مركز حمورابي

عصر حروب التجسس على سلاسل التوريد قد بدأ

كيف يمكن للولايات المتحدة أن تستعد لعالم جديد من التخريب الذي تديره الدول؟

عصر حروب التجسس على سلاسل التوريد قد بدأ
كيف يمكن للولايات المتحدة أن تستعد لعالم جديد من التخريب الذي تديره الدول؟

بقلم: كالدر والتون وكيفن كوينلان
ترجمة: صفا مهدي/ مركز حمورابي للبحوث والدراسات الإستراتيجية

مركز حمورابي للبحوث والدراسات الإستراتيجية

16 كانون الاول 2024

التخريب الذي استهدف أجهزة اتصالات حزب الله في وقت سابق من هذا العام، والذي يُعتقد أنه من تنفيذ (إسرائيل)**، كان بلا شك استثنائيًا من الناحية التقنية، ولكنه من منظور التجسس ليس أمرًا جديدًا. لطالما استهدفت وكالات الاستخبارات سلاسل التوريد واستغلتها لأغراض جمع المعلومات الاستخباراتية والتخريب، فمن الحرب الباردة في القرن العشرين إلى الصراع الجيوسياسي الحالي مع روسيا والصين، كانت اختراق سلاسل التوريد دائمًا فرصة للحصول على معلومات قيمة عن الخصوم أو تعطيل قطاعات حيوية في اقتصادهم.

في الوقت الراهن ينشغل المسؤولون الغربيون بتقييم نقاط الضعف الاستراتيجية والتكتيكية في سلاسل التوريد الخاصة بهم، في واشنطن نادرًا ما تمر مؤتمرات دون الإشارة إلى قانون CHIPS وسلاسل توريد أشباه الموصلات. تضخ الولايات المتحدة مليارات الدولارات لتطوير أنظمة تصنيع التقنيات العالية ومعالجة المواد الأساسية لدعم صناعة الإلكترونيات الدقيقة محليًا (مثل مشاريع شركة إنتل في أريزونا) وفي دول شريكة (مثل المكسيك والفلبين وغيرها).

كما دفعت المخاوف بشأن هشاشة سلاسل التوريد في قطاع الدفاع وزارة الدفاع الأمريكية إلى إعداد أول استراتيجية صناعية دفاعية لها، وأيضًا أنشأ البيت الأبيض مجلسًا لتعزيز مرونة سلاسل التوريد لتنسيق وإدارة العديد من المبادرات المتعلقة بسلاسل التوريد داخل الحكومة الأمريكية. اللافت في هذا التحول في النهج الأمريكي هو أنه استغرق وقتًا طويلًا، العولمة لم تحقق النتائج المتوقعة، المبادئ الأساسية للسياسات الاقتصادية الليبرالية، مثل المنافسة المثالية والكفاءة، تتراجع لصالح فكرة تعزيز المرونة ضد المخاطر التي يفرضها الخصوم، لا سيما الصين وروسيا.

** لمقتضيات الأمانة العلمية، وضرورات الترجمة الدقيقة، تم الإبقاء على كلمة (إسرائيل)، وهو لا يعني اعتراف المركز بها، وما هو مكتوب يمثل راي وأفكار المؤلف.

---

* Calder Walton, and Kevin Quinlan, The Era of Supply Chain Spy Wars Is Here How the United States can prepare for the new world of state-led Sabotage, FOREIGN POLICY, DECEMBER 10, 2024.

** لمقتضيات الأمانة العلمية، وضرورات الترجمة الدقيقة، تم الإبقاء على كلمة (إسرائيل)، وهو لا يعني اعتراف المركز بها، وما هو مكتوب يمثل راي وأفكار المؤلف.

الصين على سبيل المثال لم تتبنَّ يومًا فكرة فصل الأمن الوطني عن الأمن الاقتصادي، بل إن نهجها في تحقيق التقدم الوطني لا يعتمد على استراتيجية حكومية شاملة فقط، بل على استراتيجية تشمل المجتمع بأسره. فكرة أن الأمن الوطني والاقتصادي منفصلان تفتقر إلى المصداقية خارج الاقتصادات الليبرالية الغربية، فقد اتبعت الصين رؤيتها الخاصة للقوة الوطنية، بما في ذلك محاولاتها لتجنب الضغوط الاقتصادية من خلال سلاسل التوريد في القطاعات الصناعية الحيوية. بعبارة أخرى، يبدو أن صناع القرار الصينيين يدركون جيدا تاريخ التخريب في سلاسل التوريد. وسيستفيد صناع القرار في الولايات المتحدة من فهم أعمق للأشكال التاريخية للتخريب التي أثبتت نجاحها، والتغيرات التي طرأت على سلاسل التوريد، والتكتيكات التي يستخدمها خصومهم في الوقت الحاضر، تقدم هذه الدروس التاريخية إرشادات قيمة حول كيفية تحسين حماية الولايات المتحدة نفسها من استغلال سلاسل التوريد من قبل الدول المعادية اليوم.

التخريب في سلاسل التوريد الخاصة بالخصوم قديم قدم فنون الحكم والحروب، في العصور الوسطى استخدمت الجيوش الجواسيس الذين كانوا يتنكرون كتجار لمعرفة ما يشتريه الخصوم، كما كانوا يسممون مصادر المياه لدى الأعداء، وفي القرن العشرين عندما اكتشفت الاستخبارات البريطانية أن ألمانيا النازية تستخدم شركات تجارية واجهة للتجسس، حاول البريطانيون - ولكنهم لم ينجحوا على ما يبدو - تعديل التكنولوجيا التي كانت برلين تستهدفها.

بعد الحرب تطور استخدام سلاسل التوريد لجمع المعلومات الاستخباراتية وتنفيذ عمليات التخريب، وخلال الحرب الباردة المبكرة أعدت وكالة الاستخبارات المركزية الأمريكية عملية ذكية لجمع الاتصالات الأجنبية عن طريق التلاعب في تصنيع وتوريد المعدات، وتعاونت سرًا مع شركة سويسرية ذات سمعة طيبة تُدعى Crypto AG لبيع أجهزة تشفير معدلة لدول ثالثة، كانت تلك الدول تشتري أجهزة "كريبتو" معتقدة أنها تقتني أفضل تكنولوجيا سويسرية محايدة يمكن الحصول عليها.

لكن عملية وكالة الاستخبارات المركزية، التي أُطلق عليها اسم RUBICON وكُشف عنها فقط في عام 2020، سمحت للحكومة الأمريكية بقراءة الاتصالات الأجنبية بسهولة، وفي مراحل لاحقة من الحرب الباردة، اتخذت عمليات التجسس والتخريب على سلاسل التوريد أبعادًا جديدة. استهدفت أجهزة الاستخبارات السوفييتية، مثل الـ KGB والـ GRU، الدول الغربية لسرقة أكبر قدر ممكن من المعلومات العلمية والتقنية لتحقيق الاستراتيجية الأيديولوجية الكبرى للاتحاد السوفييتي ضد الإمبريالية الغربية، وعلى رأسها الولايات المتحدة.

ساهم التقارب الذي أحدثه ريتشارد نيكسون وهنري كيسنجر بين الشرق والغرب، والمعروف باسم الانفراج الدولي (Détente) في فتح قنوات العلاقات التجارية بين الكتلة السوفييتية والولايات المتحدة. رغم أن الحكومة الأمريكية فرضت قيودًا على بيع التقنيات ذات الاستخدام المزدوج خلف الستار الحديدي، استغلت الاستخبارات السوفييتية فترة الانفراج لشن هجوم باستخدام شركات تجارية واجهة لسرقة الأسرار الصناعية والعسكرية الغربية. في عام 1982، كشف عميل سوفييتي يعمل في قسم الاستخبارات العلمية والتقنية التابع

لل . KGB، والمعروف بـ Line X، عن مدى الهجوم الاستخباراتي السوفييتي على الغرب، حصل هذا العميل (فلاديمير فيتروف) على الاسم الرمزي FAREWELL من مشغليه في الاستخبارات الفرنسية، مكنت معلومات فيتروف الاستخبارات الفرنسية وحلفاءها من فهم غير مسبوق لعمليات التسلل السوفييتية السرية إلى سلاسل التوريد الغربية. قدّم فيتروف معلومات استخباراتية شديدة الحساسية تضمنت حوالي 4,000 وثيقة سرقها، والتي أصبحت تُعرف الآن بـ "ملف FAREWELL ". تم نقل هذا الملف عبر أعلى المستويات إلى البيت الأبيض ومجتمع الاستخبارات الأمريكي، سمح الملف لوكالة الاستخبارات المركزية (CIA)، بالتعاون مع بعض الشركاء الأوروبيين، بالانتقال إلى ما هو أبعد من التجسس – إلى تخريب سلاسل التوريد التي استهدفتها الكتلة السوفييتية. رغم غموض التفاصيل الدقيقة، تشير التقارير إلى أن عمليات الـ CIA تضمنت تزويد الحكومة السوفييتية بتصميم مُعدل من وكالة ناسا لمكوك فضائي، ورقائق حاسوبية معيبة، ومعلومات مضللة عن تكنولوجيا التخفي، وتوربينات معطلة تسببت في كارثة في سيبيريا عند استخدامها.

وبفضل الصحافة الاستقصائية الحديثة التي قام بها مراسل الأمن القومي زاك دورفمان، نعلم الآن أن مكتب التحقيقات الفيدرالي (FBI) كان يقوم بعمليات مماثلة، في عملية تحمل الاسم الرمزي INTERING، ضمن مكتب التحقيقات أن الاتحاد السوفييتي "سيشتري دون علمه منتجات أمريكية معطوبة بملايين الدولارات"، كما كتب دورفمان في مقال حديث بمجلة Politico. استخدم مكتب التحقيقات رجل أعمال نمساويًا له علاقات واسعة، لا يزال هويته سرية لنشر التكنولوجيا المعيبة في موسكو وحلفائها مما استنزف موارد الكتلة السوفييتية المالية، وكشف ضباط استخباراتها والمتآمرين السريين الأمريكيين وأوضح للعملاء المضادين الأمريكيين نوعية التكنولوجيا التي يسعى السوفييت للحصول عليها. كانت بلغاريا الهدف الرئيسي لعملية INTERING، حيث تلقت بفضل مكتب التحقيقات مجموعة من المنتجات المعيبة في مجال الإلكترونيات الدقيقة، ويمكن القول إن الحرب الباردة في القرن الماضي كانت أكثر بساطة مقارنة بما نواجهه اليوم. لم يكن الاتحاد السوفييتي في أي وقت مضى قوة اقتصادية كبرى على الساحة الدولية، مما أتاح للدول الغربية تهميشه بسهولة، ولكن الوضع اليوم مختلف تمامًا بالنسبة للصين وحتى لروسيا التي أظهر اقتصادها مرونة مذهلة في مواجهة العقوبات الغربية عقب غزوها الشامل لأوكرانيا.

وبينما يمكن العثور على أوجه تشابه بين الحرب الباردة في القرن العشرين والصراع الجيوسياسي الحالي بين الشرق والغرب، إلا أن هناك اختلافات رئيسية تجعل هذا التنافس أكثر تعقيدًا. أشارت وزيرة الخارجية الأمريكية السابقة (كوندوليزا رايس) في تصريحاتها الأخيرة إلى أن الوزن الاقتصادي الهائل للصين واندماجها العميق مع الاقتصاد العالمي خلال العقدين الماضيين جعلا المنافسة الحالية أكثر خطورة من الحرب الباردة السابقة.

في العصر الرقمي الحالي، تغيرت أساليب استغلال سلاسل التوريد بشكل جذري عما كانت عليه في الماضي، كتب شاشانك جوشي، محرر الدفاع في مجلة The Economist، في تقرير صدر في ايلول الماضي: "ما كان يتطلب

في الماضي إنشاء شركات وهمية وبنية تحتية مادية، إلى جانب عملاء يحملون أدوات تخريبية، يمكن الآن تحقيقه من خلال الهجمات الإلكترونية". مثال حديث على ذلك هو اختراق "سولار ويندز"(SolarWinds) الذي نفذته روسيا، والذي يُعد أكبر عملية اختراق إلكتروني معروفة في تاريخ الولايات المتحدة، واكتُشف في كانون الاول 2020.في هذا الهجوم تمكنت الحكومة الروسية من إدخال برمجيات ضارة إلى الشبكات الفيدرالية والخاصة في الولايات المتحدة عبر تحديث برمجي من شركة SolarWinds".

كان الاختراق واسع النطاق حيث طال قطاعات أساسية من البنية التحتية للأمن القومي الأمريكي، بما في ذلك وزارة الطاقة التي تدير الوكالة الوطنية للأمن النووي (National Nuclear Security Administration)، وعلى الرغم من أن الدلائل الحالية تشير إلى أن هذا الهجوم كان يهدف إلى التجسس (جمع المعلومات) وليس التخريب، إلا أن البيئة الرقمية تجعل الفارق بين التجسس والتخريب ضئيلًا جدًا.

في كثير من الأحيان يمكن أن يعتمد الفرق على تعليمات برمجية صغيرة، فإما أن تظل البرمجية للمراقبة فقط أو أن تُفعل للتسبب بأضرار، كما أشارت الباحثة القانونية البريطانية جوليت سكينجسلي في دراستها الأخيرة فإن هذا الفرق البسيط في التنفيذ له انعكاسات كبيرة في القانون الدولي، التجسس عادةً مسموح به إلا إذا تم حظره بموجب معاهدات أو أعراف دولية، بينما يُعتبر التخريب محظورًا بشكل واضح.

تتبع الصين نهجًا مختلفًا جذريًا عن الاتحاد السوفييتي في استغلال سلاسل التوريد وجمع المعلومات الاستخباراتية، خلال الحرب الباردة كان الاتحاد السوفييتي يركز على سرقة محددة للتقنيات الغربية التي تدعم صناعاته الدفاعية والفضائية، ولكنه كان يفتقر إلى القدرة على إنتاج سلع يرغب العالم بشرائها باستثناء النفط، اليوم هذا لا ينطبق على الصين، جمهورية الصين الشعبية تبنت نهجًا شاملاً يُعرف بـ"الجهد المجتمعي الكامل"(Whole of Society Approach) جمع المعلومات الاستخباراتية واستغلال سلاسل التوريد.

ساعد هذا النهج الصين على تحقيق ازدهار اقتصادي استثنائي خلال العقدين الأولين من القرن الحادي والعشرين، حيث اندمجت بعمق في الاقتصاد العالمي عبر تصنيع سلع رخيصة ومرغوبة عالميًا، إلى جانب هذا النجاح التجاري قامت الصين بتنفيذ عمليات تجسس صناعي مكثفة، أو كما يُطلق عليها بلباقة "اكتساب الملكية الفكرية"، ما جعلها تتفوق على الاتحاد السوفييتي وروسيا في نطاق وشمولية جمع المعلومات الاستخباراتية.

يجمع الحزب الشيوعي الصيني (CCP) المعلومات باستخدام أساليب علنية وسرية، حيث يمزج بين المصادر المفتوحة ووسائل جمع الاستخبارات التقليدية، سواء البشرية أو التقنية. نتيجة لذلك أصبح الحزب الشيوعي الصيني خصمًا قويًا للولايات المتحدة وللغرب بشكل عام، مما يجعل الاتحاد السوفييتي وأجهزته الاستخباراتية تبدو ضعيفة بالمقارنة. يعتمد الحزب الشيوعي الصيني استراتيجية "الاندماج العسكري-المدني" لتحقيق مفهومه للأمن الوطني الشامل، وهو ما يعني استخدام جميع آليات الحكومة الصينية، والقطاع التجاري

والجيش والجاليات الصينية في الخارج لجمع المعلومات التي تدعم هدفه الاستراتيجي الأكبر: إزاحة الولايات المتحدة من مكانتها كأقوى قوة اقتصادية وعسكرية في العالم.

ازدادت حدة هذه الاستراتيجية بشكل ملحوظ منذ تولي شي جين بينغ السلطة قبل أكثر من عقد، وقد أعلنت الصين صراحةً رغبتها في الحصول على أي معلومات اقتصادية أو عسكرية تراها ضرورية لتحقيق أهدافها، من خلال أي وسيلة ممكنة وتعكس الوثائق الاستراتيجية الصينية الرئيسية، مثل خطة "صنع في الصين 2025"، سعي الصين لأن تصبح رائدة في العديد من المجالات التكنولوجية، بما في ذلك من خلال القفز على الولايات المتحدة في بعض الحالات عبر سرقة أو التجسس الصناعي.

تشمل المجالات التكنولوجية المستهدفة من قبل الصين تقنيات متقدمة مثل الذكاء الاصطناعي والحوسبة الكمية والبيولوجيا الاصطناعية وأشباه الموصلات وتقنيات الطيران والفضاء والاتصالات والروبوتات والطاقة الخضراء والتكنولوجيا النووية، وتؤكد الوثائق الاستراتيجية الصينية أن الدولة الصينية، إذا لم تتمكن من تطوير تقنية محليًا فهي ملزمة بسرقتها من الخارج لتحقيق هدف "إحياء الأمة" بعد قرن من الهيمنة الغربية.

تحت حكم شي جين بينغ اعتمد الحزب الشيوعي الصيني مجموعة من القوانين الأمنية التي تلزم الشركات الصينية بالتعاون مع أجهزة الأمن والاستخبارات عند الطلب، وقد تسبب هذا في إثارة القلق في الغرب بشأن استخدام الصين لبعض منصاتها مثل هواوي وتيك توك لجمع المعلومات الاستخباراتية، وكذلك في مراقبة البنية التحتية الأمريكية مثل الرافعات في الموانئ. هذا بالإضافة إلى قضايا تجسس أخرى تشمل شركات مثل علي بابا في أوروبا، كما تم اعتقال مواطن صيني في تشرين الاول الماضي بتهمة نقل معلومات استخباراتية عن تحركات الأسلحة الألمانية إلى الصين.

تواجه الحكومة الأمريكية خصمًا يتبع نهجًا مختلفًا تمامًا، حيث يدمج الحزب الشيوعي الصيني بين التجارة والحكومة والجيش، في حين أن الولايات المتحدة محدودة اليدين بسبب القيود المفروضة عليها. ومن أبرز هذه القيود هو المبدأ الأيديولوجي الذي يمنع الحكومة الأمريكية من ممارسة التجسس الصناعي لصالح الشركات الأمريكية، تم تبني هذا الموقف في تسعينيات القرن الماضي بعد نهاية الحرب الباردة، وفقًا لإفادات داخلية من وكالة الاستخبارات المركزية.

بينما يرى البعض أن استخدام الحكومة الأمريكية مواردها لصالح الشركات المحلية قد يعكس شكلاً من أشكال الرأسمالية الموجهة، لا تظهر دول غربية أخرى، مثل فرنسا و(إسرائيل)، مثل هذا التحفظ في الفصل بين الاستخبارات والتجارة. وبالطبع، لا يتوانى الحزب الشيوعي الصيني عن دمج الاستراتيجيات التجارية والاستخباراتية لتحقيق أهدافه. قد يكون الوقت قد حان لإعادة النظر في حظر التجسس الصناعي في الولايات المتحدة. هل يجب أن تستمر الولايات المتحدة في تبني مبادئ اقتصادية نظرية على حساب رفاهيتها الاقتصادية؟

مع التحولات العميقة في سلاسل التوريد العالمية، أصبح من الضروري اتباع نهج شامل وتعاوني بين صناع القرار السياسي والصناعات ومجتمعات الاستخبارات، ينبغي للحكومة الأمريكية أن تعيد النظر في طريقة تعاملها مع الشركات، لتراها كشركاء حقيقيين وليس فقط "مزودين"، ففي الوقت الذي تقود فيه الشركات الخاصة اليوم تطوير التقنيات الناشئة مثل الذكاء الاصطناعي والحوسبة الكمية فإن الحكومة تفتقر إلى القدرة على متابعة التقدم السريع في هذه المجالات.

في الوقت الحالي يُعتبر القطاع الخاص المسؤول عن 85% من البنية التحتية الحيوية في الولايات المتحدة، وفي العديد من الحالات تتفوق الشركات الخاصة على الحكومة في معرفتها العميقة بالقطاعات التي تعمل فيها، خصوصًا في المجالات التكنولوجية الناشئة.

إذا استطاعت الحكومة الأمريكية تعزيز التعاون مع القطاع الخاص، فإنها ستمهد الطريق نحو اقتصاد عالمي أكثر أمانًا وازدهارًا تحت القيادة الأمريكية في عصر التحول الرقمي والتقنيات المتقدمة، النقطة الأساسية التي يجب أن تنطلق منها واشنطن هي هذه الحقيقة البسيطة: الأمن الوطني اليوم هو أمن القطاع الخاص.

مركز حمورابي للبحوث و الدراسات الاستراتيجية

أسس مركز حمورابي للبحوث والدراسات الاستراتيجية في 25-4-2012 بمدينة بابل(الحلة)، كمركز علمي بحثي يمتد الى دراسة الموضوعات السياسية و المجتمعية بصورة علمية و استراتيجية، فضلاً عن التركيز على القضايا والظواهر الحادثة والمحتملة قي الشأن المحلي والأقليمي والدولي ، ويتعامل مع باحثين من مختلف التخصصات داخل العراق وخارجه، وتحتضن بغداد المقر الرئيسي للمركز.

www.hcrsiraq.net

07810234002

hcrsiraq@yahoo.com

t.me/hammurabicrss

مركز حمورابي للبحوث والدراسيات الاستراتيجية

hcrsiraq

العراق - بغداد- الكرادة