلبات ما زالوا يعملون على تحديد قيمتها. بل بدا أنه لم تكن لديهم أي مطالب ببساطة.

جاوب المشاركون بإجابات عامة عن هذا السؤال. واشتكى البعض من عدم وجود ثقة متبادلة بين الصين والولايات المتحدة، إذ لمحوا بوضوح (وأكد بعضهم) على أن الأمور ستكون أفضل حالًا إذا وثقت الولايات المتحدة بالصين أكثر. وأشار العديد من المشاركين في الحوار إلى رغبتهم في أن تكف الولايات المتحدة عن انتقاد الصين لشنها أعمال التجسس الإلكتروني ذي الدوافع الاقتصادية – وهو أمر

[8] كان موقف الولايات المتحدة قبل ما كشف عنه إدوارد سنودن هو أن جميع أنواع التجسس الإلكتروني تتم سعيًا لهدف الأمن القومي. وبعد واقعة سنودن، تم الادعاء بأن الولايات المتحدة لا تقوم بممارسة التجسس الإلكتروني ذي الدوافع الاقتصادية وتسليم النتائج للشركات الأمريكية لتعزيز قدرتها التنافسية. ويعد هذا الادعاء معقولًا بقدر عدم توافق توفير هذه النتائج بشكل تفضيلي إلى شركة دون الأخرى مع الطريقة التي تتعامل بها الولايات المتحدة مع شركات خاصة محددة.

سيقبل به المسؤولون الأمريكيون، دون شك، مقابل عدم وجود أي تجسس إلكتروني ذي دوافع اقتصادية لتنتقده.[9] وأراد آخرون أن تتخلى الولايات المتحدة عن انتقاد الصين بشأن سياساتها تجاه حقوق الإنسان، أو بالتحديد، كبح المواقع الإلكترونية التي تبث رسائل تتعارض مع المصالح أو الوضع الحاكم للحزب الشيوعي الصيني. لا يتفق أي من الاقتراحين مع التعديل الأول للدستور. ورأى المحاورون كذلك قيمة كبيرة في الحصول على الصورة الشاملة بطريقة صحيحة، بافتراض أن التفاصيل ستتبعها: رأى أحد المشاركين مثلًا أنه إذا اتفق الطرفان على الوثوق أكثر في بعضهما البعض، سيتبع ذلك تلقائيًا التقاء فكري بشأن اختراق كوريا الشمالية. وأضاف أن ضبط النفس المتبادل يتعلق بالسيطرة على النوايا بالتناوب، ثم النشاط، وأخيرًا الأسلحة (ولربما يعكس المسؤولون الحكوميون ذلك الترتيب).[10]

عندما جاء ذكر المطالب المحددة، غلبها التخمين أو كانت بلا أهمية كبيرة للصين. وتضمنت الطلبات، على سبيل المثال، "الكف عن تمويل تكنولوجيا التحايل على الرقابة على الإنترنت،" وتخصص له الولايات المتحدة بضعة ملايين من الدولارات كل عام.[11] ومن ضمن الطلبات الأخرى "التوقف عن عرقلة وصول شركة هواوي وشركة زد.تي.إي. للسوق الأمريكية"، ويبدو أن هذا الطلب لا يعكس فهمًا واقعيًا لما قد تكون الولايات المتحدة مستعدة لتقديمه.[12] وأشار البعض إلى عدم رغبة الصين في الإضرار بعملية نقل التكنولوجيا تحت مسمى احتمالات الشك والإنكار وأعربوا عن أملهم بأن ترفع الولايات المتحدة الحظر عن نقل التكنولوجيا المتطورة إلى الصين.[13]

---

[9] سيكون على المسؤولين الأمريكيين التوقف عن تسريب المعلومات إلى الصحافة بأن الصين ارتكبت فعلًا ما في الحالات التي تؤكد فيها الهيئات المحايدة أن الصين لم ترتكب هذا الفعل (وربما حتى في الحالات التي لا تستطيع فيها التوصل إلى نتيجة). لكن هذا الأمر ليس تمامًا بالوضوح الذي يبدو عليه. في حالة إبرام اتفاق جاد، قد يضطر المسؤولون الأمريكيون إلى تعديل سلوكهم العام إذا لم يكن الإسناد مؤكدًا.

[10] حوار أجري في بكين، مايو/آيار 2015.

[11] Nicole Gaouette, and Brendan Greeley, “U.S. Funds Help Democracy Activists Evade Internet Crackdowns,” Bloomberg, April 20, 2011.

[12] حوار أجري في بكين، مايو/آيار 2015.

[13] تعرضت شركة آي بي إم IBM للانتقادات بسبب اقتراحها لنقل التنكنولوجيا إلى الصين. انظر ديفيد ولف (David Wolf) "لماذا نشتري الأجهزة إذا كانت الصين تحصل على بروتوكول الإنترنت مجانًا؟" مجلة فورين بوليسي *Foreign Policy*، 24 أبريل/نيسان 2015.

كانت الاقتراحات الأخرى التي عرضها المشاركون الآخرون أكثر منطقية، ولكن لا يتضح إن أمكن تحويل هذه المقترحات إلى أساس لاتفاق. وأعرب الكثير من المشاركين الآخرين عن استيائهم من القيادة الأمريكية في آيكان (هيئة الإنترنت للأسماء والأرقام المخصصة) وأشاروا إلى أن عشرة من خوادم الأسماء الكبرى لنطاقات مستوى القمة تقع في الولايات المتحدة (والثلاثة الآخرون في السويد واليابان وهولندا). ويرى بعض المشاركين بأنه ينبغي أن يكون لبقية العالم عمومًا، والصين تحديدًا، دور أكبر فيما يخص الإنترنت. وبالتأكيد، كانت قضية حوكمة الإنترنت قضية مثيرة للخلاف، لكنها نادرًا ما ترتبط مباشرة بمخاوف الأمن الإلكتروني. وكان الموقف الأمريكي الرسمي هو أنه تحت إشراف الولايات المتحدة، اتسع نطاق الإنترنت بسرعة كبيرة بحيث أصبح يلبي احتياجات جميع الدول. ليس النظام معطلًا، إذن لا سبب لإصلاحه في رأي الولايات المتحدة (ولم يذكر المشاركون أن أخطاء محددة تستلزم تمثيلًا أكبر لتصويبها، ولم يتمكنوا من تحديد الضرر الذي يجلبه النظام الحالي للمصالح الصينية سوى غياب الهيبة التي تقرنها الصين باستضافة هذه الخوادم).

إضافةً إلى ذلك، من شأن المرشح الواضح الآخر لحوكمة الإنترنت – وهو الاتحاد الدولي للاتصالات الخاضع للأمم المتحدة حاليًا – إدخال العديد من السمات التي قد تكون ضارة في حوكمة الإنترنت. بينما كان الإنترنت - ولا يزال إلى حد ما – صنيعة المهندسين الذين يهتمون بالابتكار وموجهًا إليهم، يمثل الاتحاد الدولي للاتصالات الحكومات وشركات الهواتف المملوكة للدول، ويخشى بعض هؤلاء يخشون. يمثل الإنترنت انتصارًا للمبادئ الهندسية من البداية إلى النهاية، ويضم نواة بسيطة نسبيًا بالإضافة إلى الأجهزة الطرفية الذكية. وعلى الجانب الآخر، يعد الاتحاد الدولي للاتصالات أكثر دراية بهياكل شركات الهواتف ذات النواة المعقدة والأجهزة الطرفية البسيطة. ويشتهر الإنترنت بأن مساره يتخطى الرقابة. وتمارس العديد من حكومات الدول الأعضاء بالأمم المتحدة الرقابة، ولا تريد حكومة الولايات المتحدة (ولا الشركات الأمريكية المصنعة للكنولوجيا الفائقة) أن تجد الإنترنت وقد أصبح آمنًا للرقابة والإشراف. ولا يتضح لماذا ترى الصين أن هذه مسألة ذات أولوية، في حين أنها لا تحتاج إلى تغيير الحوكمة الدولية للإنترنت للإبقاء على الرقابة من جانبها. وفي المجمل نحن لا نجد سببًا للاعتقاد بأن أيًا من الطرفين من شأنه استبدال القيود المفروضة على التجسس الإلكتروني ببعض التغيرات في حوكمة الإنترنت، إن لم يكن لسبب آخر سوى لأن القضية الأولى هي قضية ثنائية الأطراف والقضية الثانية هي قضية متعددة الأطراف.

والمفاجأة هي أنه رغم ثقة الصين الظاهرية في دقة تسريبات سنودن بخصوص اتساع وعمق اختراق وكالة الأمن القومي للشبكات الصينية، لم يبد المحاورون معنا الكثير من الاهتمام في السعي لتحجيم تجسس الولايات المتحدة الإلكتروني ضدهم في مقابل تحجيم الصين للتجسس الإلكتروني ذي الدوافع الاقتصادية. لا يمكننا أن نتأكد من السبب، لكن تتضح لنا إحدى الدلالات: لا يُحتمل إبرام اتفاق تقدم فيه الولايات المتحدة تنازلًا بشأن التجسس لصالح الصين مقابل توقف الصين عن التجسس الإلكتروني ذي الدوافع الاقتصادية. ففكرة إبرام اتفاقات سلوكية في الفضاء الإلكتروني تتطلب من الصين الاعتراف بتورطها في التجسس الإلكتروني ذي الدوافع الاقتصادية (وهو ما لم تقر به بعد) ويطرح إشكالية وهي أن الامتثال لهذه القواعد سيكون مدفوعًا في كل الأحوال بمشروعية أو عدم مشروعية السلوك بشكل أقل وبمنطق المعاملات بشكل أكثر (الرياء أملًا في الحصول على شيء في المقابل).

ساد بين الذين حاورناهم شعور قوي بأن الولايات المتحدة هي من ينبغي عليها تقديم التنازلات لأنها أقوى من الصين في الفضاء الإلكتروني. ويتسق التباين بين هذا الموقف والمطالبات الأمريكية بأن تكف الصين عما تعتبره الولايات المتحدة سلوك غير قانوني مع المناقشة الواردة في الفصل الثاني. وهذا يعني أن الصين تركز على القوة بينما تركز الولايات المتحدة على القانون (والأنشطة غير القانونية) كأساس للعلاقات الدولية.

البدائل للمفاوضات الثنائية مع الصين

طرح علينا العديد من المشاركين والمحاورين رفيعي المستوى على وجه التحديد أسئلة عما إذا كانت مبادئ الإنترنت التي أقرتها منظمة شنغهاي للتعاون قادرة على أن تكون أساسًا لقواعد السلوك الدولية في الفضاء الإلكتروني.[14] رفضت الولايات المتحدة التصديق على هذه المبادئ، وتحديدًا بسبب تأكيدها على سيادة الدولة على حساب حرية الإنترنت. ولكن حتى ولو كانت هذه المبادئ متسقة مع القيم الأمريكية، فإن هناك قدرًا كبيرًا من الشك داخل الولايات المتحدة أن المبادئ العامة، على هذا النحو، هي بدائل جيدة لإرشادات أكثر تحديدًا حول ما يمكن وما لا يمكن للدول القيام به في

[14] أعضاء منظمة شنغهاي للتعاون هم: الصين وروسيا وكازاخستان وقرغيزستان وطاجيكستان وأوزبكستان.

الفضاء الإلكتروني. ويغلب على الولايات المتحدة تأسيس المبادئ بناءً على التجارب العملية، لكن يبدو أن الصين تميل للعمل بترتيب عكسي.

المشكلة الكبرى التي لم تحل بعد هي ما إذا كان بوسع الاتفاقات متعددة الأطراف بشأن معايير سلوك الدول في الفضاء الإلكتروني، معالجة القضايا التي تفرِّق بين الولايات المتحدة والصين، مع الأخذ بعين الاعتبار أن الولايات المتحدة تهتم أكثر بحل المشكلات الثنائية بينما يبدو أن الصين تهتم أكثر – حتى الآن - بالحفاظ على علاقة ثنائية إيجابية. لا تعارض الولايات المتحدة المفاوضات متعددة الأطراف بشأن الفضاء الإلكتروني، حتى أنها شاركت مع فريق الخبراء الحكوميين التابع للأمم المتحدة لتفوز بالإجماع الدولي على إمكانية تطبيق قانون النزاع المسلح على الفضاء الإلكتروني بقدر تطبيقه على العالم الفعلي.[15]

للاتفاقات متعددة الجوانب مزايا عديدة عن الاتفاقات الثنائية. فهي تميل لاتخاذ وضع دائم أكثر لا وضع مؤقت. وكذلك يمكنها النظر في تصرفات عدد كبير من الأطراف وليس طرف واحد فقط. فمثلًا، حتى وقت قريب، كان المصطلح "التهديد المتواصل المتطور" يستخدم في الولايات المتحدة ليشير لا لشيء تقريبًا إلا لمجموعات القرصنة الصينية. غير أنه منذ نشوب النزاع بين روسيا وأوكرانيا، أظهرت روسيا بشكل متزايد القدرة والاستعداد على إجراء عمليات تجسس إلكترونية اختراقية طويلة الأجل على نفس القدر من التطور.[16] لذا، من الوهم أن نعتقد أن نهاية التجسس الإلكتروني ذي الدوافع الاقتصادية الذي تقوم به الصين يعني نهاية الاختراقات المثيرة للقلاقل حتى للشبكات الخاصة.

لكن الاتفاقات الثنائية يكون لها منطقها الخاص. يسهل إبرام الاتفاقيات المجدية بشكل أكبر – ادعى أحد المشاركين الصينيين أن روسيا دائمًا ما تفسد أي مفاوضات متعددة الأطراف.[17] إذا كانت الولايات المتحدة طرفًا في المفاوضات، يُتوقع أن يصطف حلفاؤها الكثيرون خلفها في أي أمر تقبل به في الفضاء الإلكتروني. كما أنه يسهل

---

[15] آليكس غريغسبي (Alex Grigsby) "فريق الخبراء الحكوميين التابع للأمم المتحدة: ماهو دور الأمم المتحدة؟" Council on Foreign Relations (Net Politics blog), April 15, 2015.

[16] كان الروس في نشاط متواصل بخصوص التجسس الإلكتروني، ولكنهن اتسموا بالمهارة الكافية لإخفاء نطاق نشاطهم بالكامل. تظهر المؤشرات المكتشفة حديثًا عن نشاطهم (1) نشاط أكثر عدوانية، أو (2) الكشف عن بعض معايير مهارتهم للإعلان عن براعتهم، أو (3) كل منهما.

[17] حوار أجري في بكين في 2015.

الحصول على صفقات واضحة في المباحثات الثنائية عن المباحثات متعددة الأطراف، إذ تتطلب هذه الصفقات أن ينقسم المشاركون إلى مجموعتين قبل أن تعرف كل مجموعة ما إذا كانت عروضها سوف تُقبل. وأخيرًا، إذا كان الهدف الأكبر من المفاوضات هو إزالة العقبات لتعزيز العلاقات بين الولايات المتحدة والصين، إذًا فلا بد من الاتفاق الثنائي. ولتوضيح هذه النقطة، إذا كان شرط الولايات المتحدة لمنح الصين الثقة الاستراتيجية مرة أخرى هو توقف الصين عن ممارسة التجسس الإلكتروني ذي الدوافع الاقتصادية، لا يمكن تحقيق هذا الأمر في إطار منتدى متعدد الأطراف.

من القضايا المتعلقة بالموضوع هي إن كان يمكن التعامل مع المشكلات الكبرى بين الولايات المتحدة والصين بالبدء بمعايير بناء الثقة على أمل استخدام الثقة الاستراتجية المكتسبة لتسهيل التوصل إلى اتفاق حول هذه القضايا الكبرى. بناء الثقة يستلزم الوقت: من أجل التوصل للمعايير الملائمة، والتأكد من أن تصرفات كل طرف محل الثقة، والتعلم من هذه التجربة. التكاليف المحتملة لاعتماد منهج قائم على معايير بناء الثقة تتضمن احتمال تأخر تناول الخلافات التي تفرق بين البلدين بسبب الجهود المبذولة في مناقشة القضايا وتأسيس مجموعة من الحلول لتقليص المشكلات. لكن إذا قررت كل من الولايات المتحدة والصين المضي قدمًا عن طريق التركيز على معايير بناء الثقة، فالمجالات المحتملة للاهتمامات المشتركة تتضمن مكافحة التطفل واستغلال الأطفال في المواد الإباحية، والجرائم الإلكترونية التي لا ترعاها الدول، وتجنيد الإرهابيين. وكذلك نادى المشاركون الصينيون بتعزيز مشاركة المعلومات، والمزيد من التعاون بين مكتب التحقيقات الفيدرالي ووزارة الأمن العام الصينية (ما يعني مزيدًا من التركيز على حل الجرائم التي يقع ضحاياها في الدولة الأخرى)، والمزيد من التعاون بين فرق التصدي للطوارئ الحاسوبية من كل جانب، ويعني هذا النهج كذلك الانتباه إلى القضايا التي تثيرها حكومة الطرف الآخر، وتبادل المعلومات بخصوص استخدام الدعاوى القضائية الخاصة لحماية حقوق الملكية الفكرية.[18]

[18] صادفت الجهود الأمريكية لتعليم الصين نظام المحاكم العامة مشكلات مع الحكومة الصينية التي ترى أن الجهود التي تدعم حكم القانون تقوض من سلطتها. يبدو أن القضاء المدني لا يتضمن قضايا السلطة هذه ويجوز تقديم ذلك كحافز على تشكيل الشركات الصينية الناشئة القائمة على التكنولوجيا الفائقة.

والمسألة الأخيرة هي ما إذا كان يجب إجراء المفاوضات بشكل متزامن (كما هو شائع) أو بشكل غير متزامن. المنهج غير المتزامن يتشكل من دوائر فعالة تبدأ عندما يقدم أحد الأطراف لفتة أو تنازلًا، ثم يرد الطرف الآخر بالمثل، ثم يقدم الطرف الأول شيئًا آخر.[19]

تتمثل الميزة الأساسية في الاستراتيجية غير المتزامنة المعتمدة على الرد بالمثل كون كل جانب يمكن أن يدعي أن عروضه مقدمة بلا سبب، لم تصدر مقابل أي شيء، وتدل على تقديره الكبير للطرف الآخر وتفانيه الكلي من أجل العدالة. ويتمثل عيب هذه الاستراتيجية، في هذه الحالة تحديدًا، في أنها لا تقدم أي خيار للتحقق، لأن الخطوات ليست معلومة صراحة بأنها مرتبطة ببعضها أو مشروطة بتصرفات الطرف الآخر. كما لا يمكن أن يؤدي النهج غير المتزامن إلى بناء المؤسسات (على سبيل المثال، جهد للتحقق ثنائي الأطراف). وليس من المستغرب أن الصين تشعر بأنه يتعين على الولايات المتحدة اتخاذ الخطوة الأولى نظرًا لتفوق الولايات المتحدة في الفضاء الإلكتروني (وربما عدة خطوات بعد ذلك أيضًا، نظرًا للتفوق المتصور من حيث القوة الشاملة للولايات المتحدة في مقابل الصين).

قانون النزاع المسلح وحق الرد

من ضمن القضايا التي خضنا فيها أثناء نقاشاتنا مع المحاورين الصينيين كانت آراؤهم بشأن مدى إمكانية تطبيق القوانين والقواعد على الفضاء الإلكتروني، مثل قانون النزاع المسلح، أو الحق في الرد بعد التعرض لهجوم. وكما أسلفنا الذكر، رغم أن الولايات المتحدة تبدي اهتمامها بالتفهم المشترك الذي يفيد بضرورة إخضاع الحرب الإلكترونية إلى قانون النزاع المسلح، تشعر الصين بالإنزعاج من المبدأ. ونظريًا، إن وضع الحرب الإلكترونية تحت مظلة قانون النزاع المسلح يفرض المزيد من القيود على هذا النشاط (مثل تجنب استهداف الأنظمة المدنية البحتة)، غير أن الصين ترى أن

---

[19] اشتهر هذا النهج عن طريق عمل نظرية اللعبة القائم على دراسات روبرت أكسيلرود (Robert Axelrod) لاستراتيجيات العين بالعين في اللعبة المنفذة بالكمبيوتر لمعضلة السجين كما صاغها روبرت أكسيلرود، *The Evolution of Cooperation*، نيويورك: Basic Books, 1984. ورشّح ذلك أيضًا في كتاب لايل جيه. غولدستين (Lyle J. Goldstein)، لقاء الصين في منتصف الطريق *Meeting China Halfway*، واشنطن العاصمة: صحافة جامعة جورجتاون، 2015، رغم أن غولدستين (Goldstein) لا يناقش تطبيق هذا النهج على العلاقات مع الصين بشأن الأمن الإلكتروني.

النتيجة الجوهرية لإخضاع الحرب الإلكترونية تحت مظلة قانون النزاع المسلح ليست تقييد الحرب الإلكترونية وإنما لشرعنتها كمفهوم وعسكرة الفضاء الإلكتروني.[20]

أثارت تأكيدات الولايات المتحدة على الحق الفردي في الرد على الهجمات الإلكترونية انزعاج المحاورين الصينيين على وجه التحديد. ذكر عدد من المشاركين في الحوار استراتيجية وزارة الدفاع الأمريكية للفضاء الإلكتروني مع ناقوس خطر: وأسماها أحدهم "السعي وراء القوة أحادية الجانب".[21] كانوا متشوقين لمعرفة إلى أي حد مثلت انحرافًا عن استراتيجية البيت الأبيض الدولية للفضاء الإلكتروني الصادرة في العام 2011 الاستراتيجية الدولية للفضاء الإلكتروني: الرخاء والأمن والانفتاح في عالم متصل بالشبكات.[22] في واقع الأمر، رغم معرفتهم أن الاستراتيجية الأخيرة تثير القلاقل، فضلها المحاورون على وثيقة وزارة الدفاع الأمريكية، ومنحوا على استراتيجية البيت الأبيض صبغة عقلانية (وهو أمر لا يميز تصريحات الصين بشأن الوثيقة ذاتها عند صدورها لأول مرة عام 2011).[23]

عندما طرحنا سؤال الحق في الرد على الهجوم الإلكتروني، لم يتحمس أي من المشاركين في الحوار من الصينيين إلى توضيح كيف يمكن للصين أن تستجيب مع السيناريو الافتراضي الذي اخترق فيه أحد جيرانها (الذي لم تتم تسميته) الحكومة الصينية وأدار المنفذ الإعلامي وأغلق العمليات ودمر أجهزة الكمبيوتر. وكان الرد المتكرر هو أن الهجمات الإلكترونية ليست هجمات فعلية وأن التعرض للهجوم الإلكتروني ليس أساسًا لإعلان حالة الحرب. إذا لم يكن الصراع الديناميكي في العالم

---

[20] تتوافق هذه النتائج مع تجارب باحثين آخرين. وعلى سبيل المثال، تقول آشلي ديكس (Ashley Deeks) إن البروفيسور هوانغ جيخيونغ (Huang Zhixiong) من جامعة واهان Wuhan University انتقد دليل تالين لوضع مستوى منخفض جدًا للمعايير لما يشكل استخدام القوة في الفضاء الإلكتروني، واعترض على حقوق الدول في المطالبة بحقوق الدفاع عن النفس، معلنًا أن الدول ليس لها الحق في شن هجمات دفاع عن النفس ضد الأطراف من غير الدول أو الخوض في هجمة إلكترونية استباقية، وقال إننا في المجمل ينبغي ألا نفكر في الوسائل التي بمقتضاها يجوز تطبيق قانون النزاع المسلح الدولي على الفضاء الإلكتروني. انظر ديكس، 2015.

[21] U.S. Department of Defense, *The Department of Defense Cyber Strategy*, April 2015.

[22] White House, 2011.

[23] لا يتضح إذا كان الاختلاف بين الوثيقتين يمثل تحولًا في استراتيجية الردع الأمريكية (خاصة بعد الهجمات الإلكترونية التي شنتها كوريا الشمالية على شركة سوني) أم يعكس حقيقة أن الوثيقة الأولى نشأت نتيجة للعملية التي تتم بين الوكالات (ولذلك تم حمايتها بعناية)، بينما نتجت الثانية عن وزارة الدفاع فقط. لم يبد على المشاركين في الحوار الاقتناع بوضع الوثيقة الثانية عندما فسرناها على هذا النحو.

الفعلي دائرًا الآن، ينبغي على الدول ألا ترد على الهجوم الإلكتروني بأعمال عدائية خاصة بهم. كان من الصعب على المشاركين تخيل وجود هجوم إلكتروني من شأنه أن يتسبب في دمار يساوي دمار الحرب. لكن ينبغي ألا يُفسر ذلك ليشير إلى أن الصين لن ترد على أي هجوم إلكتروني، ولكن ينبغي تفسيره بأنه على المفكرين الصينيين التعامل بجدية مع هذه القضية. ولذلك، لم يفكروا بعد بالتحديد في أنواع الهجمات التي يتعين عليهم الرد عليها ولا في كيفية الرد.

في ضوء التحليل السابق لطريقة التفكير الردعية للصين، تضع إجابات المشاركين الصينيين في حسبانها العلاقة الشاملة بين الصين وهدف الهجوم الإلكتروني المتصور، وذلك لا ينحصر في تقييم القوة المستخدمة والدمار الذي تسببت فيه، بل يشتمل كذلك على الدلائل السياسية المحلية للهجوم (هل تعرضت الحكومة الصينية للضغط الشعبي للرد أم أن أنباء الهجمات كانت مقتصرة على دائرة منتقاة من كبار الساسة؟) بالإضافة إلى تقييم الحكومة الصينية لقدراتها قبل الرد. باختصار، سيعتمد رد الصين في الغالب على أكثر من مجرد تقييم لأثر الهجوم الإلكتروني.

فسرنا ردود الفعل هذه على أنها دليل بأن الصين ليس لديها بعد موقف واضح لردع الهجمات الإلكترونية. يتطلب مفهوم الردع التقليدي أربعة شروط مسبقة وهي: الحدود، والإسناد، والمصداقية، والقدرة (على الرد). لذلك، تتطلب سياسة الردع الفعالة استيفاء هذه الشروط المسبقة في ضوء وجود معتدين محتملين. على سبيل المثال، حتى إذا ظن الهدف أن لديه القدرة على الإسناد، فإذا ظن المعتدي المحتمل أن هدف الهجوم الإلكتروني يفتقر إلى الثقة في إسناده، تضطرب عملية الردع. إذا كانت الصين تمتلك موقف ردع جاد للهجمات الإلكترونية، لن يضطر بقية العالم إلى تخمين ما هو هذا الموقف، لأنه سيعرفها.

لاحظ أن هذا الأمر يختلف عن القول بأن موقف الصين لردع الهجمات الإلكترونية يعكس ببساطة موقف الصين للردع عمومًا. في العموم، تبقي الصين على درجة من الغموض كاستراتيجية لتضخيم نفوذها وقدرتها على إجبار الآخرين على احترامها. رغم ذلك، أوضحت الصين أن "لصبرها حدود"[24]– وهي ترفض ببساطة بيان مدى هذه الحدود بالضبط، بل تفضل النهج القائم على التلميح باتجاهها وقربها

[24] Paul H. B. Godwin and Alice L. Miller, *China's Forbearance Has Limits: Chinese Threat and Retaliation Signaling and Its Implications for a Sino-American Military Confrontation*, Washington, D.C.: National Defense University Press, April 2013.

وتسمح لهدف الردع أن يستنبط أنه يجازف بصدور رد الفعل الصيني العنيف. وفي مجال الفضاء الإلكتروني، لم توضح الصين، بأي شكل واضح، قدرتها على تحديد الأفعال التي تتخطى خطوطها الحمراء (غير المعلنة)، وتؤكد بما لا يدع مجالًا للشك بإمكانية الإسناد في الفضاء الإلكتروني، ولم تعلن بوضوح عن رغبتها في الرد على الهجمات الإلكترونية. وحقيقةً، تمادت الصين إلى حد إرسائها دلائل مكلفة نسبيًا ليمكنها التراجع متى قررت أنها ترغب في الرد على الهجوم الإلكتروني سواء عن طريق الرد الإلكتروني أو الحركي.

كما أسلفنا في التقرير، إذا شكت الصين في قدرتها على إسناد هجوم بحسم لكنها تتصور أن الاختراق صدر من الولايات المتحدة، سيتعين عليها تقييم بعض العوامل في ردها، مثل تقييم انعدام ثقتها في إمكانياتها الإسنادية وتقييم ضعف قوتها مقابل الولايات المتحدة، ومقارنتها بمخاوفها من أن تصرفات الولايات المتحدة قد تكون موجهة نحو إحداث تغير نوعي في ميزان القوى الإجمالي. بالإضافة إلى ذلك، سيتعين على قادة الحزب الشيوعي الصيني النظر في أي عواقب محتملة على استقرار النظام الداخلي. ثمة اعتبارات إضافية من شأنها أن تشكل موقف الصين للردع الإلكتروني:

- يدرك قادة الصين تمامًا الحالة الهشة للبنية التحتية لشبكات الدولة.
- مقارنة بالمخاطر اليومية التي تواجهها البنية التحتية للصين (انقطع الإنترنت عن محافظات بأكملها بسبب حادث عارض في ألعاب الكمبيوتر)،[25] قد تبدو المخاطر الواردة من الخارج أقل إلحاحًا مما هي عليه في الولايات المتحدة.
- وفي الوقت نفسه، إذا نما إلى الأذهان أن الصين تعرضت لهجوم إلكتروني، ربما يتساوى الضغط السياسي على قيادة الحزب الشيوعي أو حتى يزيد عن الضغوط التي تشهدها الولايات المتحدة، لأن النظام يعتمد بشكل أكبر على القومية ولأن مخاطر عدم الرد من أي قائد قد تعرض موقفه للخطر (لأن السلطة في الصين توضع في أيدي الأشخاص أكثر منها في المؤسسات على خلاف الولايات المتحدة).[26]

---

[25] Owen Fletcher, "China Game Boss Sniped Rivals, Took Down Internet," *PC World*, August 29, 2009.

[26] تتمثل إحدى الاختلافات الممكنة لذلك في أن الجانب الصيني يتحكم في الإعلام بدرجة أكبر من الولايات المتحدة، وفي غياب صحافة الفضائح، بالكاد تصل أنباء الهجمات الإلكترونية على الصين إلى الإعلام الصيني لأن الحكومة تفضل الإبقاء عليها سرًا.

- منظور الصين للردع أكثر شمولًا من منظور الولايات المتحدة (كما ناقشنا في الفصل الثاني).
- تتخلف الصين عن الولايات المتحدة في صنع السياسات الخاصة بالفضاء الإلكتروني من حيث البيانات عالية المستوى، والوثائق الصادرة علنًا، وإقامة أجهزة لصناعة القرارات المتعلقة بالسياسات.

وفي العموم، اعتقد المشاركون في الحوار الذين عبروا عن رأيهم بصراحة بهذا الشأن أن الولايات المتحدة تسبق الصين كثيرًا من حيث إمكاناتها في الحرب الإلكترونية.[27] واعتقد أحدهم أن الصين أوشكت على اللحاق بها. وأعرب مشتركان عن مخاوفهما من احتمال استهداف الولايات المتحدة للبنية التحتية للقيادة والتحكم النووي بالصين.[28]

اقتراح التحمل المتبادل

نصحنا زملاؤنا الأمريكيون، الذين مروا بتجربة إجراء حوارات مع الرعايا بشأن الأمن الإلكتروني في الصين، ألا نتوقع إفصاح المتحاورين الصينيين عن الكثير كنوع من المبادرات التفاوضية. وبناءً على هذه المعلومة، قررنا أن نقترح بأنفسنا بعض النقاط ونقيس ردود أفعال المتحاورين عليها.[29] وبهذا قدمنا هذا المقترح المكون من ثلاثة أجزاء للمتحاورين الصينيين من أجل النظر فيه والتعقيب عليه.

بالنظر في رغبة الولايات المتحدة والصين في تقليص الشكوك المتبادلة في الفضاء الإلكتروني، يتبقى خيار واحد وهو التفاوض على اتفاق حول مجموعة من القواعد. وبما أن الطرفين عبرا عن مخاوفهما بشأن احتمال استهداف الطرف الآخر لبنيته التحتية الحيوية، سيكون جوهر الاتفاق هو تخلي كل من الولايات المتحدة

---

[27] حوار أجري في بكين، مايو/آيار 2015.

[28] حوارات أجريت في بكين، مايو/آيار 2015. وضعنا تعليقًا عن استنتاجات الصين من ستوكسنت في هذه الفئة، رغم أن ستوكسنت استهدفت منشأة إنتاج نووي ولم تستهدف مركز قيادة وتحكم النووي.

[29] قبل شروعنا في رحلتنا البحثية، عقدنا حلقة نقاش مدتها ساعتان مع خمسة خبراء بارزين مختصين بمنظور الصين عن الأمن الإلكتروني وأخذنا بنصائحهم وآرائهم في استطلاعات الرأي التي أعددناها للحوار. ونشعر بالامتنان للأفراد الذين شاركوا في حلقة النقاش المذكورة، والتي ساعدتنا على تنقيح أسئلة الحوار قبل سفرنا إلى الصين.

والصين عن شن الهجمات الإلكترونية على البنية التحتية الحيوية للدولة الأخرى.[30] لاقى هذا المقترح إعجاب المشاركين في الحوار، وتفاعل معه بإيجاب جميع المتحاورين من المؤسسات الأكاديمية ومراكز الأبحاث والجيش والمنظمات الحكومية.[31] أظهر المشاركون وجهات نظر متطابقة نسبيًا مع آراء نظرائهم الأمريكيين بشأن تعريف البنية التحتية الحيوية – التي تضم شبكة الكهرباء والنظام المصرفي. وذكر أحد المشاركين وجود سابقة على مثل هذا الاتفاق، ففي أوائل مايو/آيار 2015، قبل إجرائنا للقاءاتنا الميدانية ببضعة أيام، أعلنت روسيا والصين عن اتفاق عام بالتعاون سويًا في الفضاء الإلكتروني وعدم الاعتداء على بعضهما البعض فيه.[32]

المكون الأول لأي اقتراح تحمل متبادل هو إحراز تقدم فيما يخص عدم الاعتداء على البنى التحتية الحيوية منذ حواراتنا في بكين. وفي يوليو/تموز 2015، وقعت الصين على تقرير للأمم المتحدة يطالب بنبذ هذه الهجمات.[33] وكذلك ثمة دلائل على اتفاق الولايات المتحدة والصين بعدم التعدي على البنى التحتية الحيوية لبعضهما البعض – أو على الأقل ألا تبادر أي منهما بذلك.[34] غير أنه حتى كتابة هذا التقرير، لم يوجد مؤشر يذكر على أن هذه الاتفاقات قد تطورت من مرحلة "عدم الثقة" إلى شئ يمكن التحقق منه. ولهذا السبب ثمة مكونان آخران لهذا الاتفاق وهما ضروريان لاستيفاء أغراض المكون الأول.

ينطوي المكون الثاني، والمنطقي، لأي اقتراح تحمل متبادل، على اتفاق الولايات المتحدة والصين بعدم ممارسة التجسس الإلكتروني على البنى التحتية الأساسية للطرف الآخر. والسبب المنطقي لهذه الخطوة هو أن التجسس الإلكتروني دائمًا ما يكون شرطًا مسبقًا للهجوم الإلكتروني، وأنه يستحيل التمييز بين الاختراقات لأغراض التجسس

---

[30] قال أحد المشاركين أن تعريف البنية التحتية الحيوية لن يكون سهلًا لأن التعريف الدقيق لها قد يكون حساسًا. ربما يستطيع الصليب الأحمر المختص بالفضاء الإلكتروني القيام بذلك بمصداقية. ولكن في رأينا، حتى التعريف غير الدقيق كافٍ، شرط أن يكون واضحًا لا لبس فيه.

[31] حوارات الكاتب التي أجريت عام 2015.

[32] Andrey Ostroukh, "Russia, China Forge Closer Ties with New Economic, Financing Accords," *Wall Street Journal*, May 8, 2015.

[33] الجمعية العمومية للأمم المتحدة (الدورة السبعون) "فريق الخبراء الحكوميين التابع للأمم المتحدة بشأن التطورات في ميدان المعلومات والاتصالات في سياق الأمن الدولي" 22 يوليو/تموز 2015.

[34] David E. Sanger, "U.S. and China Seek Arms Deal for Cyberspace," *New York Times*, September 19, 2015.

الإلكتروني والهجوم الوشيك إذا تعرف عليه الهدف. وإذا لم تكن في نية أي طرف شن هجوم على البنية التحتية للطرف الآخر، لن يضطر أي من الطرفين إلى تعريض أنظمة البنى التحتية الحيوية للطرف الآخر للخطر، خاصة إذا تم تنفيذ الهجوم بإدخال شيفرة خبيثة في البنية التحتية للهدف. وفي الواقع، يتطلب كل من التجسس الإلكتروني والهجوم الإلكتروني الزرع المسبق لشيفرة الكمبيوتر في الأنظمة المستهدفة، والذي يتصل (يرسل إشارات لاسلكية) دوريًا بالمعتدي للحصول على المزيد من التعليمات. تسهل الأدوات المزروعة من الاختراقات التالية كثيرًا إذ يتواجد المعتدون بالفعل داخل الأنظمة المستهدفة. ويؤدي منع التجسس الإلكتروني على البنية التحتية الحيوية إلى صعوبة شن الهجمات الإلكترونية على البنية التحتية. ودون التخطيط المسبق والتجسس الإلكتروني، يلزم لشن هذه الهجمات أسابيع أو شهور أو حتى سنوات، لكن إذا تواجد كل خصم محتمل داخل البنية التحتية الحيوية للطرف الآخر، يمكن شن الهجمات في الحال.

من المرجح أن يكون لهذا الحظر مزايا عديدة، إذا طبقه الطرفان.

أولًا، التطبيق الفعال لهذا الحظر من شأنه أن يدعم الاستقرار لأنه سيحول دون تعرّض الأنظمة ذات الأهمية القصوى للاستهداف.

ثانيًا، سيزيد الحظر من تكاليف استهداف هذه الأنظمة (لأنه في حالة اكتشاف أن الصين تمارس ذلك الأمر، ستكون قد نكثت بعهدها، مما قد يؤثر على قدرتها على التفاوض بمصداقية على القضايا الأخرى في المستقبل)، كما أنه سيعالج في نفس الوقت مشكلة الوقت التي يمكن أن تشكلها الهجمات الإلكترونية المعدة مسبقًا.

ثالثًا، إذا تحقق هذا الاتفاق بأكمله، فسوف يقلل من احتمالية نشوب نزاع عرضي عبر إلزام الطرفين، ليس بعدم الاعتداء على البنية التحتية الحيوية للطرف الآخر فحسب، بل بل بتجنبها تمامًا، ما يحد من احتمال الخلط بين عمل تجسس إلكتروني والهجوم الوشيك.

رغم رفض المشاركين في الحوار عمومًا الموافقة بشكل واضح على الجانب الثاني المذكور من الاقتراح، إلا أنهم لم يردوا عليه صراحةً. فهم المشاركون المنطق الذي ربط بين الهجمات والتجسس، وكذلك فكرة أنه في حالة نبذ الفرد الاعتداء على نظام ما، يكون منطق التجسس عليه ضعيف للغاية. ولم يشعر المشاركون تمامًا بالراحة تجاه مفهوم التخلي عن جميع أنشطة التجسس ضد البنية التحتية الحيوية للولايات المتحدة.

يركز المكون الثالث لمعاهدة التحمل المتبادل على الإسناد وقبول فرض العواقب.[35] ولكن أحيانًا لا تكون المشكلة فنية لا من قريب ولا من بعيد،[36] بل سياسية: ما هي التدابير التي من شأنها إقناع الصين بقبول الأدلة (دون أن يكون من الصعب، في الوقت نفسه، التوصل إلى استنتاجات معقولة من هذه الأدلة)؟[37] إن كان هناك عملية للإسناد متفق عليها من الطرفين وإن أمكن الاعتماد على الصين للاستجابة بالرد الملائم إذا أشارت العملية إلى أن أثر الاعتداء على البنية التحتية الحيوية يشير إلى الصين، يقل بالتالي تهديد الصين على البنية التحتية الحيوية للولايات المتحدة (والعكس). تعزى المشكلة السياسية إلى أن الولايات المتحدة تكشف الصين أثناء تجسسها عليها أكثر بكثير من كشف الصين لتجسس الولايات المتحدة. تزعم الصين أنها تتعرض لهجمات متكررة من الولايات المتحدة (التي لا تزال، على سبيل المثال، المصدر الرئيسي لخوادم القيادة والتحكم للبوت والبوت-نت)، لكنها لم تقدم أي دليل على أن حكومة الولايات المتحدة توفر الحماية للمخترقين (أو على الأقل المخترقين الأفراد) أو تشن اختراقات معينة.[38]

ويعكس عزوف الصين عن قبول اتهامات الولايات المتحدة بالاختراقات الصينية حقيقة أن الصين لا يمكنها تحديد وإسناد التجسس الإلكتروني الأمريكي بقدر استطاعة الولايات المتحدة تحديد وإسناد التجسس الإلكتروني الصيني. ترتكز هذه الحقيقة على ثلاثة اختلافات: يتخلف الأمن التشغيلي الصيني عن إمكانات الولايات المتحدة، وتتخلف

---

[35] ليس من الضروري على الإطلاق رصد وإسناد جميع الاختراقات أو معظمها أو حتى جزء كبير منها – كما هو الحال في سياسة الردع. لكن من الضروري أن يتم الكشف عن بعض هذه الاختراقات بثقة كافية للتأكد بنسبة كبيرة من قيام طرف ما بالغش.

[36] يبقى عدد قليل من الهجمات الإلكترونية من دون إسناد هذه الأيام، وإن التزمت الأجهزة الاستخباراتية الصمت، لن تتوانى الشركات الخاصة عن تقديم رأيها لمن يطلبه. غير أن الدليل الذي يدعم هذه التأكيدات لا يناقش كثيرًا (لا تفضل الأجهزة الاستخباراتية الكشف عن أساليبها، والشركات الخاصة لا تحبذ الحديث هي أيضًا). إن انعدام الشفافية وراء الإسناد يتيح المجال أمام المتهم بأن يؤكد براءته ويبدو مقنعًا في قيامه بذلك الدور.

[37] لا تُنشر جميع أدلة الإسناد للجمهور (انظر مقال ديفيد إي. سانغر (David E. Sanger) ومارتن فاكلر (Martin Fackler)، بعنوان "يصرح المسئولون بأن: وكالة الأمن القومي اخترقت شبكات كوريا الشمالية قبل الهجمات على شركة سوني" نيويورك تايمز *New York Times*، 18 يناير/كانون الثاني 2015). ويشير ذلك إلى خلافات لا يمكن رأبها بين الثقة التي يضعها المسئولون الأمريكيون في الإسناد والثقة التي يشعر بها الشخص العادل غير المتحيز الذي يستند إلى مصادر مفتوحة ولكنه غير مستعد لتصديق أقوال المصادر الأمريكية بظاهرها.

[38] وفكرة أن الولايات المتحدة تزود التحقيقات في الجرائم المرتكبة ضدها بموارد أكثر من الموارد التي تزود بها التحقيق في الجرائم ضد الآخرين هي فكرة معقولة، ولكنها أيضًا عالمية وتختلف تمامًا عن أسلوب المماطلة.

قدرة الصين على تحديد الاختراقات عن إمكانات الولايات المتحدة.[39] ما دامت إمكانات الصين الإسنادية تتخلف عن قدرات الولايات المتحدة، يصعب إقناع الصين بأن مثل هذه الصفقة عادلة. بل حتى أسوأ من ذلك، وإلى أن تسترد الصين ثقتها في إمكاناتها الإسنادية الخاصة بها، لن تعتقد أن الإمكانات الإسنادية الأمريكية جيدة كذلك.[40] وأشار عدد من المشاركين إلى صعوبة التوصل إلى اتفاق مجدٍ من دون تطوير إمكانات الصين الإسنادية.

ثمة عدة طرق محتملة لإنشاء آلية إسناد جديرة بالثقة. ولكن أيًا منها لا يعالج المشكلة بشكل قاطع، وسيصعب اعتماد الكثير منها من قِبل الجانبين لاعتبارات سياسية. وثمة خيار آخر وهو تأسيس هيئة مستدامة وثنائية الأطراف لتقصي الحقائق للتحقيق في ادعاءات الهجوم الإلكتروني. تتمثل مزايا هذه الطريقة في اشتراك كلا الجانبين في المداولات، ومن ثم يكونا أكثر استعدادًا لقبول نتائج أي تحقيق مشترك. لكن تواجه هذه الطريقة بعض المخاطر. يساور الولايات المتحدة القلق بشأن مشاركة الصين، إذ تظن أن مثل هذه الهيئات ستشارك بإيعاز من حكومتها، وبالتالي لا يرجح أن تكون حرة في تقرير أنه تم تنفيذ الهجمات من قِبل الحكومة الصينية أو جيش التحرير الشعبي الصيني. ومن جانبها، تشعر الصين بأن الإمكانات الأمريكية شديدة التفوق حتى أن هذه الهيئة الدائمة قد تتحول إلى منتدى تسيطر عليه الولايات المتحدة ويتقلص دور الصين فيه إلى موضع المشاهد. وفي المقابل، إذا كان التجسس الإلكتروني الصيني بالفعل أكثر تهتكًا وأوسع نطاقًا من التجسس الإلكتروني الأمريكي، من المحتمل أن تكون القضايا التي ترفع أمام مثل هذه الهيئة صينية بأغلبية ساحقة أو تكون صينية الأصل بشكل حصري، مما يعرض الصين للإحراج والمهانة.

قد يساعد تحويل هذه الهيئة من ثنائية الأطراف إلى منتدى متعدد الأطراف في تهدئة بعض هذه المخاوف (لأن تمثيل كل من الولايات المتحدة والصين في الهيئة سيكون ضعيفًا). واقترح أحد المشاركين اتخاذ الوكالة الدولية للطاقة الذرية كنموذج

---

[39] في الولايات المتحدة، تنفَّذ نسبة كبيرة من الكشف والاختراقات من قِبل الشركات الخاصة (ويعمل بها الكثير من موظفي وكالة الأمن القومي السابقين). وما تقوم به الصين ما هو سوى بداية لإنشاء شركاتها الخاصة بالأمن الإلكتروني (انظر على سبيل المثال "انشقاق القراصنة الصينيين إلى الجانب الآخر، تحولوا إلى حراس الفضاء الإلكتروني،" جابان تايمز *Japan Times*، 30 يونيو/حزيران 2015.) وبذلك، تستطيع الولايات المتحدة شراء خبراء مختصين بالأمن الإلكتروني. حتى وإن كانت بعض الشركات الأمريكية قد ترفض الأعمال الصينية، تتوفر شركات الأمن الإلكتروني خارج الولايات المتحدة (إسرائيل وروسيا، على سبيل المثال).

[40] لعل المخترقين الذين تم اكتشافهم وهم يتجسسون يؤمنون أنه تم الكشف عنهم بشكل عادل، ولكن بغياب شهادتهم في هذا الشأن، قد يحتفظ مجتمع وضع السياسات الصيني بشكوكه.

يحتذى به، بينما رد مشارك آخر بأن هذا النموذج لا يعد ملائمًا لأن عدد مستخدمي الإنترنت يفوق من يتعامل مع المؤسسة النووية في بلده. بالإضافة إلى ذلك، لا يتضح ما إذا كانت الصين سترى فرقًا إذا تم استبدال الخبراء الأمريكيين بخبراء (وكثير منهم لديهم علاقات مع الولايات المتحدة) من دول ترى الصين أنها صديقة للولايات المتحدة.

هل يمكن خفض هذه العقبات إذا عرضت الولايات المتحدة تبادل خبراتها بشأن أساليب الإسناد مع الصين مقابل استعداد الصين للإقرار بأن هذه الأساليب تعد دليل تحقق ومن ثم تنتقل إلى إدانة من قاموا بهذه الاختراقات؟ للوهلة الأولى، يبدو هذا الاقتراح غير محتمل: تحت أغلب الظروف، لا تتبادل الدول تكنولوجيا استراتيجية أو مفاهيم تشغيلية مع الخصوم المحتملين. لكن هذا النمط العام له استثناءات. على سبيل المثال، فإن الولايات المتحدة -أثناء سعيها نحو الاستقرار النووي- قد شجعت الدول الأخرى على إدخال روابط الاستخدام المصرح به في أسلحتها النووية (وهي تكنولوجيا تمنع استخدام هذه الأسلحة عن طريق الخطأ أو بدافع من المستخدمين غير المرخص لهم). ومن المزايا الإضافية هي أن الإمكانات الإسنادية الصينية القوية يمكنها تخفيض فرص النزاع التي تنشب بفعل محفز في حال تعرض الصين لهجوم من شخص ينتحل شخصية مصدر أمريكي. ومن الناحية العملية، فالولايات المتحدة ليست مضطرة إلى مشاركة ما يعرف عادة على أنه مصادر وأساليب استخباراتية سرية، بل يمكنها الاستفادة من التطويرات الجديدة في الإمكانات الإسنادية الخاصة (أغلبها، وليس كلها، مرتبط بالشركات التي يوجد مقرها في الولايات المتحدة) لمنح الصين ثقة أكبر في إمكاناتها الإسنادية.

ومن الجدير بالإيضاح أن عرض الولايات المتحدة لمساعدة الصين على تقريب مستوى إمكاناتها الإسنادية من مستوى الولايات المتحدة لا يعني أن الولايات المتحدة ستعلم الصين كيفية رصد اختراقات التجسس الإلكتروني، أو تحسين دفاعاتها أو كيفية الحفاظ على اختراقاتها دون أن تكشفها الولايات المتحدة، ناهيك عن أنه لا علاقة لها بتحسين كفاءة الاختراقات الإلكترونية أو إمكانات الهجوم للصين. وهكذا، تقديم يد المساعدة إلى الصين لتحسين إمكاناتها الإسنادية إلى مستوى الولايات المتحدة لربما يساعد الصين على إخفاء هجماتها. وبقدر أنه لايزال على الولايات المتحدة استخدام مثل هذا الإسناد لكبح التجسس الإلكتروني الصيني (والهجمات الإلكترونية)، لا تتضح

بالضبط قيمة الخسارة وإن كانت كبيرة أو طفيفة.[41] حتى مع تزايد صعوبة إسناد الهجمات إلى الصين، لن يحدث ذلك فرقًا كبيرًا لأن الصين لا تعترف بتورطها في مواجهة الأدلة الكثيرة في يومنا هذا.

تفاعل المشاركون الصينيون في الحوار بإيجابية مع هذا الاقتراح، حتى بعد إضافة التلميح بأن الولايات المتحدة سوف تتوقع من الصين تصديق الأدلة التي تشير لإصدار مجموعة اختراقات معينة من الصين. وبالنظر إلى الحساسيات المرتبطة بطريقة عمل الإسناد في الولايات المتحدة، فإن الصفقة التي تجذب الصين للمشاركة في نظام إسنادي في مقابل إمكانية قيام الولايات المتحدة بتعليم الصين كيفية إجراء الإسناد، ستتطلب على الأغلب أبحاثًا ومحاذير إضافية قبل تبنيها كسياسة. وبالنسبة للصين، يجب تضمين اتفاق بشأن الكف عن مهاجمة البنية التحتية الحيوية رسميًا وبوضوح، ويفضل تدريجيًا، مع إرساء عواقب وخيمة في حالات الغش. غير أن هذا الاقتراح يحمل طيه بعض الاحتمالات بزيادة تكاليف التجسس الإلكتروني إلى الحد الذي تقل فيه أو تُلغى الأفعال الأقل مستوى وغير الاستراتيجية (أي، الاقتصادية). كما أنه يقلل مخاطر الإسناد الخاطئ بسبب وجود أطراف ثالثة خبيثة تسعى إلى توجيه هجماتها بطريقة أو بغيرها باستخدام خوادم أمريكية أو صينية. يبدو أن هناك أحد المجالات التي يمكن فيها الحصول على مساهمات ومكافآت من كلا الجانبين. ولهذه الأسباب، ربما يستحق الأمر المزيد من الدراسة.

وعلى الرغم من أن استخدام الإمكانات الإسنادية لطرف ثالث محايد لتنفيذ جوانب الجاسوسية غير الإلكترونية لهذه الاتفاقية هو، في رأينا، أفضل من تحسين الإمكانات الإسنادية الصينية، إلا أن الخيار الأخير يمكن أن يكون ثمنًا مقبولًا لإقناع الصين بأنها لا تستطيع تحمّل عواقب أن يتم كشفها أثناء التجسس على البنية التحتية الحيوية الأمريكية – رغم أن الصين اليوم بوسعها بكل ابتهاج تجاهل جميع الأدلة التي تظهرها وهي تتجسس حيث ينبغي ألا تكون.

---

[41] إذا سعت الصين جاهدةً، بسبب هذه الاتفاقية، إلى تجنب الإسناد (بالاستفادة جزئيًا مما تعلمته عن كيفية القيام بالإسناد)، سترتفع تكلفة ارتكاب الصين للتجسس الإلكتروني وبالتالي سيقل حجمه. ترتفع التكلفة بسبب الجهود الإضافية التي ستبذلها الصين لتجنب الإسناد، إلى جانب الاختراقات التي قد تراها بالتالي مجازفة كبيرة في هذه البيئة الجديدة.

الخاتمة

تدفع الأهمية العالمية للعلاقات بين الولايات المتحدة والصين واحتمال أن تلعب النزاعات بشأن الفضاء الإلكتروني دورًا تخريبيًا متزايدًا في العلاقة بين البلدين إلى التوصل إلى نوع من الاتفاق بشأن سلوك كل منهما في الفضاء الإلكتروني. وعلى مدار اللقاءات التي أجريناها في الصين في مايو/آيار 2015، بدا على أغلب المحاورين المشاركين معنا أنهم لا يرون أن أي اتفاق مع الولايات المتحدة منطقي أو محتمل أو حتى ضروريً أو حتى ضروريًا بالتحديد. في حين بدا على الولايات المتحدة أنها رأت العلاقة الضعيفة بين البلدين فيما يتعلق بالفضاء الإلكتروني، يبدو أن المتحاورين الصينيين في المقابل لم يجدوا أي ضرورة ملحة في إجراء التغيير. وبالتالي، كان اتفاق الولايات المتحدة والصين بشأن الفضاء الإلكتروني في سبتمبر/أيلول 2015 مباغتًا للمحاورين المشاركين معنا بقدر ما كان مباغتًا لغالبية المعنيين بالعلاقات بين الولايات المتحدة والصين (بمن فيهم مؤلفو هذا التقرير). وحتى منتصف فبراير/ شباط 2016، لم يتضح بعد إذا كان الاتفاق بشأن الفضاء الإلكتروني الذي تم إبرامه أثناء القمة بين الرئيسين شي وأوباما قد عالج قضية التجسس الإلكتروني ذي الدوافع الاقتصادية.[1]

كان أول استنتاجاتنا هو: إذا أصرّت الولايات المتحدة على تبني نهج قائم على المفاوضات يناقش نطاق التجسس الإلكتروني الصيني بالكامل، لا يحتمل تكليل هذا المسعى بالنجاح في وقت قريب، إلا إذا زادت تكلفة رفض الصين للتفاوض بخصوص قضية الفضاء الإلكتروني (زادت عن مجرد تهديد بإلغاء اجتماع القمة أو فشله). ويمكن

[1] انظر حاشية هذا التقرير لمعرفة المزيد عن الاتفاق الثنائي بين الولايات المتحدة والصين بخصوص الفضاء الإلكتروني في سبتمبر/أيلول 2015.

تحقيق ذلك من خلال ربط هذه القضية بشكل مباشر أكثر بجودة العلاقة ككل عبر إرسال الاحتجاجات إلى الصين على أعلى مستوى أو عبر استخدام أدوات أخرى، مثل التهديد بفرض عقوبات اقتصادية أو الرد بالمثل. غير أنه لا يوجد ضمان على أن الاستراتيجية المبنية فقط على فرض العقوبات على الصين بسبب تصرفاتها أو رعايتها أو استعدادها للتغاضي عن التجسس الإلكتروني سيحقق النتيجة المطلوبة وهي الحد من التجسس الإلكتروني الصيني أو إرساء القواعد بشأن الأهداف المحظورة على التجسس الإلكتروني. وهذا يعني أن الجهود المتواصلة لحل الخلافات وإرساء القواعد عن طريق الحوار والتفاوض هي أمر مرغوب فيه للغاية، حتى لو احتاج هذا النهج إلى بعض الدعم عبر التهديد بفرض العقوبات.

ومما يبعث على القلق، أنه اعتبارًا من شهر مايو/آيار 2015 لم يجد المتحاورون الذين أجرينا معهم مقابلات من الصينيين في المباحثات الثنائية المباشرة مع الولايات المتحدة بخصوص الأمن الإلكتروني سبيلًا لتحقيق الكثير بخصوص القواعد أو الحدود الخاصة المفروضة على أنشطة الفضاء الإلكتروني. غير أن نهج الصين تجاه قضية الأمن الإلكتروني يبدو في نواحٍ عديدة منصبًا في المقام الأول والأخير على محاولة تحديد وحماية مجموعة من القيم والمقترحات من أجل الحوكمة الدولية للفضاء الإلكتروني والتي من شأنها أن تعيد تعريف الأمن الإلكتروني بعيدًا عن القضايا التي تثير مخاوف الولايات المتحدة، مثل التجسس الإلكتروني ذي الدوافع الاقتصادية وتطبيق قانون النزاع المسلح على الفضاء الإلكتروني. وبإعلان الصين عن مواقفها وتقديمها لمقترحات بشأن الأمن الإلكتروني للأمم المتحدة، فهي تنادي بإعادة تعريف الأمن الإلكتروني وتضع نصب عينيها قضايا مثل السيادة الإلكترونية ونقل إدارة الإنترنت بعيدًا عن أيدي الولايات المتحدة والغرب إلى مكان أكثر ترحيبًا بالصين، مثل الأمم المتحدة.

كان فريقنا يأمل في أن يقدم المحاورون والمشاركون في الحوار من الصينيين مقترحات بشأن التغييرات في سلوك الولايات المتحدة التي من شأنها أن تشكِّل أساسًا لاتفاق بشأن القضايا الهامة، مثل التجسس الإلكتروني ذي الدوافع الاقتصادية أو التجسس الإلكتروني على البنى التحتية الحيوية، لكننا لم نجد إلا عددًا قليلًا من التساؤلات من الجانب الصيني، إن وجدت. وقد يرجع السبب في ذلك إلى الافتقار إلى الخبرة نسبيًا بشأن قضية سياسية معقدة فنيًا، بالإضافة إلى العزوف المفهوم للمشاركين في الحوار عن الخوض في السياسات الرسمية لقضية شائكة. ولم تكن الاقتراحات القليلة التي سمعناها ملحة بالنسبة للمتحاورين بقدر إلحاح المخاوف الأمريكية على المسؤولين الأمريكيين، أو كانت غير مقبولة لأنها تتطلب من المسؤولين الأمريكيين قطع وعود تتنافى مع دستور الولايات المتحدة (وتحديدًا التعديل الأول).

وهكذا يتمثل استنتاجنا الثاني في أن أي اتفاق مع الصين لتحجيم التجسس الإلكتروني ذي الدوافع الاقتصادية مقابل أمر يكون في إمكان واستعداد الولايات المتحدة تقديمه في مجال الفضاء الإلكتروني ليس من المرجح أن يكون واسع النطاق أو فعالًا على وجه التحديد، إلا إذا ارتبط بتعاون أكبر وتجنب للنزاع في العلاقة ككل.

ثم درسنا بعد ذلك إمكانية تحقيق أي تقدم في مفاوضات الأمن الإلكتروني عن طريق إبرام اتفاق يمنع كلًا من الولايات المتحدة والصين من الهجوم على الأخرى. وهنا، توصلنا إلى أرضية مشتركة أوسع؛ إذ عبر المشاركون في الحوار، وكذلك المؤلفات الصينية بشكل أعم، عن استعدادهم للقبول بهذا الاقتراح بشكل عام (رغم تفضيل بعض المشاركين لنهج متعدد الأطراف عن الاتفاق الثنائي). وقد يتحول هذا الاتفاق إلى خطوة مهمة للأمام في شأن التأكيدات المتبادلة وقد يساعد على تعزيز القواعد التي تؤكد على قابلية تطبيق قانون النزاع المسلح على الفضاء الإلكتروني، أو توضحها أو على الأقل تدعمها. وبما أن الصين أعلنت عن اتفاق مع روسيا في مايو/آيار 2015 للكف عن شن الهجمات الإلكترونية على بعضهما البعض، فقد يكون ذلك بمثابة سابقة للارتكاز عليها في المفاوضات مع الصين حول هذه القضية.[2]

وتتمثل إحدى الإضافات المنطقية في أي اتفاق بشأن تجنب استهداف البنية التحتية الحيوية في أن الاتفاق على عدم الهجوم على الأهداف يتضمن أيضًا الاتفاق على عدم التجسس عليها. إذا لم تكن الدولة تسعى إلى ضرب البنية التحتية الحيوية، فلا يكون هناك سبب يدفع حكومة أجنبية لأن تقوم بتجميع معلومات تفصيلية حول مكونات النظام، ومن ثم نقاط ضعفه. بالإضافة إلى ذلك، ونظرًا لصعوبة التمييز بين الدليل على التجسس على هذه الأنظمة والدليل على الاختراقات التي تمهد للهجمات، فإنه ينبغي على جميع الأطراف نبذ التجسس. وهنا أيضًا، وجدنا بعض الأسباب للتوصل إلى اتفاق، رغم أنها تعد التزامات أقل وضوحًا، ربما نظرًا لرفض من حاورناهم من الصينيين التأكيد على أنه دائمًا ما يستطيع ضحايا التجسس الإلكتروني استنتاج، على نحو صحيح ومعقول، أن الاختراقات تشكل استعدادات للهجوم.

وكان آخر الاقتراحات التي عرضناها على المحاورين الصينين هو الأصعب - وهو أن الولايات المتحدة قد تنظر في تبادل الأفكار بشأن الإسناد إذا وافقت الصين على معايير الإثبات المشتركة والتزمت صدقًا بمقاضاة من يثبت انتهاكهم لهذه

---

[2] مقال لكوري بينيت (Cory Bennett) بعنوان "اتحاد روسيا والصين في اتفاق قوي بشأن الفضاء الإلكتروني،" المنشور بذا هيل 8 *The Hill* مايو/آيار 2015.

المعايير. ويتطلب هذا الاتفاق طريقة ما يُتفق عليها بشكل متبادل لتحديد متى قام أحد الأطراف بخرق مسؤولياته في الاتفاق بشكل يجبر الطرف المذنِب على الاعتراف بارتكاب الخطأ. وكما أسلفنا في النقاش، يشير ضعف إمكانيات الإسناد الصيني النسبي حاليًا، بالإضافة إلى المستويات العليا من الريبة الاستراتيجية المتبادلة، إلى أن إجبار كل طرف على قبول الأدلة الظاهرية للطرف الآخر لن يتوج بالنجاح. ويشير ذلك إلى أنه قد يكون من الضروري لإحراز تقدم وضع آلية ثنائية الأطراف أو متعددة الأطراف أو دولية لتسوية النزاع المتعلق بالفضاء الإكتروني، وربما دعمها بجهود الولايات المتحدة لمساعدة الصين على تحسين إمكانياتها الإسنادية.

لن تتحقق هذه الاتفاقية بسهولة؛ إذ إنها تحمل في طياتها مخاطر سياسية ومخاطر محتملة على السياسات ويجوز ألا تنال إعجاب الصين. وفي وجود بيئة تحفها مشكلات الريبة المتبادلة مثل العلاقة الحالية بين الولايات المتحدة والصين، يصعب حشد ما يكفي من الدعم السياسي الأمريكي لهذه الخطوة. وبالنسبة للجانب الصيني، فالعديد من الأطراف الفاعلة في الصين على الأغلب يساورها الشك تجاه أي جهود أمريكية لتشكيل آراء الصين أو إمكانياتها بشأن مجال الفضاء الإلكتروني. غير أن هذا النهج أشبه بفكرة يجدر دراستها بعمق في المباحثات غير الرسمية ويجدر إجراء المزيد من الأبحاث عليها كي نتمكن من تقييم جميع تداعياتها العملية والتكنولوجية والسياسية على نحو أكمل، ولتحديد الأماكن التي يُرجح ظهور مصادر المعارضة الرئيسية منها، وكيف يمكن الحد منها.

إذا تم إبرام هذه الاتفاقية المكونة من ثلاثة أجزاء – بحيث تشمل قاعدة تنص على عدم استهداف أو اختراق البنى التحتية للطرف الآخر – مع عرض بمساعدة الصين على تحسين إمكانياتها الإسنادية في مقابل اتفاق لمتابعة اختراقات الفضاء الإلكتروني الصادرة من الصين (أو الولايات المتحدة) وإجراء التحقيقات بشأنها، بل وحتى إدانتها قضائيًا بشكل فعلي، فقد تغيِّر من طبيعة العلاقات بين الجانبين فيما يتعلق بالفضاء الإلكتروني عبر نطاق مهم من القضايا. وبالتأكيد، ستستمر الدولتان في الاختلاف بشدة بشأن بعض القضايا مثل حرية الوصول إلى المعلومات (الولايات المتحدة) مقابل التحكم في المعلومات والسيادة الإلكترونية (الصين)، وكفاءة وفاعلية تصميم الهيكل الأساسي الدولي الحالي للإنترنت (الولايات المتحدة) مقابل الهيمنة الإلكترونية (الصين)، وما إذا كان سيستمر الجانبان في القيام بالتجسس الإلكتروني لأهداف الأمن القومي، بالإضافة إلى الخلافات بشأن عدة قضايا أخرى في الفضاء الإلكتروني وما سواه. غير أنه إذا أمكن الالتزام بهذا الاتفاق بمصداقية ومتابعته عمليًا،

فإنه سيمثل تحسنًا كبيرًا في العلاقة بين الولايات المتحدة والصين فيما يتعلق بالفضاء الإلكتروني، ولهذا السبب نقول إنه جدير بالنظر وبالمزيد من البحث.

وختامًا، لا تلتقي وجهات نظر الولايات المتحدة والصين فيما يتعلق بالأمن الإلكتروني إلا في نقاط قليلة، وحتى في هذه الحالة، يصعب على الطرفين إحراز التقدم بشأن قضايا مثل عدم استهداف البنى التحتية الحيوية إذا صعب على الطرفين الحفاظ على التقدم المشار إليه في اتفاق قمة سبتمبر/آيلول 2015 بشأن الفضاء الإلكتروني. وعندما يتعلق الأمر بالتوصل إلى اتفاق شامل ومجدٍ ودائم بشأن قواعد الأهداف المشروعة في الفضاء الإلكتروني، لا يزال هناك الكثير من العمل لإنجازه، ولا يتضح إن كان التوصل إلى تلك النتيجة ممكنًا. وربما تتمثل أكثر المجالات الواعدة التي قد نرى فيها بعض احتمالات التفاوض على مجموعة من القواعد في السنوات المقبلة في تجنب استهداف البنى التحتية الحيوية أو التجسس عليها. ويجوز دعم ذلك بالجهود الرامية لوضع معايير إثبات مشتركة، وتحديد كيفية تحقيق الإسناد، وإدانة مرتكبي هذه الأعمال قضائيًا.

غير أنه لن يكون من السهل التفاوض بشأن أي اتفاقات مجدية عن الفضاء الإلكتروني. فإن توجهات الرأي في العلاقة الثنائية بين الولايات المتحدة والصين، وكذلك داخل المجتمع الصيني عمومًا ليست مبشرة حاليًا. ورغم أن استعداد الصين للتفاوض حول هذه القضايا قد يتغير في المستقبل تغييرًا جذريًا إذا قامت الدولة بتأسيس قضاء محلي أكثر فعالية يؤيد حماية حقوق الملكية الفكرية ونظام قانوني أكثر استقلالية ومهنية، إلا أنه يصعب رؤية مؤشرات هذا التطور في الوقت الحالي. وفي ظل الواقع الحالي في الصين، حيث يعين الحزب الشيوعي الصيني جميع قضاة المحاكم، ويُطلب من المحامين الجدد قسم الولاء للحزب الشيوعي،[3] وحيث يتعرض المحامون الحقوقيون [*weiquan* *lushi*] للاعتقالات الجماعية[4]، تبدو آفاق أي اتفاق شامل ومجدٍ ودائم ضئيلة في الأجل القريب إلى المتوسط. وإذا قررت كل من الصين والولايات المتحدة أنهما ترغبان في التفاوض معًا بشأن قواعد السلوكيات الخاصة بالفضاء الإلكتروني في المستقبل، فقد توفر نتائج الأبحاث الواردة أعلاه بعض الرؤى في كيفية تنفيذ ذلك.

---

[3] مقال لسوي لي وي (Sui-Lee Wee) بعنوان "الصين تأمر المحامين بحلف يمين الولاء للحزب الشيوعي،" المنشور بشبكة رويترز Reuters 21 مارس/آذار 2012.

[4] مقال لكريس باكلي (Chris Buckley) بعنوان "السلطات الصينية تعتقل وتدين محامي حقوق إنسان،" المنشور بنيويورك تايمز *New York Times* 11 يوليو/تموز 2015؛ ومقال ناش جينكينز (Nash Jenkins) بعنوان "الصين اعتقلت أكثر من 100 محامي وناشط حقوق إنسان في العطلة الأسبوعية الماضية،" المنشور بمجلة التايم *Time* 12 يوليو/تموز 2015.

الحاشية

في 25 سبتمبر/أيلول 2015، حين كان هذا التقرير قيد الإعداد والنشر النهائي، حضر الرئيس الصيني شي للولايات المتحدة في زيارة رسمية. أثناء رحلته، أعلن كل من شي والرئيس الأمريكي أوباما ما يلي

> اتفقت الولايات المتحدة والصين على ألا تقوم حكومة أي من البلدين بسرقة الملكية الفكرية باستخدام الفضاء الإلكتروني أو دعمها عن علم، بما في ذلك الأسرار التجارية أو أي معلومات تجارية سرية، بقصد الحصول على ميزة تنافسية للشركات أو القطاعات التجارية.

كما اتفق الطرفان على الآتي

> التعاون .....مع طلب التحقيق في الجرائم الإلكترونية ..... (بذل) جهود مشتركة لوضع أساليب ملائمة لسلوك الدولة في الفضاء الإلكتروني وتطويرها... (و) تأسيس آلية حوار مشترك على مستوى عال في محاربة الجريمة الإلكترونية والقضايا ذات الصلة.[1]

ولهذا، وبعد فترة قصيرة نسبيًا من المفاوضات التي عُقدت قبل القمة، ألزم الرئيس الصيني دولته بالاعتراف والالتزام بقواعد التجسس الإلكتروني التي تشجب أغلب سلوكيات الصين التي تعترض عليها الولايات المتحدة مع عدم وضع قيود جديدة

[1] البيت الأبيض، "صحيفة الوقائع": جاءت زيارة الرئيس شي جين بينغ (Xi Jinping) الرسمية للولايات المتحدة "واشنطن" في 25 سبتمبر/أيلول 2015

على أنواع السلوك الإلكتروني التي تعتبره الولايات المتحدة سلوكًا شرعيًا.[2] جاءت هذه الاتفاقية، بأقل تقدير، لتكون نقلة فارقة لتعاملات الصين والولايات المتحدة حول قضايا الفضاء الإلكتروني. إضافة إلى ذلك، وباستعادة الأحداث الماضية، نجد مؤشرات على أن هذه النتيجة لم تكن خارج نطاق الاحتمال (بسبب عدم قيام أي من المحاورين المشاركين معنا بالدفاع عن التجسس الإلكتروني ذي الدوافع الاقتصادية، على سبيل المثال)، بل كانت النتيجة غير متوقعة إلى حد بعيد، ولم يكن أمرًا تنبأ به أي محلل جاد من جانب أي من الطرفين قبل انعقاد القمة على حد علمنا.

ماذا تعني هذه الاتفاقية، ولماذا وقعت الصين عليها؟ على الرغم من أن توضيح الحقائق سيظهر بعد تحرير هذا التقرير وأن قضية العلاقات بين الولايات المتحدة والصين ستستمر في التطور، نقدم بعض التفسيرات المحتملة رغم ذلك. يجوز الجمع بين جميع هذه التفسيرات، ويجوز أن يكون كل تفسير قد لعب دورًا، ولذا نطلق عليها نتائج وتفسيرات مستقبلية محتملة ما دامت غير واضحة حتى الآن:

- لن تؤدي الاتفاقية لتغيير جذري. ربما تستكمل الصين التجسس الإلكتروني ذا الدوافع الاقتصادية.[3] حتى وإن تمكنت الولايات المتحدة من كشف وإسناد عمليات الاختراق، قد تستمر الحكومة الصينية في إنكار تواطؤها (أو ستصرح بأن "الصين دولة كبيرة، ولا يمكننا أن نعرف كل شيء تدعون أنه حدث لدينا"). لم يتم إنشاء أي نظام رقابي وافق الطرفان على قبول نتائجه (ولم يكن هناك حديث عن كيفية تأسيس نظام). لم تتعرض الحكومة الصينية للإحراج بتوقيع هذه الاتفاقية لأنها لم تصرح رسميًا قط عن أن التجسس الإلكتروني ذا الدوافع الاقتصادية ليس أسوأ من التجسس الإلكتروني الذي يهدد الأمن القومي، كما أنها لم تعترف بالمشاركة في التجسس الإلكتروني ذي الدوافع الاقتصادية (ومن هنا يأتي التلميح بأن الاتفاقية لن تغير أي شيء من قيام الصين بالتجسس الإلكتروني ذي الدوافع الاقتصادية في السابق). وبالفعل، ندد الرئيس الصيني شي بالتجسس الإلكتروني ذي الدوافع الاقتصادية بينما كان في سياتل قبل الإعلان على الاتفاقية.

---

[2] على سبيل المثال، لاحظ أن التجسس التجاري – التي لم تقر الولايات المتحدة بارتكابه حتى 2013 – يعتبر مسموحًا به، طالما لا يتم إعطاء النتائج للشركات التجارية.

[3] ألمحت الشواهد المبكرة إلى محاولات الاختراق المتواصلة بعد انتهاء القمة بأن تجسس الصين الإلكتروني ذي الدوافع الاقتصادية لم يتوقف مباشرة، انظر بول موزور (Paul Mozur) "تقول إحدى شركات الأمن الإلكتروني أن القراصنة الصينيين يستمرون في مهاجمة الشركات الأمريكية"، نيويورك تايمز *New York Times*، 20 أكتوبر/تشرين الأول 2015.

- تؤدي هذه الاتفاقية إلى تغيير ملموس، وانعقدت تحت الضغط. يرجح ممارسة نوعين من الضغط. النوع الأول كان تهديد الولايات المتحدة بفرض عقوبات، وربما هو ما جعل الصين تتخلى عن أفعالها. رغم أن حجم الاقتصاد الصيني يساوي ثلثي حجم الاقتصاد الأمريكي، إلا أن الصين شعرت بأنها قد تكون معرضة للخطر نظرًا للتوجهات الاقتصادية الأخيرة غير المواتية. الاقتصاد الصيني متذبذب (حيث انخفض مؤشر سوق الأوراق المالية بشدة في الصين في صيف 2015 على الرغم من محاولات إنعاشه)؛ إذ يفتقر إلى العدد الكبير من الحلفاء الذين تحظى بهم الولايات المتحدة والذين قد يساعدوها في جهودها في مواجهة الأزمات، كما أن جيش الصين لا يزال أقل منها قوة، وكذلك تخشى الصين من هيمنة الولايات المتحدة على الفضاء الإلكتروني، وتفتقر إلى القوة الناعمة التي تتميز الولايات المتحدة بها. ولأن الاقتصاد الصيني يعتمد على التصدير للولايات المتحدة أكثر من استيراده منها، فقد تخسر الصين الكثير في الحرب التجارية الشاملة مع الولايات المتحدة. وأخيرًا، بدت الولايات المتحدة مستعدة لاتخاذ مخاطر تصعيدية ضد التجسس الإلكتروني الصيني، عندما ازداد الأمر سوءًا باختراق مكتب إدارة شؤون الموظفين. فإذا كان استعداد الصين للتوصل إلى اتفاقية حول قواعد الاستهداف في الفضاء الإلكتروني يعكس تقييمها لعلاقات القوى، قد تكون هذه الاتفاقية فعالة ومستمرة لفترة طويلة. لربما ظهر النوع الثاني من الضغط بسبب استنتاج القيادة الصينية أن أنشطة الصين في الفضاء الإلكتروني تتسبب في مخاطر كبيرة غير مقبولة على العلاقات بين الولايات المتحدة والصين وسعت إلى تهدئة التوترات في هذا المجال من أجل تجنب احتمالية المنافسة والمواجهة الاستراتيجية العارمة بين الولايات المتحدة والصين.[4]
- كانت الصين على استعداد للتنازل لأن قيمة التجسس الإلكتروني ذي الدوافع الاقتصادية بالنسبة لها كانت مخيبة للآمال *(أو في تدنٍّ)*. ربما لم تعد الصين تحصد الكثير من المزايا من سرقة حقوق الملكية الفكرية (أي أنه لكي تكون أحد الطهاة المشهورين عالميًا سيتطلب الأمر ما هو أكثر من سرقة كتاب جيد

[4] يعكس هذا التعليق رأيًا سعت الفقرة السابقة إلى إرسائه، وهو أن قادة الصين يقدرون قيمة الاستقرار في العلاقة الكلية مع الولايات المتحدة. فإذا تم النظر إلى الفضاء الإلكتروني على أنه يعرِّض هذه العلاقة للخطر، قد تغير القيادة رأيها في قيمة الفضاء الإلكتروني المطلق إن كان سيتسبب ذلك في فرض تكاليف تعرِّض الاستقرار الجغرافي والاستراتيجي الأعم للخطر.

عن الطهي). فمثلًا، أظهرت صحيفة الدعوى المتعلقة بإدانة ضباط جيش التحرير الصيني الخمسة نسبة ضئيلة من سرقة الملكية الفكرية مقارنةً بالاستيلاء على بيانات ملكية الأعمال.[5] عند التفاوض، ينبغي أن تتنازل عن أمر يهتم به الطرف الآخر أكثر منك كوسيلة لإقناعه بالتنازل عن أمور تهمك حقًا. ومن ثم، تنازلت الصين عن هذه القضية كي تتمكن من التمسك بما تريده في القضايا الأخرى.[6] ومع ملاحظة ذلك، ليس ثمة دليل أن الولايات المتحدة قد قدمت أي تنازلات تعويضية من جانبها منذ القمة.

- وأخيرًا، أرادت الصين كبح جماح القراصنة المستقلين التابعين لها، وأدى هذا الاتفاق إلى إعطاء بكين المزيد من الصلاحية للقيام بذلك (تمامًا مثلما منح الاتفاق بشأن المناخ الصادر في ديسمبر/كانون أول 2014 بكين المزيد من الصلاحية للضغط على الحكومات الإقليمية والمحلية للتصرف بجديه تجاه قضية التلوث). قد تخشى القيادة الصينية من أن يقوم القراصنة غير المقيدين أو الذين يعملون في الخفاء بتهديد النظام القائم في الصين بشكل عام. وقد تخشى من تحول نظر القراصنة من الشركات الأجنبية إلى الشركات الصينية، وربما تثني الشركات الصينية عن الاستثمار في تطوير منتجاتها. وما هو أسوأ، من وجهة نظر بكين، هو أنهم قد يوجهون مهاراتهم في الاختراق ضد الحكومة المركزية. قد يستغل المسؤولون الصينيون هذه الاتفاقية لإضفاء الصبغة المهنية على مجتمع القراصنة لديها. ربما شعروا بالحرج بعد أن شبههم مدير مكتب التحقيقات الفيدرالي باللصوص الثمالى وكانوا بالتأكيد في قمة الحرج بسبب المقالة المنشورة في صحيفة وول ستريت جورنال *Wall Street Journal* والتي كشفت عن علاقة بين الجيش الصيني والاختراقات، ونُشرت قبل يومين من زيارة الرئيس الصيني شي إلى البيت الأبيض.[7]

---

[5] وزارة العدل، مكتب الشؤون العامة، "اتهمت الولايات المتحدة خمسة قراصنة عسكريين صينيين بالتجسس الإلكتروني ضد شركات أمريكية ومنظمة تابعة لوزارة العمل من أجل الحصول على ميزة تفوق تجاري"، واشنطن، 19 مايو/آيار 2014.

[6] بحث جاك جولدسميث (Jack Goldsmith) فيما إن كانت الولايات المتحدة قد وافقت على الكف عن تقويض جدار الصين الناري العظيم. انظر جاك جولدسميث، "ما هي أسباب اتفاقية الفضاء الإلكتروني بين الولايات المتحدة والصين؟" *Lawfare blog*، 26 سبتمبر/أيلول 2015.

[7] جوش شين (Josh chin)، "أحد قراصنة التجسس الإلكتروني التابع للجيش الصيني"، صحيفة *Wall Street Journal*، 23 سبتمبر/أيلول 2015.

يبدو أن قادة الصين يعتقدون (إذا دلت المناقشات التي جرت عقب القمة مع عدد قليل من المحاورين الصينين على شيء) أن هذه الاتفاقية تسمح للصين بتنفس الصعداء بعيدًا عن تهديدات الولايات المتحدة بفرض عقوبات اقتصادية. وقد يذهبون إلى أن الولايات المتحدة لا تستطيع الادعاء بأن الصين لم تحافظ على وعدها إلى أن تجد أن عملًا من أعمال التجسس الإلكتروني ذي الدوافع الاقتصادية المرفوضة قد بدأ بعد إبرام الاتفاقية. ومن ثم، فإن الحديث المتواصل عن العقوبات أو أي شكل من أشكال الضغط يحمل سوء نية. لكن لا يتضح ما إذا كانت التوقعات قد تحققت في المستقبل. شهدت الأسابيع اللاحقة أنباءً عن شركات صينية بعينها تتعرض للعقوبات ووردت تقارير بأن الصين ألقت القبض على مواطنيها باتهامات التجسس الإلكتروني ذي الدوافع الاقتصادية، في ظل الضغط الأمريكي.[8] واعتبارًا من فبراير/شباط 2016، بدأ يتضح التفسير والمعنى النهائي للاتفاقية الموقعة بين الولايات المتحدة والصين بشأن الفضاء الإلكتروني.[9]

---

[8] مقال للكتاب هانا كوشلير (Hannah Kuchler) وجيف داير (Geoff Dyer) وجينا شون (Gina Chon) ولوسي هورنبي (Lucy Hornby) ودميتري سافاستوبولو (Demetri Savastopulo) بعنوان "الولايات المتحدة تستهدف مقرصنين أمريكيين في خلاف بشأن الفضاء الإلكتروني،" المنشورة بالفاينانشال تايمز *Financial Times*، 7 أكتوبر/تشرين الأول 2015، ص 1؛ ومقال إلين ناكاشيما (Ellen Nakashima) وآدم غودمان (Adam Goldman) بعنوان "في سابقة من نوعها، اعتقال مقرصنين صينيين بأمر من الحكومة الأمريكية،" المنشور في واشنطن بوست *Washington Post* 9 أكتوبر/تشرين الأول 2015. واعتبارًا من 12 أكتوبر/تشرين الأول 2015، كان ينبغي تأكيد هذا التقرير بتقرير مماثل له في صحيفة *New York Times*

[9] ظهرت تقارير في خريف 2015 ورد فيها رأي بعض المراقبين أن الجيش الصيني حد من مشاركته في التجسس الإلكتروني ذي الدوافع الاقتصادية، إذ يبدو أن وزارة الأمن الوطني الصينية تولت السيطرة على هذه القضية إلى حد أكبر من ذي قبل، غير أن ثمة مراقبين آخرين يرون استمرار المعدل العالي لسرقة حقوق الملكية الفكرية بسبب أفعال أطراف غير حكومية داخل الصين. انظر على سبيل المثال، شانون تيزي Shannon Tiezzi، "بدء محادثات جديدة عالية المستوى بين كل من الولايات المتحدة والصين بشأن الفضاء الإلكتروني، *The Diplomat*، 2 ديسمبر/كانون الأول 2015.

المراجع

"Admit Nothing and Deny Everything," *The Economist*, June 8, 2013. As of December 2, 2015: http://www.economist.com/news/china/21579044-barack-obama-says-he-ready-talk-xi-jinping-about-chinese-cyber-attacks-makes-one

Alperovich, Dmitri, *Revealed: Operation Shady RAT*, white paper, Santa Clara, Calif.: McAfee, August 3, 2011. As of December 2, 2015: http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

"An International Code of Conduct for Information Security—China's Perspective on Building a Peaceful, Secure, Open and Cooperative Cyberspace," statement prepared for a conference in Geneva hosted by the UN Institute for Disarmament Research, February 10, 2014. As of November 30, 2015: http://www.unidir.ch/files/conferences/pdfs/a-cyber-code-of-conduct-the-best-vehicle-for-progress-en-1-963.pdf

Austin, Greg, "No Easy Solutions in US-China Cyber Security," *East Asia Forum*, October 6, 2015. As of December 1, 2015: http://www.eastasiaforum.org/2015/10/06/no-easy-solutions-in-us-china-cyber-security

Axelrod, Robert, *The Evolution of Cooperation*, New York: BasicBooks, 1984.

Bhattacharjee, Yudhijit, "A New Kind of Spy: How China Obtains American Technological Secrets," *New Yorker*, May 5, 2014. As of December 2, 2015: http://www.newyorker.com/magazine/2014/05/05/a-new-kind-of-spy

Beech, Eric, and Ben Blanchard, "U.S., Chinese Officials Meet on Cyber Security Issues: White House," Reuters, September 12, 2015. As of December 1, 2015: http://www.reuters.com/article/2015/09/13/us-usa-china-cybersecurity-idUSKCN0RC0S420150913

Bennett, Cory, "Russia, China Unite with Major Cyber Pact," *The Hill*, May 8, 2015. As of December 2, 2015: http://thehill.com/policy/cybersecurity/241453-russia-china-unit-with-major-cyber-pact

Blackwill, Robert D., and Ashley J. Tellis, *Revising U.S. Grand Strategy Toward China*, Washington, D.C.: Council on Foreign Relations, Council Special Report No. 72, May 2015. As of November 30, 2015: http://carnegieendowment.org/files/Tellis_Blackwill.pdf

Bodeen, Christopher, "U.S. Says Hacking Undermines China's Interests," *Pioneer Press*, April 9, 2013. As of December 2, 2015: http://www.twincities.com/ci_22984979/us-says-hacking-undermines-chinas-interests

Braun, Stephen, "Official Says Hackers Hit Up to 25,000 Homeland Security Employees," *Washington Post*, August 23, 2014. As of November 30, 2015: https://www.washingtonpost.com/business/economy/official-says-hackers-hit-up-to-25000-homeland-security-employees/2014/08/22/a855b6c0-2a52-11e4-958c-268a320a60ce_story.html

Buckley, Chris, "China Takes Aim at Western Ideas," *New York Times*, August 19, 2013. As of December 1, 2015: http://www.nytimes.com/2013/08/20/world/asia/chinas-new-leadership-takes-hard-line-in-secret-memo.html

———, "Chinese Authorities Detain and Denounce Rights Lawyers," *New York Times*, July 11, 2015. As of December 2, 2015: http://www.nytimes.com/2015/07/12/world/asia/china-arrests-human-rights-lawyers-zhou-shifeng.html

"Canada National Research Council 'Hacked by Chinese Spies,'" BBC, July 29, 2014.

Carr, Jeffrey, "Cyber Attacks: Why Retaliating Against China Is the Wrong Reaction," *The Diplomat*, August 6, 2015. As of December 1, 2015: http://thediplomat.com/2015/08/cyber-attacks-why-retaliating-against-china-is-the-wrong-reaction

Center for Strategic and International Studies, *The Economic Impact of Cybercrime and Cyber Espionage*, July 2013. As of November 30, 2015: http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime.pdf

———,"Significant Cyber Incidents since 2006," March 10, 2014. As of December 2, 2015: http://csis.org/files/publication/140310_Significant_Cyber_Incidents_Since_2006.pdf

Chang, Amy, *Warring State: China's Cybersecurity Strategy*, Washington, D.C.: Center for a New American Security, December 2015, pp. 7, 10. As of November 30, 2015: http://www.cnas.org/sites/default/files/publications-pdf/CNAS_WarringState_Chang_report_010615.pdf

Chen, Te-Ping, "Snowden Alleges U.S. Hacking in China," *Wall Street Journal*, June 23, 2013. As of December 2, 2015: http://www.wsj.com/articles/SB10001424127887324577904578562483284884530

Chen Weihua and Li Xiaokun, "China Demands Charges Be Dropped," *China Daily*, May 22, 2014. As of November 30, 2015: http://usa.chinadaily.com.cn/epaper/2014-05/22/content_17533404.htm

Cheng, Dean, "Chinese Views on Deterrence," *Joint Forces Quarterly*, No. 60, spring 2011, pp. 92–94.

Chin, Josh, "Cyber Sleuths Track Hacker to China's Military," *Wall Street Journal*, September 23, 2015. As of December 2, 2015: http://www.wsj.com/articles/cyber-sleuths-track-hacker-to-chinas-military-1443042030

"China Behind Cyberattack on US Sites, Report Says," *San Francisco Chronicle*, May 8, 2015. As of December 1, 2015: http://www.sfgate.com/news/article/China-behind-cyberattack-on-U-S-sites-report-6252140.php

"China Hackers Defect to Other Side, Become Cyber Gatekeepers," *Japan Times*, June 30, 2015. As of December 2, 2015: http://www.japantimes.co.jp/news/2015/06/30/asia-pacific/china-hackers-defect-side-become-cyber-gatekeepers/#.Vl-dm2SDFBc

"China's Head of Cyberspace Discusses How to Build Mutual Trust with U.S.," *GW Today*, December 3, 2014. As of December 1, 2015: http://gwtoday.gwu.edu/china%E2%80%99s-head-cyberspace-discusses-how-build-mutual-trust-us

"China Voice: Drop Cold War Mentality on China's Cybersecurity," Xinhua, April 22, 2014. As of December 2, 2015: http://english.cntv.cn/2014/04/22/ARTI1398148113852301.shtml

Cho, Meeyoung, "Low-Risk 'Worm' Removed at Hacked South Korea Nuclear Operator," Reuters, December 30, 2014. As of December 1, 2015: http://www.reuters.com/article/2014/12/30/nuclear-southkorea-cybersecurity-idUSL3N0UE1A320141230

Chung, Jae Ho, "China's Evolving Views of the Korean-American Alliance, 1953–2012," *Journal of Contemporary China*, Vol. 23, No. 87, 2014, pp. 425–442.

Claburn, Thomas, "Chinese Hackers Angered by Microsoft's Epic Fail," *Information Week*, October 23, 2008. As of December 2, 2015: http://www.informationweek.com/software/operating-systems/chinese-hackers-angered-by-microsofts-epic-fail/d/d-id/1073270?

Clapper, James R., "Statement of Record: Worldwide Threat Assessment of the U.S. Intelligence Community," Washington, D.C.: Director of National Intelligence, February 26, 2015. As of December 2, 2015: http://www.dni.gov/files/documents/Unclassified_2015_ATA_SFR_-_SASC_FINAL.pdf

Clayton, Mark, "Exclusive: Cyberattack Leaves Natural Gas Pipelines Vulnerable to Sabotage," *Christian Science Monitor*, February 27, 2013. As of December 2, 2015: http://www.csmonitor.com/Environment/2013/0227/Exclusive-Cyberattack-leaves-natural-gas-pipelines-vulnerable-to-sabotage

CSIS—*See* Center for Strategic and International Studies.

Culpan, Tim, "Decade-Long Cyberspy Attack Hacked Southeast Asian Targets," Bloomberg, April 12, 2015. As of December 2, 2015: http://www.bloomberg.com/news/articles/2015-04-12/decade-long-cyber-spying-campaign-hacked-southeast-asia-targets

Deeks, Ashley, "Tallinn 2.0 and a Chinese View of the Tallinn Process," *Lawfare blog*, May 31, 2015. As of November 30, 2015: https://www.lawfareblog.com/tallinn-20-and-chinese-view-tallinn-process

Dilanian, Ken, "NSA Director: China Can Damage U.S. Power Grid," Associated Press, November 20, 2014. As of November 30, 2015: http://www.salon.com/2014/11/20/nsa_director_china_can_damage_us_power_grid

Dong Qingling, "Confidence-Building for Cybersecurity Between China and the United States," *China International Studies*, July/August 2014, pp. 57–68. As of November 30, 2015: http://www.ciis.org.cn/english/2014-09/23/content_7254470.htm

"The Dragon's New Teeth," *The Economist*, April 7, 2012. As of December 1, 2015: http://www.economist.com/node/21552193

"Espionage Report: Merkel's China Visit Marred by Hacking Allegations," *Spiegel* online, August 27, 2007. As of December 2, 2015: http://www.spiegel.de/international/world/espionage-report-merkel-s-china-visit-marred-by-hacking-allegations-a-502169.html

Fletcher, Owen, "China Game Boss Sniped Rivals, Took Down Internet," *PC World*, August 29, 2009. As of December 2, 2015: http://www.pcworld.com/article/171018/article.html

Fisher, Roger, William Ury, and Bruce Patton, *Getting to Yes: Negotiating Agreement Without Giving In*, London: Penguin Publishing, 1981.

Frizell, Sam, "NSA Director on Sony Hack: 'The Entire World Is Watching,'" *Time*, January 8, 2015. As of December 1, 2015: http://time.com/3660757/nsa-michael-rogers-sony-hack

Gantz, John F., Joe Howard, Richard Lee, Harish N. Taori, Ricardo Villate, Christian A. Christiansen, Albert Wang, Christian Lachawitz, Thomas Vavra, Rich Rodolfo, Attaphon Satidkanitkul, Ravikant Sharma, Alejandro Florean, Stephen Minton, and Marcel Warmerdam, *The Dangerous World of Counterfeit and Pirated Software: How Pirated Software Can Compromise the Cybersecurity of Consumers, Enterprises, and Nations . . . and the Resultant Costs in Time and Money,* Framingham, Mass.: International Data Corporation, 2013. As of December 2, 2015: http://news.microsoft.com/download/presskits/antipiracy/docs/IDC030513.pdf

Gaouette, Nicole, and Brendan Greeley, "U.S. Funds Help Democracy Activists Evade Internet Crackdowns," Bloomberg, April 20, 2011. As of December 2, 2015: http://www.bloomberg.com/news/articles/2011-04-20/u-s-funds-help-democracy-activists-evade-internet-crackdowns

Garamone, Jim, "Cybercom Chief Details Cyberspace Defense," American Forces Press Service, September 23, 2010. As of February 12, 2016: http://archive.defense.gov/news/newsarticle.aspx?id=60987

"German Government and Companies Attacked by Chinese Hackers," *Want China Times*, February 26, 2013.

Godwin, Paul H. B., and Alice L. Miller, *China's Forbearance Has Limits: Chinese Threat and Retaliation Signaling and Its Implications for a Sino-American Military Confrontation*, Washington, D.C.: National Defense University Press, April 2013. As of December 2, 2015: http://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/ChinaPerspectives-6.pdf

Goldsmith, Jack, "What Explains the U.S.-China Cyber 'Agreement?'" *Lawfare blog*, September 26, 2015. As of December 2, 2015: https://www.lawfareblog.com/what-explains-us-china-cyber-agreement

Goldstein, Lyle J., "How China Sees America's Moves in Asia: Worse than Containment," *National Interest*, October 29, 2014. As of November 30, 2015: http://nationalinterest.org/feature/how-china-sees-americas-moves-asia-worse-containment-11560

———, *Meeting China Halfway*, Washington, D.C.: Georgetown University Press, 2015.

Gorman, Siobhan, and Julian E. Barnes, "Cyber Combat: Act of War," *Wall Street Journal*, May 31, 2011. As of December 2, 2015: http://www.wsj.com/articles/SB10001424052702304563104576355623135782718

Gorman, Siobhan, August Cole, and Yochi Dreazen, "Computer Spies Breach Fighter-Jet Project," *Wall Street Journal*, April 21, 2009. As of December 2, 2015: http://www.wsj.com/articles/SB124027491029837401

Grigsby, Alex, "The UN GGE on Cybersecurity: What is the UN's Role?" Council on Foreign Relations *(Net Politics blog)*, April 15, 2015. As of December 2, 2015: http://blogs.cfr.org/cyber/2015/04/15/the-un-gge-on-cybersecurity-what-is-the-uns-role/

Gullo, Karen, "California Man Guilty of Stealing DuPont Trade Secrets," *Bloomberg Business*, March 5, 2014. As of December 2, 2015: http://www.bloomberg.com/news/articles/2014-03-05/california-man-guilty-of-stealing-dupont-trade-secrets

Guo Ji, "Cyber Should Not Become a New Tool of American Hegemony: Starting from an Explanation of the 'PRISM-gate' Incident [Wangluo buying chengwei Meiguo baquan xi gongju: Cong 'Lingjingmen' shijian shuokai qu]," *Seeking Truth* [*Qiu Shi*], No. 15, 2013, pp. 57–59.

Ikenberry, G. John, *After Victory: Institutions, Strategic Restraint, and the Rebuilding of Order After Major Wars*, Princeton, N.J.: Princeton University Press, 2000.

Inkster, Nigel, "Chinese Intelligence in the Cyber Age," *Survival*, Vol. 55, No. 1, February–March 2013, pp. 45–66.

Jackson, David, "Obama, China's Xi to Hold Tense Meetings on Cybersecurity, Military," *USA Today*, September 21, 2015. As of December 1, 2015: http://www.usatoday.com/story/news/2015/09/21/obama-china-xi-jinping-white-house-meeting-cybersecurity/72519380

Jenkins, Nash "China Arrested More than 100 Human-Rights Lawyers and Activists over the Weekend," *Time*, July 12, 2015. As of December 2, 2015: http://time.com/3954935/china-arrests-lawyers-human-rights

Jiang Chong, "Cyber: The Invisible New Battlefront [*Wangluo: Kanbujian de xin zhanxian*]," *Seeking Truth* [*Qiu Shi*], No. 13, 2010, pp. 53–55.

Jiang Li, Zhang Xiaolan, and Xu Feibiao, "The International Cybersecurity Dilemma and a Way Out [uoji wangluo anquan hezuo de kunjing yu chulu]," *Contemporary International Relations* [*Xiandai guoji guanxi*], No. 9, 2013, pp. 52–58.

Kang, Cecilia, "Hillary Clinton Calls for Web Freedom, Demands China Investigate Google Attack," *Washington Post*, January 22, 2010. As of February 12, 2016: http://www.washingtonpost.com/wp-dyn/content/article/2010/01/21/AR2010012101699.html

Kravets, David, "FBI Director Says Chinese Hackers Are Like a 'Drunk Burglar,'" *Ars Technica*, October 6, 2014. As of December 2, 2015: http://arstechnica.com/tech-policy/2014/10/fbi-director-says-chinese-hackers-are-like-a-drunk-burglar

Krebs, Brian, "Chinese Hackers Blamed for Intrusion at Energy Industry Giant Telvent," *Krebs on Security*, September 12, 2012. As of December 2, 2015: http://krebsonsecurity.com/2012/09/chinese-hackers-blamed-for-intrusion-at-energy-industry-giant-telvent/

Krekel, Brian, George Bakos, and Christopher Barnett, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation*, Washington, D.C.: The U.S.-China Economic and Security Review Commission, 2009. As of December 2, 2015: http://nsarchive.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-030.pdf

Kuchler, Hannah, Geoff Dyer, Gina Chon, Lucy Hornby, and Demetri Savastopulo, "U.S. Targets Chinese Groups in Cyber Feud," *Financial Times*, October 7, 2015, p. 1. As of December 2, 2015: http://www.ft.com/intl/cms/s/0/4ba9e99a-6d0f-11e5-aca9-d87542bf8673.html

Lagorio, Christine, "State Department Computers Hacked," CBS News, July 11, 2006. As of December 2, 2015: http://www.cbsnews.com/news/state-department-computers-hacked

Lam, Lana, "NSA Targeted China's Tsinghua University in Extensive Hacking Attacks, Says Snowden," *South China Morning Post*, June 22, 2013. As of December 2, 2015: http://www.scmp.com/news/china/article/1266892/exclusive-nsa-targeted-chinas-tsinghua-university-extensive-hacking?page=all

Lampton, David M. "A Tipping Point in US-China Relations Is Upon Us," *US-China Perception Monitor*, May 11, 2015. As of November 30, 2015: http://www.uscnpm.org/blog/2015/05/11/a-tipping-point-in-u-s-china-relations-is-upon-us-part-i

Landler, Mark, and David E. Sanger, "U.S. Demands China Block Cyberattacks and Agree to Rules," *New York Times*, March 12, 2013. As of December 2, 2015: http://www.nytimes.com/2013/03/12/world/asia/us-demands-that-china-end-hacking-and-set-cyber-rules.html

Lieberthal, Kenneth, and Wang Jisi, *Addressing U.S.-China Strategic Distrust*, Washington, D.C.: The John L. Thornton China Center, Brookings Institution, 2012. As of November 30, 2015: http://www.brookings.edu/~/media/research/files/papers/2012/3/30-us-china-lieberthal/0330_china_lieberthal.pdf

Lieberthal, Kenneth, and Peter W. Singer, *Cybersecurity and U.S.-China Relations*, Washington, D.C.: 21st Century Defense Initiative, The John L. Thornton China Center, Brookings Institution, February 2012. As of November 30, 2015: http://www.brookings.edu/~/media/Research/Files/Papers/2012/2/23%20cybersecurity%20china%20us%20singer%20lieberthal/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.PDF

Lindsay, Jon R., Tai Ming Cheung, and Derek Reveron, *China and Cybersecurity: Espionage , Strategy, and Politics in the Digital Domain*, Oxford: Oxford University Press, 2015.

"Look Who's Listening," *Economist*, June 15, 2013. As of December 2, 2015: http://www.economist.com/news/briefing/21579473-americas-national-security-agency-collects-more-information-most-people-thought-will

Lu Chuanying, "An Attempt to Analyze the Current Global Governance Dilemma in Cyberspace [Shixi dangqian wangluo kongjian quanqiu zhili kunjing]," *Contemporary International Relations* [*Xiandai guoji guanxi*], No. 11, 2013, pp. 48–54.

Ma Xinming, "What Kind of Internet Order Do We Need?" *Chinese Journal of International Law*, Vol. 14, No. 2, 2015, pp. 399–403. As of November 30, 2015: http://chinesejil.oxfordjournals.org/content/14/2/399.short

Mandiant, *APT1: Exposing One of China's Cyber Espionage Units*, March 2013. As of December 1, 2015: http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

Markoff, John, and David Barboza, "Researchers Trace Data Theft to Intruders in China,"*New York Times*, April 5, 2010. As of December 2, 2015: http://www.nytimes.com/2010/04/06/science/06cyber.html

Mastro, Oriana Skylar, "Why Chinese Assertiveness Is Here to Stay," *Washington Quarterly*, Vol. 37, No. 4, winter 2015, pp. 151–170.

McAfee Foundstone Professional Services and McAfee Labs, *Global Energy Cyberattacks: "Night Dragon,"* white paper, Santa Clara, Calif.: McAfee, February 10, 2011. As of December 2, 2015: http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf

McReynolds, Joe, "Chinese Thinking on Cyber Deterrence," in Philip C. Saunders and Andrew Scobell, eds., *PLA Influence on Chinese National Security Policymaking*, Stanford, Calif.: Stanford University Press, 2015.

Miller, Joe, "Israeli Iron Dome Firms 'Infiltrated by Chinese Hackers,'" BBC, July 31, 2014. As of December 2, 2015: http://www.bbc.com/news/technology-28583283

Mozur, Paul, "Cybersecurity Firm Says Chinese Hackers Keep Attacking U.S. Companies," *New York Times*, October 20, 2015. As of December 21, 2015: http://www.nytimes.com/2015/10/20/technology/cybersecurity-firm-says-chinese-hackers-keep-attacking-us-companies.html

———, "New Rules in China Upset Western Tech Companies," *New York Times*, January 29, 2015. As of November 30, 2015: http://www.nytimes.com/2015/01/29/technology/in-china-new-cybersecurity-rules-perturb-western-tech-companies.html

Nakashima, Ellen, "Indictment of PLA Hackers Is Part of Broad U.S. Strategy to Curb Chinese Cyberspying," *Washington Post*, May 22, 2014. As of December 1, 2015: https://www.washingtonpost.com/world/national-security/indictment-of-pla-hackers-is-part-of-broad-us-strategy-to-curb-chinese-cyberspying/2014/05/22/a66cf26a-e1b4-11e3-9743-bb9b59cde7b9_story.html

———, "Security Firm Finds Link Between China and Anthem Hack," *Washington Post*, February 27, 2015a. As of November 30, 2015: https://www.washingtonpost.com/news/the-switch/wp/2015/02/27/security-firm-finds-link-between-china-and-anthem-hack

———, "With Series of Major Hacks, China Builds Database on Americans," *Washington Post*, June 5, 2015b. As of November 30, 2015: https://www.washingtonpost.com/world/national-security/in-a-series-of-hacks-china-appears-to-building-a-database-on-americans/2015/06/05/d2af51fa-0ba3-11e5-95fd-d580f1c5d44e_story.html

———, "U.S. Developing Sanctions Against China over Economic Spying," *Washington Post*, August 30, 2015c. As of December 1, 2015: https://www.washingtonpost.com/world/national-security/administration-developing-sanctions-against-china-over-cyberespionage/2015/08/30/9b2910aa-480b-11e5-8ab4-c73967a143d3_story.html

Nakashima, Ellen, and Adam Goldman, "In a First, Chinese Hackers Are Arrested at the Behest of the U.S. Government," *Washington Post*, October 9, 2015. As of December 2, 2015: https://www.washingtonpost.com/world/national-security/in-a-first-chinese-hackers-are-arrested-at-the-behest-of-the-us-government/2015/10/09/0a7b0e46-6778-11e5-8325-a42b5a459b1e_story.html

Nathan, Andrew J., and Andrew Scobell, "How China Sees America: The Sum of Beijing's Fears," *Foreign Affairs*, September/October 2012. As of November 30, 2015: https://www.foreignaffairs.com/articles/china/2012-08-16/how-china-sees-america

Novetta, "Cyber Security Coalition Releases Full Report on Large-Scale Interdiction of Chinese State Sponsored Espionage Effort," Washington, D.C., October 28, 2014. As of December 2, 2015: https://www.novetta.com/2014/10/cyber-security-coalition-releases-full-report-on-large-scale-interdiction-of-chinese-state-sponsored-espionage-effort

Obama, Barack, "Executive Order—'Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities,'" Washington, D.C.: The White House, April 1, 2015. As of December 2, 2015: https://www.whitehouse.gov/the-press-office/2015/04/01/executive-order-blocking-property-certain-persons-engaging-significant-m

"Obama Raises Spectre of Future Cyber War Ahead of Xi Jinping's Visit, Promises That China Cannot Win," *South China Morning Post*, September 12, 2015. As of December 1, 2015: http://www.scmp.com/news/world/article/1857499/obama-issues-tough-warning-china-against-cyber-attacks-ahead-xi-jinpings?page=all

"Official Urges China-U.S. Trust on Cyber Security," Xinhua, April 10, 2013. As of December 2, 2015: http://www.chinadaily.com.cn/china/2013-04/10/content_16388107.htm

Oh, Julia, "Cyber Cooperation in Northeast Asia: An Interview with James Lewis," National Bureau of Asian Research, Policy Q&A, March 17, 2015. As of November 30, 2015: http://nbr.org/downloads/pdfs/psa/Lewis_interview_031715.pdf

Ostroukh, Audrey, "Russia, China Forge Closer Ties with New Economic, Financing Accords," *Wall Street Journal,* May 8, 2015. As of December 2, 2015: http://www.wsj.com/articles/russia-china-forge-closer-ties-with-new-economic-financing-accords-1431099095

Perlez, Jane, "Strident Video by Chinese Military Casts U.S. as Menace," *New York Times*, October 31, 2013. As of November 30, 2015: http://sinosphere.blogs.nytimes.com/2013/10/31/strident-video-by-chinese-military-casts-u-s-as-menace/?_r=0

Perlroth, Nicole, "Nissan Is Latest Company to Get Hacked," *New York Times*, April 24, 2012. As of December 2, 2015: http://bits.blogs.nytimes.com/2012/04/24/nissan-is-latest-company-to-get-hacked/?_r=0

———, "Hackers in China Attacked the *Times* for Last Four Months," *New York Times*, January 31, 2013. As of December 2, 2015: http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html

———, "China Is Said to Use Powerful New Weapon to Censor the Internet," *New York Times*, April 10, 2015. As of December 1, 2015: http://www.nytimes.com/2015/04/11/technology/china-is-said-to-use-powerful-new-weapon-to-censor-internet.html?_r=0

Qian Yingyi, Jia Qingguo, Bai Chong'en, and Wang Jisi, "Building Mutual Trust Between China and the U.S.," in Shao Binhong, ed., *The World in 2020 According to China: Chinese Foreign Policy Elites Discuss Emerging Trends in International Politics*, Leiden, The Netherlands: Koninklijke Brill NV, 2014, pp. 277–291.

Rauscher, Karl Frederick, and Zhou Yonglin, *Fighting Spam to Build Trust*, New York: EastWest Institute, 2011. As of November 30, 2015: http://www.eastwest.ngo/sites/default/files/ideas-files/China-US-Fighting-Spam.pdf

Riley, Michael A., and Sophia Pearson, "China-Based Hackers Target Law Firms to Get Secret Deal Data," Bloomberg, January 31, 2012. As of December 2, 2015: http://www.bloomberg.com/news/articles/2012-01-31/china-based-hackers-target-law-firms

Sanger, David E., "U.S. and China Seek Arms Deal for Cyberspace," *New York Times*, September 19, 2015. As of December 2, 2015: http://www.nytimes.com/2015/09/20/world/asia/us-and-china-seek-arms-deal-for-cyberspace.html

Sanger, David E., and Martin Fackler, "N.S.A. Breached North Korean Networks Before Sony Attacks, Officials Say," *New York Times*, January 18, 2015. As of December 2, 2015: http://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html

Sasso, Brendan, "Report: China Hacked Obama, McCain Campaigns in 2008," *The Hill*, June 7, 2013. As of December 2, 2015: http://thehill.com/policy/technology/304111-report-china-hacked-obama-mccain-campaigns

Schmidt, Michael S., and David E. Sanger, "5 in China Army Face U.S. Charges of Cyberattacks," *New York Times*, May 19, 2014. As of November 30, 2015: http://www.nytimes.com/2014/05/20/us/us-to-charge-chinese-workers-with-cyberspying.html

Schwartz, Matthew J., "Lockheed Martin Suffers Massive Cyberattack," *InformationWeek Dark Reading*, May 30, 2011. As of December 2, 2015: http://www.darkreading.com/risk-management/lockheed-martin-suffers-massive-cyberattack/d/d-id/1098013?

Sefton, Eliot, "Chinese 'Hacked French Ministry for G20 Data,'" *The Week*, March 8, 2011. As of December 2, 2015: http://www.theweek.co.uk/technology/7229/chinese-%E2%80%98hacked-french-ministry-g20-data%E2%80%99

Segal, Adam, "Chinese Responses to the International Strategy for Cyberspace," Council on Foreign Relations, May 23, 2011. As of December 2, 2015: http://blogs.cfr.org/asia/2011/05/23/chinese-responses-to-the-international-strategy-for-cyberspace

Shambaugh, David, "Coping with a Conflicted China," *Washington Quarterly*, Vol. 34, No. 1, winter 2011, pp. 7–27.

———, "In a Fundamental Shift, China and the US Are Now Engaged in All-Out Competition," *South China Morning Post*, June 14, 2015. As of November 30, 2015: http://www.scmp.com/comment/insight-opinion/article/1819980/fundamental-shift-china-and-us-are-now-engaged-all-out?page=all

Shen Yi, "Responding to the Challenge of the 'Offensive Internet Freedom Strategy': Analyzing Sino-US Competition and Cooperation in Global Cyberspace" ["Yingdui jingongxing hulianwang ziyou zhanlüe de tiaozhan: Xi Zhong-Mei zai quanqiu xinxi kongjian de jingzheng yu hezuo"], *World Economics and Politics* [*Shijie jingji yu zhengzhi*], No. 2, 2012, pp. 69–79.

Swaine, Michael D., "Chinese Views of Cybersecurity in Foreign Relations," *China Leadership Monitor*, No. 42, fall 2013. As of December 1, 2015: http://carnegieendowment.org/files/CLM42MS.pdf

Taylor, Rob, "Australian Spy HQ Plans Stolen by Chinese Hackers: Report," Reuters, May 27, 2013. As of December 2, 2015: http://www.reuters.com/article/2013/05/28/us-australia-hacking-idUSBRE94R02A20130528#843ZBaqbOaYt0CzQ.97

Tejada, Carlos, "Microsoft, the 'Guardian Warriors' and China's Cybersecurity Fears," *Wall Street Journal*, July 29, 2014. As of December 1, 2015: http://blogs.wsj.com/digits/2014/07/29/microsoft-the-guardian-warriors-and-chinas-cybersecurity-fears

Thornburgh, Nathan, "Inside the Chinese Hack Attack," *Time*, August 25, 2005. As of December 2, 2015: http://content.time.com/time/nation/article/0,8599,1098371,00.html

Tiezzi, Shannon, "Taiwan Complains of 'Severe' Cyber Attacks from China," *The Diplomat*, August 15, 2014. As of December 2, 2015: http://thediplomat.com/2014/08/taiwan-complains-of-severe-cyber-attacks-from-china

———, "U.S., China Open New High-Level Cyber Talks," *The Diplomat*, December 2, 2015. As of December 21, 2015: http://thediplomat.com/2015/12/us-china-open-new-high-level-cyber-talks

"Twelve Chinese Hacker Groups Responsible for Attacks on U.S.," Homeland Security News Wire, December 16, 2011. As of December 2, 2015: http://www.homelandsecuritynewswire.com/dr20111216-twelve-chinese-hacker-groups-responsible-for-attacks-on-u-s

UN General Assembly (70th session), "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security," July 22, 2015. As of December 2, 2015: https://disarmament-library.un.org/UNODA/Library.nsf/93a4b64e6849591d85257ddc006cbf21/49ef2dd67a02448b85257ea0006d13dd/$FILE/A%2070%20174%20GGE%20on%20Information%20&%20Telecomms%20in%20the%20field%20of%20International%20Security.pdf

U.S. Department of Defense, *The Department of Defense Cyber Strategy*, April 2015. As of December 2, 2015: http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

U.S. Department of Homeland Security, "Cyber Storm: Securing Cyberspace," Web page, December 1, 2015. As of December 2, 2015: http://www.dhs.gov/cyber-storm-securing-cyber-space

U.S. Department of Justice, Office of Public Affairs, "U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage," Washington, D.C., May 19, 2014. As of December 2, 2015: http://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor

Wang Xu, "China 'Open to' Cybersecurity Teamwork," *China Daily*, September 18, 2015. As of November 30, 2015: http://europe.chinadaily.com.cn/china/2015-09/18/content_21912724.htm

Wee, Sui-Lee, "China Orders Lawyers to Swear Allegiance to the Communist Party," Reuters, March 21, 2012. As of December 2, 2015: http://www.reuters.com/article/2012/03/21/us-china-lawyers-idUSBRE82K0G320120321#MKvsxt7iv05FtiVj.97

Welch, Dylan, "Chinese Hackers 'Breach Australian Media Organizations' Ahead of G20," Australian Broadcasting Corporation, November 13, 2014. As of December 2, 2015: http://www.abc.net.au/news/2014-11-13/g20-china-affliliated-hackers-breaches-australian-media/5889442

White House, *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, Washington, D.C., May 2011, p. 10.

———, "Fact Sheet: President Xi Jinping's State Visit to the United States," Washington, D.C., September 25, 2015. As of December 2, 2015: https://www.whitehouse.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states

Winterbottom, Vaughan, "In China, Constitutionalism Is a Dirty Word," *The Interpreter*, January 28, 2014. As of December 1, 2015: http://www.lowyinterpreter.org/post/2014/01/28/In-China-constitutionalism-is-a-dirty-word.aspx

Wolf, David, "Why Buy the Hardware When China Is Getting the IP for Free?" *Foreign Policy*, April 24, 2015. As of December 2, 2015: http://foreignpolicy.com/2015/04/24/ibm-technology-transfer-china-virginia-rometty-strategy-lenovo-huawei-it

Wong, Edward, "Chinese Colonel's Hard-Line Views Seep into the Mainstream," *New York Times*, October 3, 2015. As of November 30, 2015: http://www.nytimes.com/2015/10/03/world/asia/chinese-colonels-hard-line-views-seep-into-the-mainstream.html

Yadron, Danny, James T. Areddy, and Paul Mozur, "Chinese Hacking Is Deep and Diverse, Experts Say," *Wall Street Journal*, May 29, 2014. As of December 2, 2015: http://www.wsj.com/articles/china-hacking-is-deep-and-diverse-experts-say-1401408979

Yang Jian, "The Nature of the Contextual Contradictions in America's Use of the Phrase 'Cyberspace Global Commons' [Meiguo 'Wangluo kongjian quanqiu gongyu shuo' de yujing maodun jiqi benzhi]," *International Survey* [*Guoji guancha*], No. 1, 2013, pp. 46–52.

Yi Wenli, "Divergence Between China and the U.S. and the Path Toward Cooperation in Cyberspace" ["Zhong-Mei zai Wangluo Kongjian de Fenqi yu Hezuo Lujing"], *Contemporary International Relations* [*Xiandai Guoji Guanxi*], Vol. 22, No. 4, July/August 2012, pp. 124–141.

Yui, Monami, and Shingo Kawamoto, "Chinese Criminals Blamed for Record Japan Bank Cybertheft," Bloomberg, December 17, 2014. As of December 2, 2015: http://www.bloomberg.com/news/articles/2014-12-17/chinese-criminals-blamed-for-record-japan-bank-cybertheft

Zhi Linfei, "Commentary: U.S. Should Think Twice Before Retaliating Against China over Unfounded Hacking Charges," Xinhua, August 3, 2015. As of December 1, 2015: http://www.china.org.cn/world/Off_the_Wire/2015-08/03/content_36211902.htm

Zhou Wa, "Internet Regulation a Sovereign Issue: FM," *China Daily*, May 20, 2011. As of December 2, 2015: http://www.chinadaily.com.cn/china/2011-05/20/content_12545488.htm

Zhu Junqing, "Commentary: U.S. Wronging of China for Cyber Breaches Harm Mutual Trust," Xinhua, June 6, 2015.

منذ تأسيس جمهورية الصين الشعبية في عام 1949، اتسمت العلاقات بين الولايات المتحدة والصين بقدر كبير من الصراع والتحدي والريبة الاستراتيجية. وقد زاد ثقل التوترات التي تفرق بين البلدين في السنوات الأخيرة. وللأسف، تنعكس هذه التوترات على الفضاء الإلكتروني بقدر ما تنعكس على العلاقات في العالم المادي. وفي الواقع، من بين جميع المجالات التي اضطربت فيها العلاقة بين الطرفين، كان مجال الفضاء الإلكتروني أكثرها إثارة للخلاف. شرعت كل من الولايات المتحدة والصين في بدء مفاوضات رسمية عام 2013 سعيًا إلى تسوية هذه الخلافات، إلاأنها توقفت فجأة عام 2014، وذلك عندما أوقفت الصين المفاوضات ردًا على إدانة الولايات المتحدة لعدد من الضباط العسكريين الصينيين باتهامات تتعلق بأنشطة تجسس إلكتروني. وتستكشف هذه الدراسة خيارات السياسة الأمريكية لإدارة العلاقات مع الصين بشأن هذا الموضوع السياسي الشائك من خلال استخدام الاتفاقات وقواعد السلوك. وينظر التقرير في مسألتين أساسيتين: هل يمكن لكل من الولايات المتحدة والصين تحقيق نتائج مجدية من خلال المفاوضات الرسمية بخصوص المعايير والقواعد الخاصة بالفضاء الإلكتروني؟ و في تلك الحالة، ما هي أكثر المجالات التي من المرجح أن يتم التوصل فيها إلى اتفاق وما الأمور التي يمكن استبدالها بأخرى؟ التحليل الوارد هنا مهم لمجموعتين: المجموعة المعنية بعلاقات الولايات المتحدة مع الصين، وتلك المعنية بوضع قواعد السلوك فيما يختص بالفضاء الإلكتروني، ولا سيما القواعد التي تعزِّز الأمن والحرية.

RAND CORPORATION

www.rand.org

$19,50

ISBN-10 0-8330-9249-9
ISBN-13 978-0-8330-9249-6

Arabic translation
[Getting to Yes with China in Cyberspace]
RR-1335/2-RC