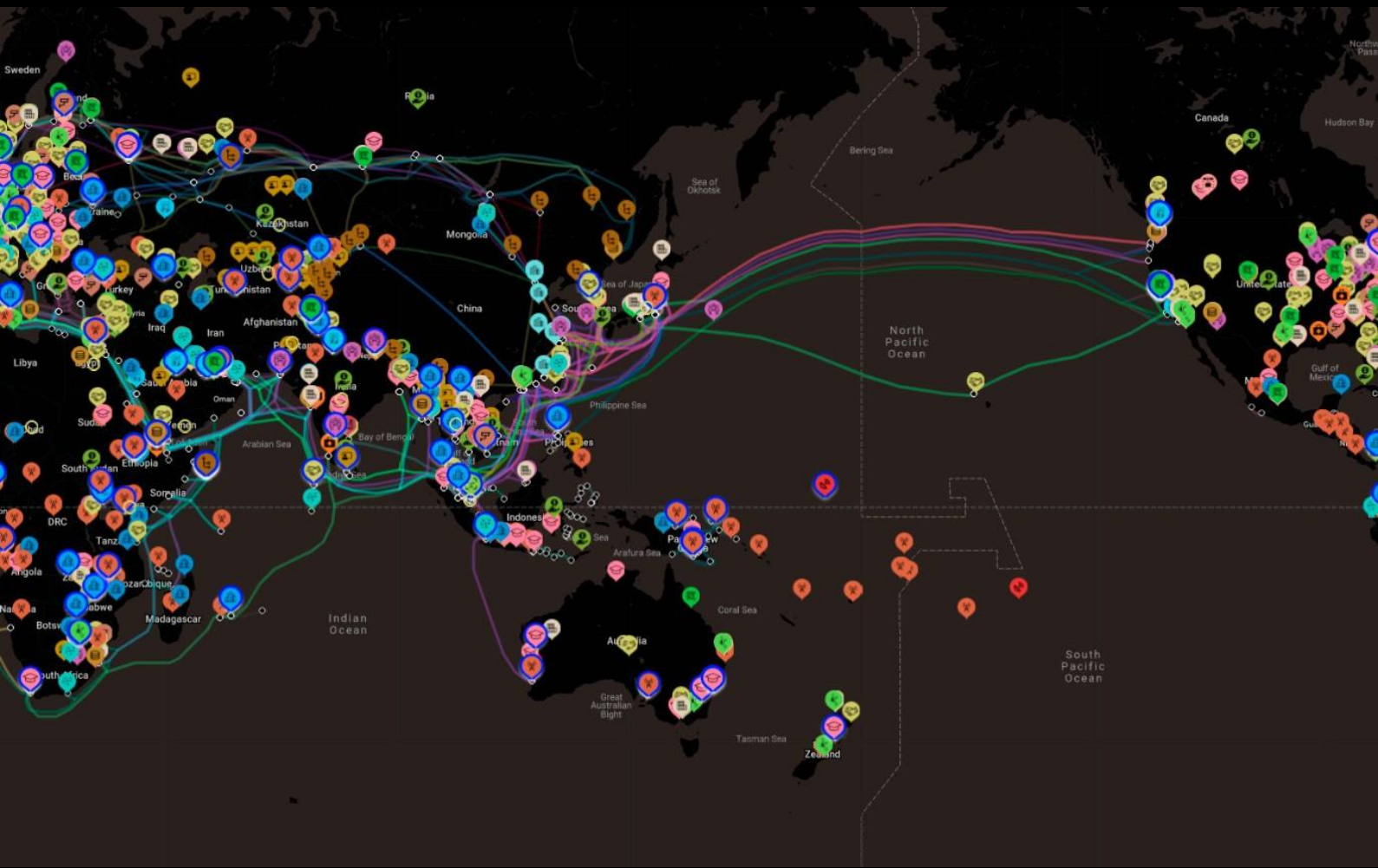
مشروع Mapping China’s Technology Giants (رسم خرائط شركات التكنولوجيا الصينية العملاقة)

سلاسل التوريد والنظام البيئي العالمي لجمع البيانات

الدكتورة سامانثا هوفمان والدكتور ناثان أتريل



تم ترجمة محتوى ASPI هذا بواسطة SDL، ولا يُعتد إلا بالمحتوى الأصلي باللغة الإنجليزية.

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE
INTERNATIONAL CYBER POLICY CENTRE
TWENTY YEARS OF ASPI STRATEGY FOR A SAFER FUTURE 2001 - 2021

حول المؤلفين

الدكتورة سامانثا هوفمان هي كبيرة محلّلين لدى المركز الدولي للسياسة السيبرانية التابع لمعهد ASPI.

الدكتور ناثان أتريل هو محلّل لدى المركز الدولي للسياسة السيبرانية التابع لمعهد ASPI.

شكر وتقدير

تتقدم بالشكر إلى دانيال كيف، وشيريل يو على كل ما بذلوه من جهد في هذا المشروع. ونودّ كذلك أن نتقدم بالشكر إلى زملائنا المراجعين الخارجيين ليندسي غورمان، وكارا فريدريك، وكريس كراولي. كما أننا ممتنون كذلك للتعليقات القيّمة والمساعدة المُقدَّمة من بيتر ماتيس وتوم أورين ومايكل شوبيريدج وفيرغوس هانسون.

يشكّل هذا التقرير البحثي جزءًا من مشروع Mapping China's Technology Giants، وهو مشروع يمتد لسنوات عديدة يهدف إلى رسم خرائط شركات التكنولوجيا الصينية الرائدة وتحليل التوسّع الخارجي لها. يهدف هذا المشروع إلى:

- تحليل التوسّع العالمي لمجموعة رئيسية من شركات التكنولوجيا الصينية العملاقة من خلال رسم خرائط للأماكن الرئيسية لنشاطها الخارجي.
- تزويد العامّة بتحليل لهياكل الحوكمة وسياسات دولة الحزب التي نشأت فيها هذه الشركات وترتبط بها ارتباطًا وثيقًا.

وقد تم إطلاق مشروع Mapping China's Technology Giants من قِبَل باحثين لدى المركز الدولي للسياسة السيبرانية التابع لمعهد ASPI. وتم تمويل إعادة إطلاق هذا المشروع وما يرتبط به من أبحاث بمنحة قدرها 270000 دولار أمريكي قدّمتها وزارة الخارجية

ما المقصود بـ ASPI؟

أُسِّس معهد السياسة الإستراتيجية الأسترالي (ASPI) في عام 2001 بوصفه مؤسسة فكرية مستقلة وغير حزبية. ويتمثل هدفه الأساسي في تزويد الحكومة الأسترالية بأفكار جديدة بشأن خيارات أستراليا في مجالات الدفاع والأمن والسياسة الإستراتيجية. إن معهد ASPI مسؤول عن تثقيف العامة بشأن مجموعة من القضايا الإستراتيجية، وخلق فكر جديد للحكومة وتسخير التفكير الإستراتيجي على المستوى الدولي. تتم الإشارة إلى مصادر تمويل معهد ASPI في تقريرنا السنوي المتاح عبر الإنترنت على الموقع www.aspi.org.au وفي قسم الشكر والتقدير في منشوراتنا الفردية. يظل معهد ASPI مستقلاً في محتوى البحث وفي جميع القرارات التحريرية.

المركز الدولي للسياسة السيبرانية التابع لمعهد ASPI

يُعَد المركز الدولي للسياسة السيبرانية (ICPC) التابع لمعهد ASPI صوتًا رائدًا في المناقشات العالمية حول التقنيات السيبرانية والناشئة والمهمة، والقضايا المتعلقة بالمعلومات والتدخل الأجنبي، ويركز على التأثير الذي تخلفه هذه القضايا في السياسة الإستراتيجية الأوسع نطاقًا. ويضم المركز مزيجًا متناميًا من الخبرات والمهارات مع فِرَق من الباحثين الذين يركزون على السياسة والتحليل الفني وعمليات الإعلام والتضليل، والتكنولوجيات المهمة والناشئة، وبناء القدرات السيبرانية، والتحليل عبر الأقمار الصناعية، والمراقبة، والقضايا المتعلقة بالصين.

يعمل مركز ICPC على إثراء النقاش العام في منطقة المحيطين الهندي والهادئ ودعم تطوير السياسات العامة من خلال إنتاج أبحاث أصلية وتجريبية قائمة على البيانات. ويثري مركز ICPC المناقشات الإقليمية عن طريق التعاون مع معاهد البحوث من مختلف أنحاء العالم وجلب خبراء عالميين رائدين إلى أستراليا، بما في ذلك من خلال الزمالات. ومن أجل تطوير القدرات في أستراليا وفي منطقة المحيطين الهندي والهادئ، يمتلك مركز ICPC فريقًا لبناء القدرات يتولى تنظيم ورش العمل، وبرامج التدريب، والتدريبات واسعة النطاق للقطاعين العام والخاص.

ونود أن نشكر جميع أولئك الذين يدعمون مركز ICPC ويسهمون فيه بوقتهم وفكرهم وشغفهم بالموضوعات التي نعمل عليها. إذا كنت ترغب في دعم عمل المركز، فيرجى الاتصال بـ: icpc@aspi.org.au

إخلاء مسؤولية مهم

يهدف هذا المنشور إلى توفير معلومات دقيقة وموثوقة في ما يتعلق بالموضوع الذي يتم تناوله. يتم توفيره على أساس أن الناشر لا يشارك في تقديم أي شكل من أشكال المشورة أو الخدمات المهنية أو غيرها. ولا ينبغي لأي شخص أن يعتمد على محتويات هذا المنشور من دون الحصول أولاً على المشورة من أحد المختصين المؤهلين.

ASPI

الهاتف 5100 6270 2 61+
البريد الإلكتروني enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au
facebook.com/ASPI.org
@ASPI_ICPC

حقوق الطبع والنشر © لمعهد السياسة الإستراتيجية الأسترالي المحدود لعام 2021

يخضع هذا المنشور لحقوق الطبع والنشر. ولا يمكن إعادة إنتاج أي جزء منه أو تخزينه في نظام استرجاع أو نقله بأي صورة أو بأي طريقة (إلكترونية أو آلية أو عبر النسخ المصغر أو النسخ الضوئي أو التسجيل أو خلاف ذلك)، باستثناء ما يُسمح به بموجب *قانون حقوق الطبع والتأليف لعام 1968*، دون إذن كتابي سابق. ويجب توجيه الاستفسارات إلى الناشرين. على الرغم مما سبق، تُمنح المؤسسات التعليمية (بما في ذلك المدارس والكليات المستقلة والجامعات ومعاهد التعليم الفني والتكميلي) الإذن لعمل نسخ من الأعمال المحمية بموجب حقوق الطبع والنشر لأغراض تعليمية فقط من دون الحصول على إذن صريح من معهد ASPI وبشكل مجاني.

تم نشر التقرير أول مرة في

يونيو/حزيران 2021. ISSN

2209-9689 (عبر الإنترنت)،
ISSN 2209-9670 (نسخة مطبوعة).

صورة الغلاف: ناثان أتريل، مركز ICPC التابع لمعهد ASPI

مؤّل هذا التقريرَ وزارةُ الخارجية الأمريكية.

مشروع Mapping China’s Technology Giants

سلاسل التوريد والنظام البيئي العالمي لجمع البيانات

الدكتورة سامانثا هوفمان والدكتور ناثان أتريل

تقرير السياسة
المختصر رقم 2021/45

المحتويات

ما المشكلة؟ 03

ما الحل؟ 03

1. النظام البيئي لبيانات جمهورية الصين الشعبية 05

1.1 أهمية الجهات التي تضع المعايير 07

1.2 الاستفادة من القيمة الإستراتيجية للبيانات 08

1.3 نظرة شاملة 09

2. إطار عمل أمن البيانات المتطور لجمهورية الصين الشعبية 11

2.1 لوائح البيانات: تقييد الأفراد والمنظمات مع تمكين الدولة 13

2.2 قواعد البيانات: وضع المعايير 16

3. إعادة النظر في نقاط ضعف سلسلة التوريد الرقمية 18

3.1 الوصول إلى البيانات في المراحل النهائية: دراسة حالة شركة GTCOM 19

3.2 قوة المعالجة 21

4. التوصيات 23

الملحق: مشروع قانون أمن البيانات ومشروع قانون حماية المعلومات الشخصية 24

المراجع 26

الاختصارات 30

ما المشكلة؟

تشارك معظم الشركات الـ 27 التي يتم تعقُّب أنشطتها ضمن مشروع Mapping China's Technology Giants بشكل كبير في جمع كميات هائلة من البيانات الشخصية والتنظيمية ومعالجتها بصورة كاملة بدءًا من حسابات وسائل التواصل الاجتماعي الشخصية مرورًا ببيانات المدن الذكية ووصولاً إلى البيانات الطبية الحيوية.[1] وتعتمد عملياتهم التجارية وما يرتبط بها من أشكال التعاون الدولي على تدفق كميات هائلة من البيانات، التي غالبًا ما تخضع لقوانين خصوصية البيانات في ولايات قضائية متعددة. لكن في الوقت الحالي، تغفل المناقشات السياسية العالمية الحالية والاستجابات السياسية اللاحقة المتعلقة بأمن سلسلة التوريد الرقمية عن المشهد الرئيسي لأنها عادةً ما تعطي الأولوية لاحتمال حدوث اضطرابات أو تعديلات خبيثة في سلسلة التوريد. وعلى الرغم من ذلك، تبدأ أخطار سلسلة التوريد الرقمية، وفق ما حدّدناه في هذا التقرير، عند مستوى التصميم (الشكل 1).

بالنسبة إلى جمهورية الصين الشعبية، فإن مسؤولية تصميم سلسلة التوريد تقع على عاتق دولة الحزب الصيني، وذلك من خلال فرض التوقّعات ووضع جدول الأعمال في ما يتعلق بالقوانين والوثائق السياسية واتخاذ الإجراءات مثل تعبئة موارد الدولة، لتحقيق أهداف مثل وضع معايير التكنولوجيا. ومن خلال هذه المعايير والسياسات والقوانين، تعمل دولة الحزب على صقل قدرتها على مراقبة أنشطة الشركات للتأكد من إمكانية قيامها باستخلاص القيمة الإستراتيجية والاستفادة من العمليات العالمية الخاصة بها. ويشمل ذلك الاستفادة من عمليات جمع البيانات من خلال الأنشطة التجارية العالمية اليومية لتلك الشركات، التي وضّحها المركز الدولي للسياسة السيبرانية التابع لمعهد ASPI في تقرير *Engineering global consent*.[2] إن التكنولوجيا ليست حيادية القيمة، فالجهة التي تضع المعايير ومن ثَمَّ تحدد اتجاه التكنولوجيا لا تقل في أهميتها عن جهة تصنيع المنتج. وستكون لهذا المنظور تأثيرات بالغة في فعالية قوانين حماية البيانات ومفاهيم أمن سلسلة التوريد الرقمية.

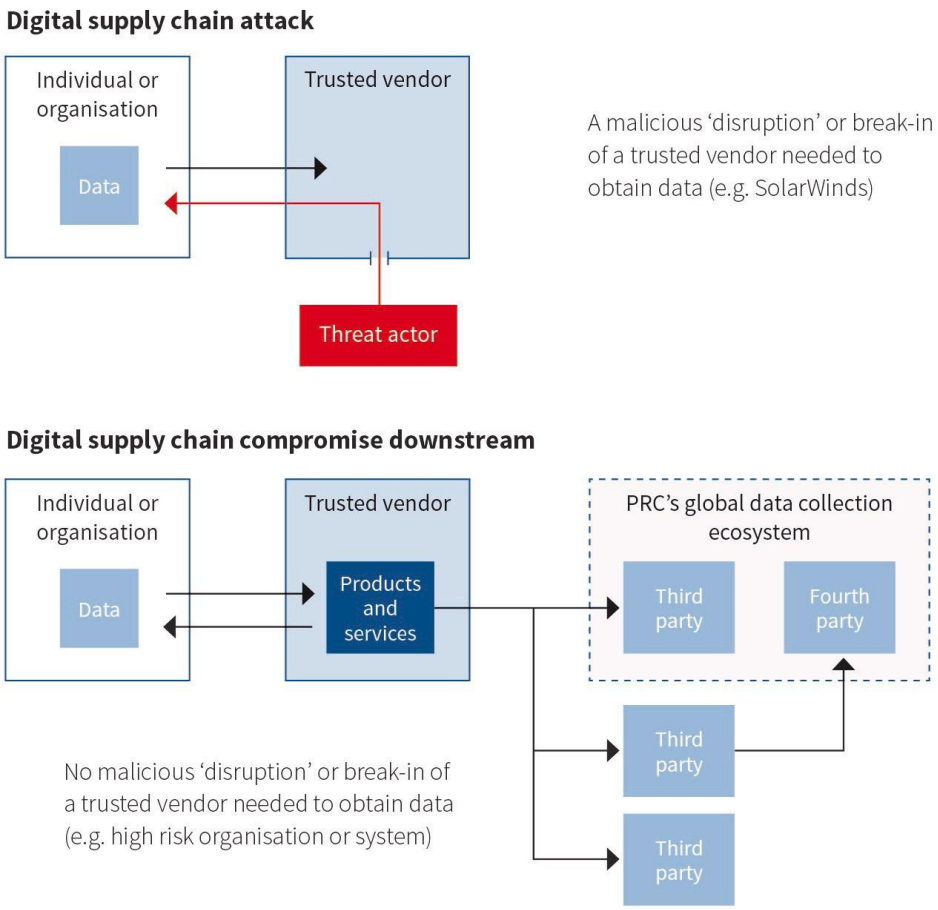
ما الحل؟

يوصي هذا التقرير الحكومات والشركات التجارية وغيرها من المنظمات باتباع نهج متعدد التخصصات لبذل العناية الواجبة. ومن المفترض أن يتضمن هذا النهج التفكير الإستراتيجي الأساسي الذي يتمثل في الطرق التي تستخدم بها دولة الحزب الصيني التكنولوجيا. كما يجب أن يتضمن اتساع نطاق ما يُعرف بـ "أمن الدولة" في الصين وتداعيات القوانين واللوائح المعمول بها في جمهورية الصين الشعبية، التي تركز على أمن البيانات والأمن السيبراني.

يتعين على كل الحكومات أن تعمل على تحسين أُطُرها التنظيمية المتعلقة بأمن البيانات وحماية الخصوصية. إذ إن ذلك من شأنه أن يضعها في مكانات أخلاقية وقانونية أفضل لاتخاذ تدابير سياسية جادة طويلة الأجل بشأن مجموعة كاملة من القضايا. ومع ذلك، لن تتصدى هذه الجهود وحدها لكل التحديات الفريدة التي تفرضها دولة الحزب الصيني أو غيرها من التحديات الجيوسياسية الموضحة في هذا التقرير.

يجب كذلك أن يتضمن النهج الأكثر شمولاً، الذي من شأنه أن يساعد على ضمان حماية البيانات بشكل أفضل، تعريفًا أفضل للأخطار المرتبطة بسلسلة التوريد الرقمية وإعادة صياغة المناقشات السياسية العالمية بشأن هذه القضايا. ويلزم إدراك الطريقة التي تظهر بها أخطار سلسلة التوريد بشكل أكبر، بما في ذلك التدخل المتعمد من قِبَل الجهات الفاعلة الخبيثة بهدف الوصول إلى المعلومات ومراقبتها وجمعها بشكل أكثر دقة. وينبغي أن تشتمل الإجراءات المُتبعة لإدارة انعدام أمن البيانات وانتهاكات الخصوصية المحتملة في سلاسل التوريد على تحسين النُهُج التي تركِّز على الأخطار لتنظيم عمليات نقل البيانات.

الشكل 1: اختراق سلسلة التوريد الرقمية من دون اختراق أو تغيير خبيث



المصدر: رسم توضيحي لمؤلفي معهد ASPI.

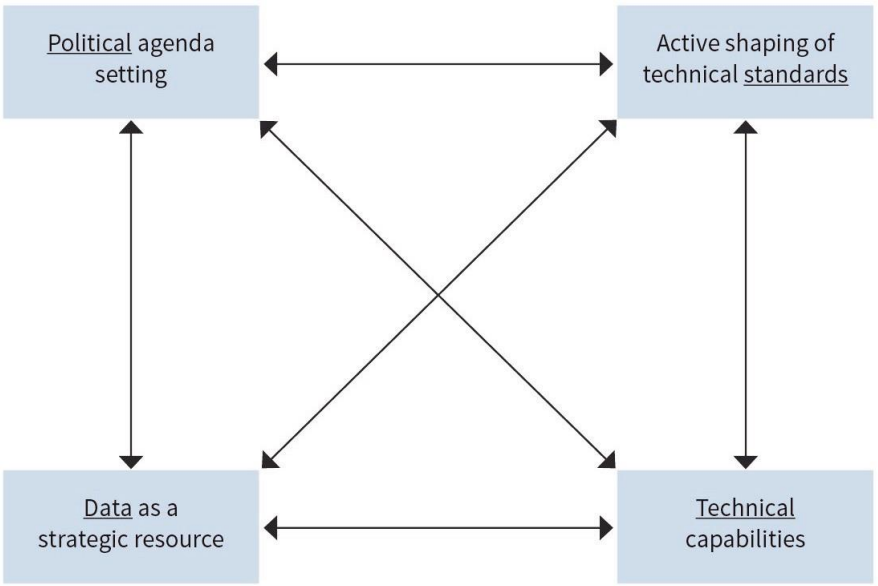
1. النظام البيئي لبيانات جمهورية الصين الشعبية

تم توضيح النظام البيئي العالمي لجمع بيانات جمهورية الصين الشعبية في التقرير السياسي "*Engineering global consent: the Chinese Communist Party's data-driven power expansion*" الذي أعدَّه المركز الدولي للسياسة السيبرانية التابع لمعهد ASPI.[3] وقد أوضحنا، في ذلك التقرير، الطرق التي استفادت بها دولة الحزب الصيني بشكل مباشر وغير مباشر من المؤسسات التجارية، التي تتخذ من جمهورية الصين الشعبية مقرًا لها، من أجل الوصول إلى مجموعة البيانات التي تساعد على زيادة انتاجية هذه المؤسسات.

استند ذلك التقرير إلى الطريقة التي أوضحت بها دولة الحزب الصيني أهدافها في ما يتعلق باستخدام البيانات وأمن الدولة، بالإضافة إلى دراسة حالة قسم الدعاية الخاص بشركة Global Tone Communication Technology Co. Ltd (التي نتناولها ببحث أعمق في قسم " الوصول إلى البيانات في المراحل النهائية" من هذا التقرير).

لقد قمنا ضمن مشروع Mapping China's Technology Giants بتوضيح أهمية تعريف مفهوم "النظام البيئي العالمي لبيانات جمهورية الصين الشعبية" بمزيد من التفصيل. ففي هذا القسم، نركز على طبيعة العلاقات بين وضع جدول الأعمال السياسي، والتشكيل النشط للمعايير الفنية الدولية، والإمكانات الفنية، والبيانات بوصفها موردًا إستراتيجيًا. حيث تؤثر هذه العلاقات بشكل مباشر في أنشطة الشركات التجارية، على الصعيدين المحلي والعالمي (الشكل 2).

الشكل 2: النظام البيئي لبيانات جمهورية الصين الشعبية



المصدر: رسم توضيحي لمؤلفي معهد ASPI.

الإمكانات الفنية هي حجر الأساس للنظام البيئي لبيانات جمهورية الصين الشعبية. حيث تتضمن هذه الإمكانات مهارات الصين المتقدمة للتعامل مع العمليات الهجومية السيبرانية، وتشمل كذلك العمليات التجارية العادية التي تجريها الشركات الصينية في أي مكان في العالم، ما يوفر لدولة الحزب إمكانية الوصول إلى البيانات أو جمعها أو معالجتها أو إجراء أكثر من عمليه من هذه العمليات الثلاث معًا.

تم الإبلاغ بالتفصيل وعلى نطاق واسع عن قدرة دولة الحزب على الوصول إلى كميات هائلة من المعلومات الشخصية والمعلومات المتعلقة بالملكية الفكرية من خلال عملياتها السيبرانية التي ترعاها الدولة، وقد وردت هذه البلاغات في لوائح الاتهام التي تصدرها وزارة العدل الأمريكية.[4] وعلى الرغم من ذلك، تشير سياسات جمهورية الصين الشعبية وتشريعاتها، التي صاغها الحزب الشيوعي الصيني عمدًا، إلى أن قدرة دولة الحزب على الوصول إلى البيانات تتجاوز العمليات العادية للشركات التي تتخذ من جمهورية الصين الشعبية مقرًا لها وتزاول أنشطة عالمية. ومن المهم أيضًا أن تحتل شركات التكنولوجيا العاملة في جمهورية الصين الشعبية التي تتمتع بنفوذ عالمي كل طبقة من طبقات "مجموعة التكنولوجيا".

في الجدول 1، قمنا بتوضيح "مجموعة التكنولوجيا" بالرجوع إلى نموذج الربط بين الأنظمة المفتوحة الموحد ISO (حيث إنه يُستخدَم في عمليات تبادل الشبكات والبيانات، ويمكن أيضًا أن يوضِّح النظام البيئي لصناعة التكنولوجيا).[5] ثم قمنا بتطبيقه على الشركات ذات الصلة بمشروع Mapping China's Technology Giants ونظرائها في الولايات المتحدة، التي كانت تمارس أنشطة مهيمنة في كل طبقة من طبقات النموذج لعدة عقود.

جدول 1: النظام البيئي للأعمال التكنولوجية، بالرجوع إلى نموذج الربط بين الأنظمة المفتوحة المبسط

الشركات الكائنة في جمهورية	الشركات الكائنة في الولايات	أمثلة عامة	تصنيفات البرامج/الأجهزة
طبقة التطبيقات	تطبيقات البرامج	منصات الإنترنت (على سبيل المثال، وسائل التواصل الاجتماعي، ومواقع الويب، وتطبيقات الأجهزة المحمولة)، ومحركات التعلّم الآلي (المُقدَّمة من موفري الخدمات السحابية)، وجهات معالجة المحتوى	Google وFacebook وApple وAmazon وMicrosoft وPayPal وZoom وSalesforce وAdobe	Baidu، وAlibaba، وTencent، وJD.com، وByteDance، وAnt Group، وMegvii، وCloudWalk، وiFlyte، وSenseTime، وYITU، وPing An Tech، وInspur، وHuawei، وCETC
طبقة الشبكة	البنية التحتية للتخزين والبرامج	شبكات تسليم المحتوى والتخزين السحابي والبنية التحتية	Cloudflare وAkamai وGoogle وMicrosoft وAmazon وIBM وOracle وApple	Alibaba وTencent وByteDance وPing An Tech وInspur وHuawei وCETC
	الأجهزة	نظام الملاحة عبر الأقمار الصناعية، وأجهزة الشبكات، وأجهزة الاستشعار، وأشباه الموصلات، ومعدات الربط الشبكي اللاسلكية المحمولة	Cisco وJuniper و Global (GPS) Positioning System وGoogle وAmazon وApple وNvidia وAMD و Texas Instruments وQualcomm، وIntel وBroadcom وMicrosoft وIBM	Huawei وZTE وBeiDou وNuctech وMeiya Pico وHikvision وUniview وDahua وMegvii وiFlytek وSenseTime وDJI و Huawei's HiSilicon وSMIC وCETC
الطبقة المادية	البنية التحتية لشركة الاتصالات	الكابلات البحرية، وشبكات الألياف الضوئية، والمعدات اللاسلكية المحمولة لشبكة شركة الاتصالات (المحطات الأساسية لشبكات الجيل الخامس 5G)	AT&T وSprint وVerizon وCogent وComcast وFacebook وGoogle وAmazon وMicrosoft وT-Mobile US	Hengtong وChina Mobile وChina Telecom و China PEACE cable Ltd وUnicom وHuawei وCETC

المصدر: رسم توضيحي لمؤلفي معهد ASPI.

إن المصالح التجارية هي المحرك الأساسي لشركات التكنولوجيا في كل مكان. ويكمن الفارق بين الولايات المتحدة والصين في أن الطريقة التي تتعامل بها الصين مع فائدة البيانات تتجاوز الطريقة التقليدية لجمع المعلومات الاستخباراتية. وبالنسبة إلى دولة الحزب الصيني، تسهم البيانات والمعلومات المستمدة من تلك البيانات في كل شيء. فعلى الصعيد المحلي، يبدأ ذلك بحل المشكلات السياسية ليصل إلى التحكم في المعلومات وإكراه الدولة. وعلى الصعيد العالمي، يبدأ ذلك بتوسيع الدور الذي تؤديه جمهورية الصين الشعبية في الاقتصاد العالمي ليصل إلى فهم كيفية تشكيل بيئة التشغيل العالمية والتحكم فيها. وفي القسمين الآتيين، سنشرح بالتفصيل كيف تعمل القوانين والسياسات والإجراءات التي تتبعها دولة الحزب الصيني، التي تنطبق على شركات التكنولوجيا الكائنة في جمهورية الصين الشعبية، على إنشاء نظام بيئي يوفر لها إمكانية الوصول إلى البيانات التي يمكن لتلك الشركات الحصول عليها.

1.1 أهمية الجهات التي تضع المعايير

إنَّ التكنولوجيا ليست حيادية القيمة. فهي تكتسب قيمة من ينشئها. لذا فإن الأهمية تُعزى إلى الجهة التي تضع المعايير، ومن ثَمَّ تحدد اتجاه التكنولوجيا. فنحن نعلم، على سبيل المثال، أن للذكاء الاصطناعي تاريخًا من التحيز العرقي والاجتماعي الاقتصادي الذي يعود إلى مرحلة التصميم، وهو يعكس التحيزات المتأصلة للمصممين وطرق اختيار البيانات المُستخدَمة في خوارزميات تعلم الآلة.[6] لذا يجب تصميم التكنولوجيات بطريقة تجعلها "حيادية القيم"[7] لتجنب هذه المشكلات، لكن هذه الحيادية قد لا تكون واقعيةً على الإطلاق.[8]

إنَّ المجتمعات الديموقراطية الليبرالية لا توافق على المعنى الذي تعنيه "القيم" في هذا السياق. فالاتحاد الأوروبي، على سبيل المثال، يولي أهمية كبيرة لتطوير التكنولوجيا المحلية ليس فقط بسبب المنافسين الإستراتيجيين مثل جمهورية الصين الشعبية، لكن أيضًا بسبب الولايات المتحدة. ويتطلب هذا عادةً الدخول في علاقات معقدة مع شركات التكنولوجيا العملاقة في الولايات المتحدة مثل Google، وApple، وFacebook.[9] يتمثل كذلك جزء من حماية القيم لأي مجتمع ديمقراطي ليبرالي في منع تدخل الليبرالية الداخلية والخارجية على حد السواء. كما يتعلق الأمر بوضع لوائح ومعايير تحمي القواعد والحريات التي تقوم عليها القيم الديموقراطية بشكل أساسي. وعندما يتعلق الأمر بأوروبا والاقتصاد الرقمي، فإن جزءًا كبيرًا من هذا الجهد المبذول يوجَّه حاليًا نحو مساءلة شركات التكنولوجيا الأمريكية.[10]

تقوم دولة الحزب الصيني بإنشاء آليات وهياكل سلطة تُمكِّنها من تحقيق أعلى مستوى من الوصول إلى قواعد البيانات محليًا وعالميًا. ويتجلى هذا بوضوح من خلال وضع جدول أعمالها (المنصوص عليه في وثائق الحزب والسياسة)، وفرض التوقّعات (التي تشير إليها القوانين الجديدة) واستقبال الاتصالات من الحزب الشيوعي الصيني (مثل الخطابات وتقارير وسائل الإعلام التابعة للدولة).

يتمثل جزء من الجهود التي يبذلها الحزب الشيوعي الصيني في محاولات جمهورية الصين الشعبية لوضع المعايير التي تُوجِّه تصميم التكنولوجيات. فعلى سبيل المثال، يلزم تصميم أنظمة التعرف على الوجه في جمهورية الصين الشعبية بطريقة تُمكِّنها من التعرف على "وجوه الإيغور" [11] ومن الأمثلة الأخرى منصات وأنظمة البيانات الضخمة المُصمَّمة لتصنيف الأفراد استنادًا إلى نسخة مُسيَّسة من الأشخاص الذين يرى الحزب الشيوعي الصيني أنهم مشتبه فيهم أو يُشكِّلون مصدر تهديد (مثل مقدمي الالتماس، أو أهل التبت، أو الإيغور، أو ممارسي الفالون غونغ).[12] إذ يجري بالفعل، داخل جمهورية الصين الشعبية، بحث عن التكنولوجيات وتطويرها لتلبية احتياجات دولة الحزب (راجع قسم "قواعد البيانات: وضع المعايير"). وعندما يتم تصدير هذه التكنولوجيات، فإن مستخدمها النهائي لا يستطيع محو مثل هذه الميزات التصميمية، سواء أكان شركة عالمية أم حكومة أجنبية.

1.2 الاستفادة من القيمة الإستراتيجية للبيانات

لقد عمدت دولة الحزب الصيني إلى صياغة إستراتيجية تهدف إلى الاستفادة من القيمة الإستراتيجية للبيانات وقوة المعلومات لتعزيز هيمنة الحزب الشيوعي الصيني على المجتمع. ففي عام 2013، نُقل عن شي جين بينغ قوله إن "البيانات الضخمة هي المورد "المجاني" للمجتمع الصناعي. فكل من يتمتع بحيازة البيانات يتمتع بحق المبادرة ".[13]

في عام 2016، ساعدت الخطة الخمسية الـ 13 للصين على إنشاء "نظام إدارة أمن البيانات الضخمة" جنبًا إلى جنب مع الجهود الرامية إلى تحسين حوكمة الفضاء السيبراني من خلال التوصل إلى اتفاق دولي حول أفكار جمهورية الصين الشعبية بشأن أمن الفضاء السيبراني [14] وتواصل الخطة الخمسية الـ 14، التي تم الكشف عنها في عام 2021، تنفيذ الأولويات ذات الجوانب المتعددة التي تتبناها دولة الحزب في ما يتعلق بتطوير البيانات الضخمة واستخدامها للحوكمة الاقتصادية والاجتماعية، كما تدعو إلى بناء بنية تحتية جديدة للبيانات وتحسين القواعد التي تحكم جمع البيانات وتخزينها واستخدامها.[15]

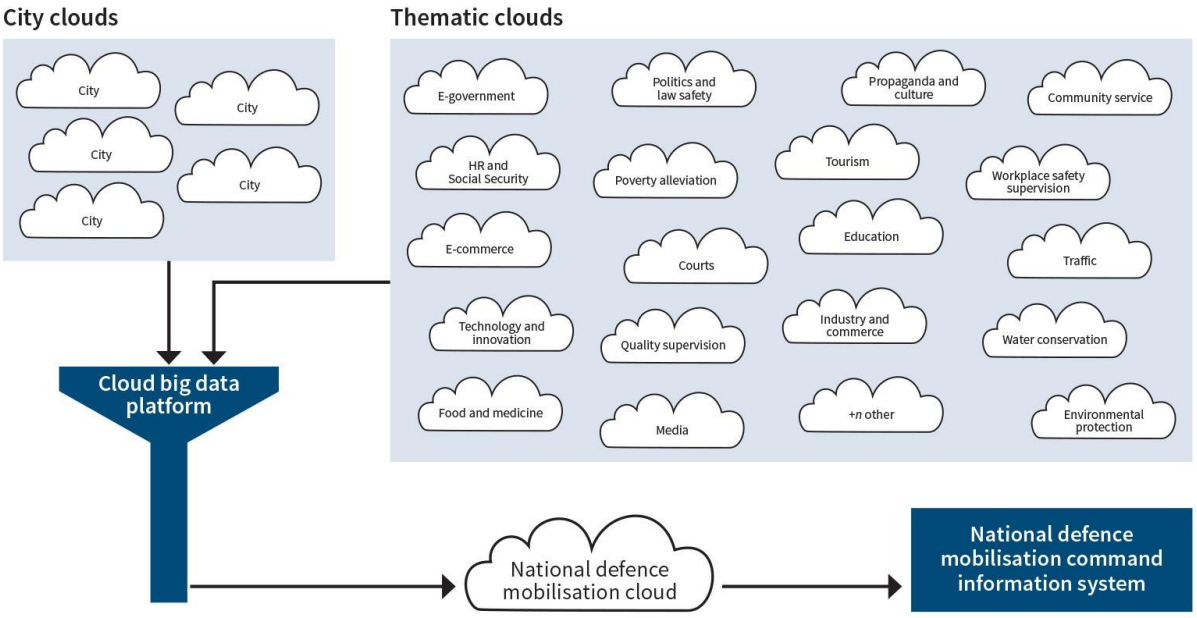
بالإضافة إلى التنمية الاقتصادية، عادةً ما تصف دولة الحزب تكنولوجيات البيانات الضخمة على أنها تسهم في "الإدارة الاجتماعية" (وتُسمى أيضًا "الحوكمة الاجتماعية").[16] وتشمل الإدارة الاجتماعية هذه قائمة واسعة ومتداخلة ببنود جدول الأعمال تبدأ من توفير الإمكانات اللازمة لتحسين إدارة الخدمات العامة لتصل إلى تعزيز "الأمن العام". وفي نهاية المطاف، تشير الإدارة الاجتماعية إلى إدارة دولة الحزب *لنفسها* إلى جانب إدارتها للمجتمع. وتعتمد هذه العملية على تشكيل بيئتها التشغيلية وإدارتها والتحكم فيها من خلال الإمكانات التي تعزز توفير الخدمات والقدرة على إدارة الأخطار.[17]

وتحظى التكنولوجيات الرقمية الجديدة والناشئة باهتمام لأنها تُعد موردًا من شأنه تحسين إمكانية الحوكمة اليومية وتسهيل حل المشكلات. وعند تبسيط عملية توفير الخدمات الحكومية، يمكن أن يُسهّل تطبيق هذه التكنولوجيات في المستقبل عملية الاتصال عبر الأجهزة الحكومية واسعة الانتشار في جمهورية الصين الشعبية [18] والواقع أن التكنولوجيات الرقمية والقائمة على البيانات لها استخدامات متعددة. فعلى سبيل المثال، يمكن لهذه التكنولوجيات المساعدة على تبسيط خدمات الرعاية الحضرية والاجتماعية. ومن نواحٍ أخرى، يمكن لهذه الخدمات نفسها أن تؤثر في تطوير نموذج الحوكمة الشمولي لدولة الحزب والطريقة التي تحدد بها ما تعتقد أنه تهديدات ناشئة والطريقة التي تستجيب بها لهذه التهديدات.

وتُستخدَم البيانات على هذا النحو بطرق توفر التيسير وتتيح التحكم على حد السواء. كما تتشابك الخدمات الروتينية مع أدوات المراقبة والإكراه بطرق غير ممكنة من الناحية القانونية في المجتمعات الديموقراطية الليبرالية، أو يمكن أن تواجه تحديات حقيقية من العامّة ووسائل الإعلام والمجتمع المدني عند حدوثها. ولا ينطبق هذا التمييز ببساطة على الطرق التي تستخدم بها مختلف الإدارات الحكومية في جمهورية الصين الشعبية تكنولوجيات مماثلة (مثل الطرق التي تستخدم بها مكاتب الأمن العام التكنولوجيات في مقابل الطرق التي تستخدمها مكاتب سلامة العمل الصناعي).

من بين الأمثلة على ذلك النتائج التي توصلت إليها منظمة مراقبة حقوق الإنسان بشأن منصة العمليات المشتركة المتكاملة في شينجيانغ، التي تُستخدَم لجمع البيانات بشكل مركزي عن السلوكيات الفردية وتحديد الأشخاص "الذين يشكلون تهديدًا محتملاً". ويُعد أحد المقاييس المُستخدَمة لتحديد التهديدات هو استخدام الطاقة في عدادات الكهرباء الذكية: فيمكن أن يشير الاستخدام المرتفع للطاقة بشكل غير طبيعي إلى نشاط "غير قانوني"، لكن مثل هذه العدادات الذكية قد تحسّن أيضًا دقة قراءات العدادات عند الاستخدام العادي.[19] ومن الأمثلة الأخرى على ذلك بناء مجموعات البيانات لاستخدامها في نظام تعبئة الدفاع الوطني لجمهورية الصين الشعبية (منصة الاستجابة للأزمات) باستخدام البيانات المُستمدة من مجموعة متنوعة من الشبكات السحابية الحكومية، تمتد من المدن الذكية لتصل إلى الشبكات السحابية المتعلقة بالسياحة (الشكل 3).[20]

الشكل 3: مفهوم تعبئة الدفاع الوطني وتكامل بيانات المدن الذكية ومعالجتها



المصدر: رسم توضيحي لمؤلفي معهد ASPI.

على الرغم من الفوائد التي من الممكن أن تجنيها التكنولوجيا، فإن الحزب الشيوعي الصيني يدرك أيضًا مصادر الضرر الناشئة عن التكنولوجيا واستخدامها، كما يدرك أن التكنولوجيا ليست حلاً شاملاً لمشكلاته. وقد وصف شي جين بينغ العلم والتكنولوجيا بأنهما سلاح ذو حدين: "فمن ناحية، يمكن أن يُفيدا المجتمع والشعب. ومن ناحية أخرى، يمكن أن يستخدمهما بعض الأشخاص لإلحاق الضرر بالمصلحة العامة ومصالح الأشخاص".[21] يمكن أن تشمل هذه الأخطار الشركات أو الجهات المسؤولة التي يمكنها استخدام قدر أكبر من السلطة بمساعدة التكنولوجيا.[22] كما يمكن أن تشمل استخدام التكنولوجيا من قِبَل المعارضين السياسيين للحزب الشيوعي الصيني للتنظيم ضد دولة الحزب، سواء من داخل أو خارج جمهورية الصين الشعبية.[23]

1.3 نظرة شاملة

تتوجه كذلك خطط جمهورية الصين الشعبية الرامية إلى الاستفادة من القيمة الإستراتيجية للبيانات وقوة المعلومات لصقل قوة الدولة نحو الصعيد العالمي. وترى دولة الحزب أن اعتمادها على التكنولوجيات الناشئة في الغرب (في الولايات المتحدة على وجه التحديد) يشكل تهديدًا لأمن الدولة، مخافة أن تستغل القوى الأجنبية هذا الاعتماد، خصوصًا في الأزمات.[24] ويساعد هذا الخوف على تطوير الإمكانات التكنولوجية المحلية لدى جمهورية الصين الشعبية.[25] ويشمل الجهد الذي تبذله جمهورية الصين الشعبية في ما يتعلق بهذه الإمكانات التخطيط لتطوير البيانات الضخمة من أجل بناء "نظام بيئي صناعي" يضم "مؤسسات رئيسية ذات توجه عالمي ومؤسسات صغيرة ومتوسطة الحجم مبتكرة ذات ميزات خاصة".[26] ويتضمن أيضًا هذا الجهد التخطيط لتصدير المعايير التكنولوجية الناشئة في جمهورية الصين الشعبية، التي تم تصورها في مشروع China Standards 2035.[27] ويتم تضمين الفوائد والأهداف الاقتصادية في كل خطة، ويخطط الحزب الشيوعي الصيني من خلال هذه الفوائد والأهداف أيضًا لطموحات سياسية محددة.

في إطار رؤيتها العالمية (راجع الشكل 4)، تضمن دولة الحزب الصيني أنها جزء من التوسع المدفوع بقوى السوق ونجاح شركات التكنولوجيا الصينية العملاقة. ففي ظل حكم شي جين بينغ، أظهرت الحكومة على نحو متزايد الحصانة الدبلوماسية الكامنة في مفاهيم أمن الدولة وقوانينها داخل جمهورية الصين الشعبية. فضلاً على ذلك، فإن تمتع الشركات بالحق في مزاولة أعمالها التجارية في الصين وفق تقدير دولة الحزب أصبح أمرًا واضحًا تمامًا. ومن شأن القدرة على الاستفادة من فوائد البيانات أن تساعد على تحقيق الرؤية العالمية للحزب الشيوعي الصيني، حيث يستطيع الحزب، من خلال معالجة تلك البيانات وتطبيقها، تحسين جهوده الرامية إلى تشكيل بيئة التشغيل العالمية الخاصة به وإدارتها والتحكم فيها.

الشكل 4: مثال توضيحي: رؤية دولة الحزب الصيني لجمهورية الصين الشعبية على مستوى العالم

سعت دولة الحزب الصيني منذ تأسيسها إلى عصرنة جمهورية الصين الشعبية بهدف أن تكتسب الثراء والقوة على حد السواء وأن تعود إلى المكانة العالمية التي يعدها الحزب المكانةَ المناسبة للصين [1].

ويمكن وصف طموحات دولة الحزب بأنها تشتمل على ثلاث محاور للجهد الذي تبذله:

1 العصرنة الشاملة لجمهورية الصين الشعبية في ظل حكم دولة الحزب.

2 توحيد المناطق التي تدَّعي دولة الحزب بأنها تقع ضمن حدود "الصين" واستيعابها من الناحية الاقتصادية والاجتماعية والثقافية.

3 التحول إلى قوة عالمية تعمل على تشكيل النظام الدولي والطرق التي تتفاعل بها الدول القومية مع بعضها.

إنَّ "مبادرة الحزام والطريق" التي حظيت برواج شديد في بكين () هي مجرد جزء واحد من رؤية أكبر لـ "نوع جديد من العلاقات الدولية" () و"مجتمع ذي مصير مشترك للبشرية"(). وفي إطار هذه المفاهيم، حددت دولة الحزب رؤية للعلاقات الدولية تشبه إلى حد كبير الطريقة التي تستخدم بها دولة الحزب نفوذها للسيطرة على جمهورية الصين الشعبية والمجتمع الصيني [2]. وفي الواقع، هناك أيضًا صيغة دولية لمفهوم الإدارة الاجتماعية، وقد استُخدمت للإشارة إلى ما يسمى "العجز في الحوكمة الاجتماعية" بسبب عدم فعالية المؤسسات الدولية والنظام الدولي القائم على القواعد [3]. وترى دولة الحزب أن "العجز" في الإدارة الاجتماعية الدولية لم يمنع "الدول الغربية" من امتلاك قوة خطابية قوية [4]؛ ومن ثم، فإن جمهورية الصين الشعبية تحتاج إلى تطوير "قوتها الخطابية"، وهذا المفهوم وصفه المحلِّل ناديغ رولاند بأنه "القدرة على التأثير في الصيغ والأفكار التي يقوم عليها النظام الدولي" [5].

قد يكون التقدم في كل من هذه المحاور متفاوتًا؛ لكن لا يمكن التغاضي عن هذه الأهداف لمجرد أنها تبدو غير قابلة للتحقيق أو لأن النتائج تبدو غير كاملة في الوقت الحالي.

المصادر: رسم توضيحي لمؤلفي معهد ASPI. راجع التعليق الختامي للاطلاع على الاستشهادات التفصيلية.[28]

2. إطار عمل أمن البيانات المتطور لجمهورية الصين الشعبية

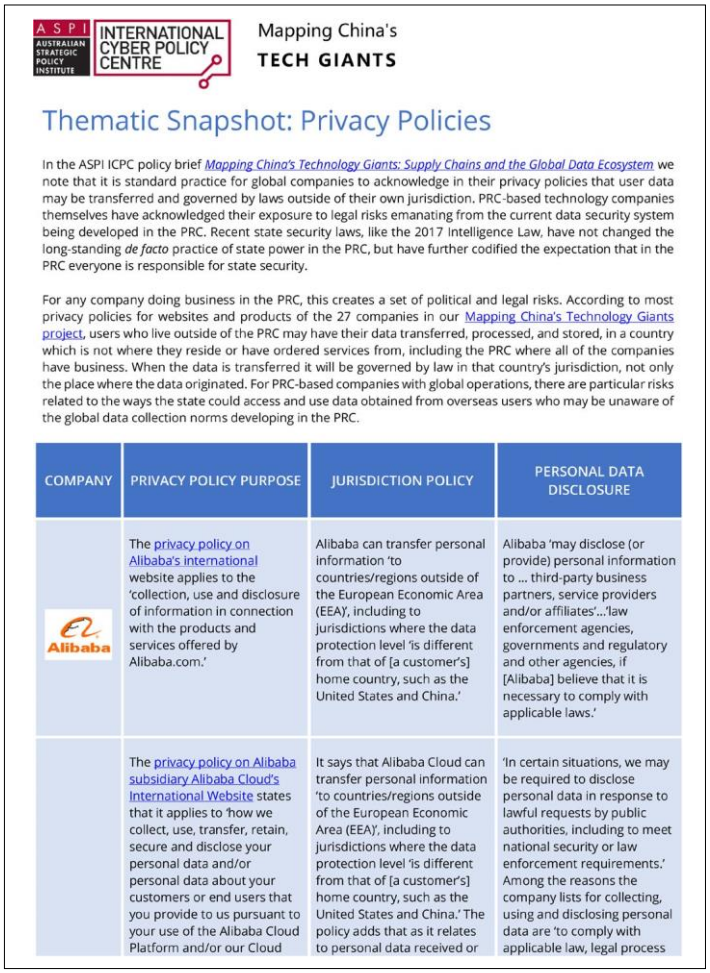
تُسبّب تشريعات جمهورية الصين الشعبية المتعلقة بأمن الدولة[29] إثارة القلق لدى الحكومات الأجنبية بشأن تَعرُّض أي مؤسسة تجارية كائنة في جمهورية الصين الشعبية للمطالب السياسية لدولة الحزب.[30] ولم تُغيّر قوانين أمن الدولة الحديثة، مثل قانون الاستخبارات الصادر عام 2017، ممارسات سلطة الدولة *الفعلية* المعمول بها منذ فترة طويلة في جمهورية الصين الشعبية، لكنها عملت على تقنين توقعات أن يكون كل مواطن في الصين مسؤولاً عن أمن الدولة.[31] وقد ساعدت تقييمات هذه الأخطار على معالجة الأخطار السياسية والقانونية الواضحة الناشئة عن ممارسة الأعمال التجارية مع شركات التكنولوجيا الكائنة في جمهورية الصين الشعبية.

حاول بعض المحلِّلين التقليل من أهمية مثل هذه القوانين من خلال الادعاء بأن القانون في جمهورية الصين الشعبية ليس صحيحًا بشكل مطلق، ومن خلال وصف الامتثال لقوانين جمهورية الصين الشعبية بأنه "قابل للتفاوض".[32] إنَّ حرية المسؤولين في فرض القانون والجهود التي تبذلها الشركات للحفاظ على حرية العمل تترك مجالات مفتوحة تثير الشك في صحتها، لكن الادعاء الوارد أعلاه، في إطار هذا السياق، غير صحيح. وقد يكون القانون في جمهورية الصين الشعبية قابلاً للتفاوض، كما هو الحال في أي مكان آخر، لكن دولة الحزب تقرر ما إذا كان القانون قابلاً للتفاوض على نحو مطلق وتضع حدودًا لهذا التفاوض.

إنَّ دولة الحزب نفسها ليست ملزمة، بشكل حاسم، بالقانون حينما تواجه تحديات أو حينما تتعرض مصالحها للتهديد. ومن الأمثلة الحديثة على ذلك شركة Alibaba ومؤسسها جاك ما الذي اختفى فترةً وجيزة في نهاية عام 2020 عقب انتقاده العلني لموقف الجهات التنظيمية في جمهورية الصين الشعبية إزاء الأعمال التجارية الكبرى، متهمًا إياها بأنها تتعامل بعقلية "الإقراض مقابل الرهن" التي ضيقت الخناق على مجال الابتكار.[33] ففي إبريل/نيسان 2021، تم الإعلان عن فرض غرامات على Alibaba تبلغ 2,8 مليار دولار أمريكي بعد أن أفاد التحقيق أنها أساءت استغلال وضعها في السوق لعدة سنوات.[34] ولا أحد في جمهورية الصين الشعبية أكبر أو أقوى من أن يخضع لمطالب دولة الحزب.[35]

أقرت شركات التكنولوجيا التي تتخذ من جمهورية الصين الشعبية مقرًا لها بتعرضها للأخطار القانونية الناشئة في جمهورية الصين الشعبية. فمن الممارسات المُتبَعة للشركات العالمية الإقرارُ في سياسات الخصوصية الخاصة بهذه الشركات بأنه يمكن نقل بيانات المستخدم وإخضاعها لقوانين خارج نطاق ولايتها القضائية.
وفق معظم سياسات الخصوصية الخاصة بمواقع الويب ومنتجات الـ 27 شركة التي يغطيها مشروع Mapping China Technology Giants، قد يتم نقل بيانات المستخدمين الذين يعيشون خارج جمهورية الصين الشعبية ومعالجتها وتخزينها في دولة لا يقيمون فيها أو لم يطلبوا خدمات منها، أي الدول التي تعمل فيها كل الشركات، بما في ذلك جمهورية الصين الشعبية. عندما يتم نقل البيانات، فستخضع للقانون المعمول به في الولاية القضائية لتلك الدولة، لا القانون المعمول به في المكان الذي نشأت فيه تلك البيانات فحسب (الشكل 5).[36]

الشكل 5: النتائج الجديدة لمشروع *Mapping China's Technology Giants* "لقطات موضوعية"



ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE | INTERNATIONAL CYBER POLICY CENTRE

Mapping China's
TECH GIANTS

Thematic Snapshot: Privacy Policies

In the ASPI ICPC policy brief *Mapping China's Technology Giants: Supply Chains and the Global Data Ecosystem* we note that it is standard practice for global companies to acknowledge in their privacy policies that user data may be transferred and governed by laws outside of their own jurisdiction. PRC-based technology companies themselves have acknowledged their exposure to legal risks emanating from the current data security system being developed in the PRC. Recent state security laws, like the 2017 Intelligence Law, have not changed the long-standing *de facto* practice of state power in the PRC, but have further codified the expectation that in the PRC everyone is responsible for state security.

For any company doing business in the PRC, this creates a set of political and legal risks. According to most privacy policies for websites and products of the 27 companies in our Mapping China's Technology Giants project, users who live outside of the PRC may have their data transferred, processed, and stored, in a country which is not where they reside or have ordered services from, including the PRC where all of the companies have business. When the data is transferred it will be governed by law in that country's jurisdiction, not only the place where the data originated. For PRC-based companies with global operations, there are particular risks related to the ways the state could access and use data obtained from overseas users who may be unaware of the global data collection norms developing in the PRC.

COMPANY	PRIVACY POLICY PURPOSE	JURISDICTION POLICY	PERSONAL DATA DISCLOSURE
Alibaba	The privacy policy on Alibaba's international website applies to the 'collection, use and disclosure of information in connection with the products and services offered by Alibaba.com.'	Alibaba can transfer personal information 'to countries/regions outside of the European Economic Area (EEA)', including to jurisdictions where the data protection level 'is different from that of [a customer's] home country, such as the United States and China.'	Alibaba 'may disclose (or provide) personal information to ... third-party business partners, service providers and/or affiliates'...'law enforcement agencies, governments and regulatory and other agencies, if [Alibaba] believe that it is necessary to comply with applicable laws.'
	The privacy policy on Alibaba subsidiary Alibaba Cloud's International Website states that it applies to 'how we collect, use, transfer, retain, secure and disclose your personal data and/or personal data about your customers or end users that you provide to us pursuant to your use of the Alibaba Cloud Platform and/or our Cloud	It says that Alibaba Cloud can transfer personal information 'to countries/regions outside of the European Economic Area (EEA)', including to jurisdictions where the data protection level 'is different from that of [a customer's] home country, such as the United States and China.' The policy adds that as it relates to personal data received or	'In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.' Among the reasons the company lists for collecting, using and disclosing personal data are 'to comply with applicable law, legal process

المصدر: الموقع الإلكتروني لمشروع Mapping China's Technology Giants، عبر الإنترنت.

أوضحت معظم الشركات الـ 27 أنها تلتزم بحماية المعلومات الشخصية، لكنها تقر بأنه قد يُطلب منها الكشف عن البيانات الشخصية لتلبية متطلبات إنفاذ القانون أو أمن الدولة. ويمكن بشكل كبير إضفاء طابع سياسي على التعريف الخاص بما يلبي الحد المسموح لعد القضية قضية أمن وطني أو قضية جنائية في جمهورية الصين الشعبية، وعملية التعريف هذه ليست مماثلة لتلك التي تحدث في المجتمعات الديموقراطية الليبرالية.

إنَّ النظام السياسي المُتبَع في جمهورية الصين الشعبية هو السبب وراء هذه الأخطار. ويُشكِّل القانون في جمهورية الصين الشعبية في المقام الأول أداة سياسية وحاكمة لإنفاذ السلطة السياسية. ومن المفترض أن يُطبَّق القانون من قِبَل دولة الحزب وأن يعمل على دعم سلطة الدولة وتوسيع نطاقها. ويعتمد تطبيق القانون على قيادة الحزب الشيوعي الصيني حيث يعمل على تعزيز قدرة الحزب على الحكم، لكن سلطته لا تتجاوز سلطة دولة الحزب حتى لو استُخدم لإدارة أعضائه.[37] ومع ذلك، فإن القانون الذي تعمل به سلطة الدولة لا يُعَد أداة غير حادة فحسب. ومن المهم التفكير في العواقب المترتبة على حقيقة أن القانون يُستخدم أيضًا كأداة لتحديد توقعات الدولة وتحقيقها من خلال أجهزتها وكياناتها وأفرادها.

تساعد التطورات الجديدة المتصلة بجمع البيانات وتخزينها ونقلها على أن تصبح هذه القضايا أكثر وضوحًا. وتناقش حاليًا دولة الحزب الصيني مشروع قانون أمن البيانات (DSL) ومشروع قانون حماية المعلومات الشخصية (PIPL).[38] ففي إبريل/نيسان 2021، صدرت نسخ المشروع الثاني بشكل علني (راجع ملحق هذا التقرير للاطلاع على الترجمات الخاصة بمواد مشروعات القوانين التي نركز عليها في هذا القسم). ومن المتوقع سن قانونَي كلا المشروعين في عام 2021. ومن المتوقع كذلك مناقشة النسخة الثالثة وربما النهائية من مشروع قانون أمن البيانات في اجتماع اللجنة الدائمة لمجلس الشعب الصيني في الفترة من 7 إلى 10 يونيو/حزيران 2021.[39]

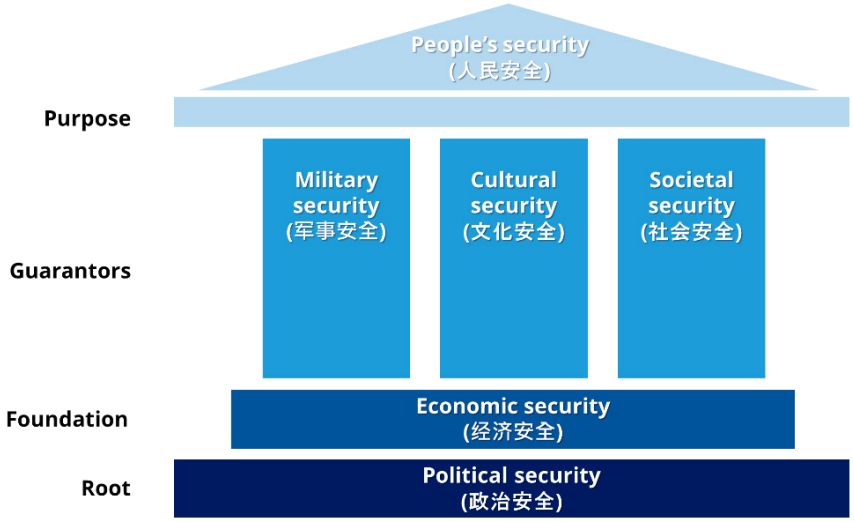
إنَّ هذه القوانين ليست منفصلة عن بقية التشريعات. وينبغي أن تُقرأ جنبًا إلى جنب مع مجموعة من تشريعات أمن الدولة الأخرى ذات الصلة، بما في ذلك على سبيل المثال، قانون أمن الدولة (الصادر عام 2015) وقانون الأمن السيبراني (الصادر عام 2016).

2.1 لوائح البيانات: تقييد الأفراد والمنظمات مع تمكين الدولة

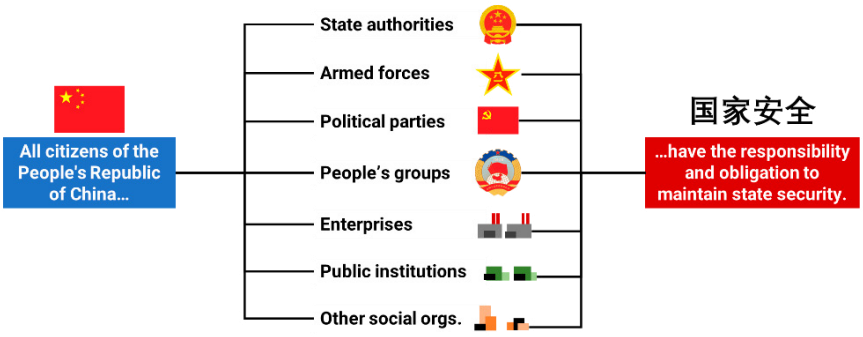
تجب قراءة مشروع قانون أمن البيانات ومشروع قانون حماية المعلومات الشخصية معًا. ويكمن الفرق الرئيسي بينهما في أن مشروع قانون أمن البيانات يحدد مسؤوليات الدولة المتعلقة بإنشاء نظام أمن البيانات وضمان أمن البيانات، في حين يحدد مشروع حماية المعلومات الشخصية حدود ومتطلبات حماية المعلومات الشخصية للأفراد والكيانات.[40]

إنَّ الأمر الذي يجعل إطار العمل فريدًا من نوعه، مقارنةً بقوانين أي دولة أخرى تُنظِّم أمن البيانات، هو أن أمن البيانات يشكل جزءًا واضحًا من إستراتيجية أمن دولة الحزب، وهو يتعلق في المقام الأول بحماية احتكار الحزب الشيوعي الصيني للسلطة (الشكل 6). وينص مشروع قانون أمن البيانات على أن الجهود الرامية إلى ضمان أمن البيانات لا بد أن تلتزم بـ "النظرة الشاملة لأمن الدولة" التي تتبناها دولة الحزب.[41]
ينص المشروع على أن الدولة هي الجهة المسؤولة عن قيادة نظام أمن البيانات، مشيرًا إلى أن "الجهاز القيادي المركزي لأمن الدولة" هو "المسؤول عن اتخاذ القرارات بشأن الأعمال المتعلقة بأمن البيانات والتنسيق الشامل لها، وإجراء الأبحاث، وصياغة إستراتيجيات أمن البيانات الوطنية والمبادئ التوجيهية والسياسات الرئيسية ذات الصلة وتوجيه تنفيذها".[42]

الشكل 6: مثال توضيحي: مفهوم أمن الدولة في جمهورية الصين الشعبية



According to the State Security Law (2015), Article 3, 'All state security work shall adhere to the comprehensive state security outlook, regard people's security as the purpose, regard political security as the root, regard economic security as the foundation, regard military, cultural, and social security as the guarantors, [and] regard promoting international security as the dependent to maintain state security in all fields, build a state security system, and walk a path of state security with Chinese characteristics' [1].



According to the State Security Law (2015), Article 11, 'All citizens, state authorities, armed forces, political parties, people's groups, enterprises, public institutions, and other social organisations of the People's Republic of China shall have the responsibility and obligation to maintain state security ...' [2].

الشكل 6 (تابع): مثال توضيحي: مفهوم أمن الدولة في جمهورية الصين الشعبية

The **comprehensive state security outlook (总体国家安全观)** is the phrase used under Xi Jinping to describe the concept of **state security (国家安全)**. While the phrase is new under Xi Jinping, the state security concept it describes is not; rather, it's part of the fabric of the political system. At the root of the concept is **political security (政治安全)**. It refers to the requirement to guarantee the CCP's leadership authority, and to protect the party-state from political threats that can emerge from *both inside and outside the party and inside and outside the PRC's geographical borders*. The state security concept also includes 'guarantors' such as **cultural security (文化安全)**, which is best summed up as the party-state's version of what is and is not 'China'. It also includes traditional components of national security such as **military security (军事安全)**, although this also carries political weight because the People's Liberation Army is the CCP's army [3].

المصادر: رسم توضيحي لمؤلفي معهد ASPI. راجع التعليق الختامي للاطلاع على الاستشهادات التفصيلية.[43]

لا ينص القانون على أن الكيان الحزبي هو المسؤول فحسب، بل ينص أيضًا على حقه في وضع أي سياسات مهمة. ويترادف مصطلح "الجهاز القيادي المركزي لأمن الدولة" المنصوص عليه في الوثائق القانونية مع مصطلح اللجنة المركزية لأمن الدولة، وهي هيئة تابعة للحزب الشيوعي الصيني بقيادة شي جين بينغ.[44] وعليه، فإن نشاط الإدارات التنظيمية الحكومية الأخرى وأجهزة الأمن العامة وأجهزة أمن الدولة المعنية ببذل الجهود المتعلقة بأمن البيانات سيعتمد على عملية اتخاذ القرار والإستراتيجية التي تُكلَّف اللجنة المركزية لأمن الدولة بالإشراف عليها وتطبيقها.[45]

ينطبق كذلك مشروع قانون أمن البيانات على أنشطة معالجة البيانات التي تتم "خارج أراضي جمهورية الصين الشعبية"، وإذا نُظر إلى هذه الأنشطة على أنها "تضر بأمن الدولة، أو المصلحة العامة، أو الحقوق والمصالح المشروعة للمواطنين ومنظمات جمهورية الصين الشعبية"، فتجب متابعتها لغرض المسؤولية القانونية "وفق القانون". وتوضح القوانين والممارسات المعمول بها التطبيق العالمي لهذه المفاهيم.

يُجرّم قانون الأمن الوطني الجديد في هونغ كونغ، الصادر في عام 2020، "الانفصالية" و"التخريب" و"الإرهاب" و"التواطؤ" بالإضافة إلى دعم أي من تلك الأنشطة من جانب أي شخص، بغض النظر عن المكان الذي تتم فيه هذه الممارسات حول العالم.[46]

من جهة أخرى، يهدف مشروع قانون حماية المعلومات الشخصية إلى تنظيم سلطة الأفراد والكيانات القائمة على معالجة البيانات الشخصية لمواطني جمهورية الصين الشعبية داخل الدولة وخارجها. فهو يعمل على وضع نظام أقوى لحماية خصوصية بيانات الأفراد من الأفراد الآخرين والشركات الأخرى.[47] وينطبق مشروع القانون هذا على الأنشطة التي تتم خارج جمهورية الصين الشعبية التي تشمل معالجة المعلومات الشخصية للأفراد المقيمين داخل أراضي جمهورية الصين الشعبية عندما تقوم الجهات الفاعلة الخارجية بتقديم منتجات أو خدمات إلى هؤلاء الأفراد، ويعمل على تحليل وتقييم سلوك الأفراد المقيمين داخل جمهورية الصين الشعبية أو "الحالات الأخرى المنصوص عليها في القانون أو اللوائح الإدارية". وكما هو الحال في مشروع قانون أمن البيانات، فإن هذا المشروع يترك الباب مفتوحًا أمام إمكانية استخدام القانون للغرض المنشود، وهو حماية سلطة الحزب الشيوعي الصيني حيثما لزم الأمر. وتوضِّح قوانين، مثل قانون الاستخبارات، حالات محددة يمكن فيها استخدام تشريعات أخرى لتبرير هذا الوصول إلى المعلومات، كما يوضح قانون، مثل قانون الأمن القومي في هونغ كونغ، حقيقة أن المعارضين السياسيين لدولة الحزب قد يكونون مستهدفين أيضًا في "حالات أخرى" غامضة.[48]

ينطبق كذلك مشروع قانون حماية المعلومات الشخصية ظاهريًا على الدولة. فعلى سبيل المثال، ينص المشروع على أن أي استرجاع للمعلومات الشخصية يتطلب الخضوع لـ "التزامات منصوص عليها بشكل قانوني"، ويجب الوفاء بهذه الالتزامات "وفق السلطة والإجراءات المنصوص عليها في القوانين".[49] ومع ذلك، تنص المادة 19 من هذا المشروع على ما يأتي:

> عندما يقوم معالجو المعلومات الشخصية بمعالجة المعلومات الشخصية في الحالات التي تنص فيها القوانين واللوائح الإدارية على سرية المعلومات أو عدم وجوب الكشف عنها، فمن المقبول عدم إخطار الفرد.

ومن هذا المنطلق، فإن أي حالة ينطبق عليها قانون الاستخبارات الصادر عام 2017 يمكن عدم إخضاعها لتدابير الحماية الخاصة بقانون حماية المعلومات الشخصية. وتنص المادة 7 من قانون الاستخبارات على ما يأتي:

> يتعين على أي منظمة وأي مواطن، وفق القانون، تقديم الدعم والمساعدة والتعاون في ما يتعلق بأعمال الاستخبارات الوطنية، والحفاظ على سرية أي عمل استخباراتي يصبح معلومًا لديهم.[50]

لذلك، تتمثل أهمية الأمر في أن التكنولوجيا الرقمية يمكن تطبيقها بطرق تعمل على توسيع نطاق الإمكانات المذكورة أعلاه لدولة الحزب، لكن يمكن إدارة الحوكمة الخاصة باستخدامها على نحو يحد من سلطة المسؤولين التقديرية في ما يتعلق بتطبيقها. وهذا لا يعني أن هذه اللوائح تحد من نفوذ دولة الحزب. بل في الواقع تعمل هذه اللوائح على تعزيز نفوذها المطلق على التكنولوجيات الرقمية وتدفق البيانات.

2.2 قواعد البيانات: وضع المعايير

يتضمن مشروعا القانونين توجيهات حول الطريقة التي تتوقع بها دولة الحزب تطوير أنظمة أمن البيانات وخصوصية البيانات. وينص مشروعا القانونين على أنه يجب جمع البيانات وتخزينها ومعالجتها في جمهورية الصين الشعبية على نحو يتفق مع المفاهيم والأهداف الأمنية العليا لدولة الحزب. ونظرًا إلى المفهوم الأمني لدولة الحزب على وجه الخصوص الذي يوجه أمن البيانات، تجدر الإشارة إلى أن شي جين بينغ دعا إلى تعزيز "قيادة الحزب للأعمال المتعلقة بالتوحيد القياسي" ووصف هذا التوحيد بأنه "القيادات العليا" للمنافسة الاقتصادية والتكنولوجية الدولية.[51]

بالإضافة إلى تحديد المؤسسات والجهات المسؤولة عن أمن البيانات، يحدد مشروع قانون أمن البيانات توقعات الطريقة التي سيعمل بها نظام التوحيد القياسي في جمهورية الصين الشعبية في ما يتصل بأمن البيانات على وجه الخصوص. وينص مشروع قانون أمن البيانات على أن الهيئات الإدارية التابعة لمجلس الدولة وغيرها من الهيئات ذات الصلة بمجلس الدولة مسؤولة عن تنظيم "صياغة المعايير المتعلقة بالتكنولوجيا والمنتجات وأمن البيانات ومراجعتها بشكل مناسب من أجل تطوير البيانات واستخدامها".[52] وتُعد هيئة التوحيد القياسي الصينية (SAC) أهم هيئة تابعة لمجلس الدولة، وهي تابعة للإدارة الصينية لتنظيم السوق (SAMR). ووفق قانون التوحيد القياسي المُعدَّل الصادر في عام 2017،[53] يتعين على هيئة التوحيد القياسي الصينية الإشراف على بدء وضع المعايير وتطبيقها. وعلى المستوى العملي، تضع اللجان الفنية معايير يتم اعتمادها بعد ذلك من قِبَل هيئة التوحيد القياسي الصينية.[54]

وتتألف اللجان الفنية التي تعمل على وضع المعايير من أصحاب المصلحة ومعظمهم كيانات حكومية، ومعاهد بحثية ذات صلة بالحكومة، ومؤسسات تجارية. تتمثل عديد من المعايير التي يضعها أصحاب المصلحة هؤلاء في متطلبات إلزامية يتعين على الشركات أيضًا أن تفي بها حتى تتمكن من تقديم عطاءات ناجحة إلى أحد المشروعات التي يتم إطلاقها على المستوى المحلي. وقد أشار التقرير الصادر في مارس/آذار 2021 عن هيئة *PVM*/إلى وثائق مثل "GA/T1400.3—2017" بشأن "أنظمة تطبيق المعلومات المتعلقة بصور الفيديو في مجال الأمن العام" التي أنشأها مكتب تكنولوجيا المعلومات العلمية والتكنولوجية التابع لوزارة الأمن العام بالتنسيق مع العديد من الشركات التي يشملها مشروع *Mapping China's Technology Giants* بما فيها Uniview وHikvision وDahua.[55]

مع وضع المعايير على المستوى المحلي، يُتوقع كذلك وضعها على المستوى العالمي، ليس فقط من خلال أنشطة السوق، بل أيضًا من خلال سعى جمهورية الصين الشعبية إلى المشاركة في وضع معايير التكنولوجيا الدولية وصياغتها. كما أن هيئة التوحيد القياسي الصينية مسؤولة عن تمثيل جمهورية الصين الشعبية ضمن الهيئات الدولية لوضع المعايير.[56] ويتضمن كل من مشروع قانون حماية المعلومات الشخصية ومشروع قانون أمن البيانات أحكامًا تنص على أن الدولة مطالبة بالمشاركة في وضع القواعد والمعايير التكنولوجية الدولية الخاصة بأمن البيانات وحماية المعلومات الشخصية.[57] فالتوقعات واسعة المجال لوضع المعايير هذه تتيح مسارات طبيعية لجمهورية الصين الشعبية لاستغلال مشاركة البيانات في المراحل النهائية بطرق يمكن أن تُضعِف أمن الدول الأخرى، كما سنوضح في القسم أدناه.

3. إعادة النظر في نقاط ضعف سلسلة التوريد الرقمية

لا يلزم أن تكون كل الطرق المُستخدَمة للحصول على البيانات تدخلية أو تخريبية أو سرية أو حتى غير قانونية، بل قد تكون جزءًا من عمليات تبادل بيانات الأعمال العادية. يوضح الشكل 1 (في الصفحة 3) كيفية اختراق سلسلة التوريد الرقمية من دون أي تدخل أو تغيير خبيث. كما أن العلاقات القائمة على مشاركة البيانات التي تحقق مزايا تجارية هي العلاقات نفسها التي يمكن أن تُعرّض المنظمة للاختراق.
فالتفكير في الأخطار من حيث الاضطراب المحتمل وحده يتجاهل الطرق التي تتعرض من خلالها سلسلة التوريد لأخطار تنشأ عن العمليات العادية التي لا يلزم أن تسبب أي اضطراب.

لقد تجلّى ضعف سلاسل التوريد في ظل جائحة كوفيد-19، الأمر الذي زاد من أهمية مرونة سلسلة التوريد. ونظرًا إلى أننا أصبحنا أكثر اتصالاً بعضنا ببعض من الناحية الرقمية، فقد اتسع مجال الأمور التي تُشكِّل خطرًا على سلسلة التوريد لتشمل الأخطار التي تهدد سلسلة التوريد الرقمية المتمثلة في المنتجات الإلكترونية التي نعتمد عليها والبيانات التي تتدفق من خلالها.

عادةً ما تعطي المناقشات حول أمن سلسلة التوريد الرقمية الأولوية لاحتمال حدوث اضطرابات أو تغييرات خبيثة في سلسلة التوريد. ومن الأمثلة على ذلك الهجمات السيبرانية، والمكونات المُغيَّرة المُدرجة في سلسلة التوريد، ومحدودية الوصول إلى الإمدادات الحيوية مثل أشباه الموصلات. ويُعد هذا النوع من الأخطار التي تسببها الجهات الفاعلة التابعة للدولة وغير التابعة لها التي تمتلك موارد جيدة مفهومًا بشكل جيد بالفعل لدى الحكومات التي تضع في حسبانها أمن سلسلة التوريد.[58] وكما أشرنا في قسم "النظام البيئي لبيانات جمهورية الصين الشعبية"، فإن الإمكانات المتطورة التي تتمتع بها جمهورية الصين الشعبية للتعامل مع العمليات الهجومية السيبرانية وقدرتها على الحصول على البيانات من خلال هذه الطرق معروفة أيضًا بشكل جيد. لكن التهديد الذي تتعرض له سلسلة التوريد الرقمية لا يتطلب بالضرورة إجراء تعديلات خبيثة أو عمليات اختراق سيبرانية للشبكة.

يُشكِّل الهجوم الذي تعرضت له سلسلة التوريد الخاصة بشركة SolarWinds في عام 2020 مثالاً على الهجوم السيبراني لسلسلة التوريد الذي يتم ارتكابه من خلال الاقتحام الخبيث للبرامج. ففي تلك الحالة، قامت الجهات التي تشكل تهديدًا، التي كانت على الأرجح من أصل روسي،[59] بخرق خدمة تحديث البرامج لمنصة SolarWinds Orion لتسهيل توزيع التعليمات البرمجية الخبيثة على عملاء Orion.[60]

هناك خطر آخر يهدد سلسلة التوريد في مجال الأمن السيبراني، وهو خطر مخفي عن مرأى الجميع، يتمثل في وضع "الملصقات البيضاء" على منتجات الشركة المُصنِّعة للمعدات الأصلية [61] وهذا ما تعرضت له شركة Honeywell، الموجودة في الولايات المتحدة، حيث خضعت لإجراءات فحص دقيقة في عام 2018 بسبب بيعها كاميرات Dahua تحت علامتها التجارية الخاصة، وتم حظر شركة Dahua في الولايات المتحدة بموجب قانون تفويض الدفاع الوطني.[62] ومن الأمثلة البسيطة على الأخطار التي يتعرض لها العملاء في مثل هذه الحالات أنهم قد يقومون برصد نقاط الضعف المتعلقة بالأمن السيبراني لمنتجات Honeywell، ولا يدركون أنه ينبغي لهم في الواقع رصد نقاط الضعف لمنتجات شركة Dahua الأساسية.

تشمل مجالات المناقشة الأخرى مصداقية البائعين. لقد سلّطت المناقشات التي أُجريت في أستراليا قبل بضع سنوات حول بائعي شبكات الجيل الخامس 5G الضوء على أهمية ملكية البنية التحتية للشبكات والتحكم فيها.[63] وعلى نطاق أوسع، وجهّت هذه المناقشات المنظمات نحو أخطار البائعين الذين ستُنقل بيانات معدات مؤسساتهم، إلى جانب الالتزامات التي يتعين على هؤلاء البائعين الوفاء بها تجاه حكومات "دولهم".[64] ويوجّه مركز الأمن السيبراني الأسترالي ((ACSC، وهو الجهة الأسترالية الرائدة في مجال الأمن السيبراني، المنظمات نحو تحديد أخطار سلسلة التوريد الرقمية، ويلبّي هذه الحاجة لوضع السيطرة والنفوذ والتدخل الأجنبي في الحسبان.[65]

في حين أن هذه المناقشات من المرجح أن تؤدي إلى استجابات سياسية مهمة تعالج بعض نقاط الضعف في سلسلة التوريد الرقمية، فإنها لا تتناول النطاق الكامل للأخطار الموجودة حاليًا. في ما يتعلق بالأمثلة الواردة أعلاه على شركتَي SolarWinds وHoneywell، ينظر المسؤولون المعنيون بضمان الأمن السيبراني عادةً إلى التغييرات التي تحدث في النشاط العادي على أنها مؤشر على وجود مشكلة أو تهديد. وفي ما يتعلق بالحالات التي تحدث فيها الأخطار ضمن عمليات تبادل البيانات القياسية، فيمكن، بناءً على ما سبق، تجنبها بسهولة.

3.1 الوصول إلى البيانات في المراحل النهائية: دراسة حالة شركة GTCOM

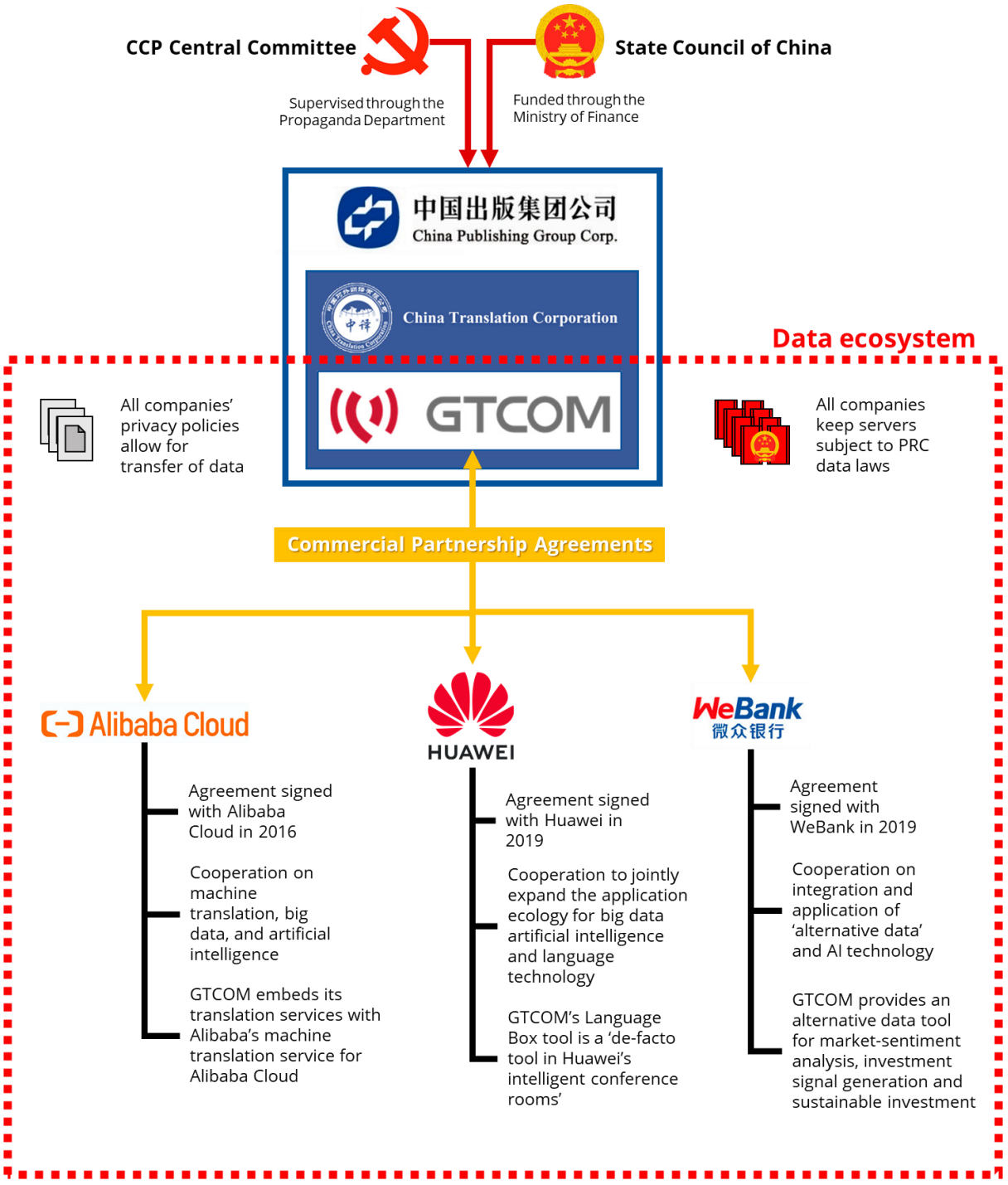
يركز موجز السياسة الخاص بتقرير *Engineering global consent* الذي أعده مركز ICPC التابع لمعهد ASPI على شركةGlobal Tone Communication Technology Co. Ltd، وهي شركة تابعة لمؤسسة مملوكة للدولة تخضع مباشرة لهيئة الدعاية المركزية التابعة للحزب الشيوعي الصيني المخولة بجمع البيانات الضخمة على مستوى العالم دعمًا لأهداف دولة الحزب في مجال الدعاية وأمن الدولة.66 ويشمل النظام البيئي للبيانات الناشئ عن الشراكات التجارية التي تدخلها شركة GTCOM بعضًا من أكبر شركات التكنولوجيا وأهمّها في جمهورية الصين الشعبية. وبالنسبة إلى شركة GTCOM، يوفر التعاون الإستراتيجي مع الشركات المعروفة عالميًا التي تتخذ من جمهورية الصين الشعبية مقرًا لها، وخصوصًا شركتَي Huawei وAlibaba Cloud، المساعدة في مجالين رئيسيين على النحو الآتي:

- إتاحة فرصة لجمع البيانات الضخمة من خلال توفير خدمات الترجمة لكلتا الشركتين، اللتين تتوغلان بشكل كبير في الأسواق.
- تطوير الإمكانات التي تدعم عملية جمع البيانات الضخمة أو تحقيقها.

كما يوضح الشكل رقم 7، تُبرِم شركة GTCOM اتفاقيات شراكة تجارية توفر لها إمكانية الوصول إلى البيانات الضخمة من خلال شركات التكنولوجيا الأخرى الموجودة في جمهورية الصين الشعبية.

يمكن أن تحدث عمليات نقل البيانات من خلال عمليات مُضمنة مباشرة في النظام البيئي. وتقدم إحدى شركات التكنولوجيا مثل GTCOM دراسة حالة مهمة حول الطريقة التي قد يصل بها النظام البيئي إلى البيانات بشكل يتجاوز النظام التنظيمي للبيانات في جمهورية الصين الشعبية.

الشكل 7: شركة GTCOM ومفهوم النظام البيئي العالمي لجمع البيانات



المصادر: رسم توضيحي لمؤلفي معهد ASPI.

3.2 قوة المعالجة

تعطي دولة الحزب الأولوية لجمع البيانات محليًا وعالميًا. وكما ذكرنا أعلاه، تقوم دولة الحزب بإنشاء نظام بيئي يتيح إمكانية الوصول إلى أي بيانات ضخمة من خلال المؤسسات التجارية. كما تدرك أن التكنولوجيا ستتماشى في نهاية المطاف مع أفكارها المتعلقة بمعالجة مخرجات محددة وتوفيرها. فإمكانية جمع البيانات أمر مفيد، لكن إمكانية الوصول إلى البيانات وجمعها لتحليلها واستخلاص رؤى مفيدة منها أمر عظيم.

يعتمد نموذج الأعمال التجارية لشركات الإنترنت العملاقة مثل Facebook وGoogle وByteDance وTencent بشكل كبير على البيانات واستخدام الذكاء الاصطناعي. فهذه الشركات تجمع كميات كبيرة ومتنوعة من البيانات من مستخدمي منصات الخدمات الخاصة بهم. فعلى سبيل المثال، قد يجمعون بيانات مثل بيانات تفضيلات المستخدم على المنصة، والسلوكيات التي يتم إجراؤها على المنصة (مثل المدة التي يستغرقها المستخدم الفردي في التنقل من صفحة إلى أخرى)، ومدة بقاء المستخدم على الصفحة، والمنتجات التي يضعها المستخدم في عربة التسوق الخاصة به، وأصدقاء المستخدم، بالإضافة إلى معلومات العالم الحقيقي مثل مسارات الجري للمستخدم وموقع منزل المستخدم. ثم يتم تجميع البيانات لإنشاء ملفات تعريف للمستخدمين الفرديين لأغراض التسويق والإعلان، وكذلك لتحسين المنصة. ويؤدي هذا بدوره إلى زيادة تفاعل المستخدم ويوفر فرصًا إضافيةً لجمع مزيد من البيانات. كما يتولى وسطاء البيانات مهمة مماثلة في تجميع البيانات وتحليلها، لكنهم عادةً ما يستخدمون البيانات التي قاموا باستخراجها بحرية من الإنترنت أو التي قاموا بشرائها من مصادر أخرى.

ليس بالضرورة أن يكمن القلق في جمع البيانات، بل في القدرة على استنتاج تفاصيل حساسة عن الأفراد من خلال تجميع وحدات بت من البيانات التي تبدو غير ضارة من مجموعة متنوعة من المصادر. ولا تُعد عملية تنسيق موقع جغرافي واحد غير مرتبط بالنشاط المعني ذات أهمية، لكن استخدام بيانات الموقع التي يتم جمعها مع مرور الوقت من هاتف محمول واحد يساعد على تحديد موقع سكن الفرد ومعرفة نمط حياته. فكل المطلوب هو تحديد المواقع الرئيسية الثلاثة التي يوجد فيها الفرد، وهي موقع السكن، وموقع العمل، وأي موقع آخر يذهب إليه باستمرار.

من الممكن استخدام هذا النوع من البيانات لاستهداف الأفراد، مثل تحديد تحركات الرئيس الأمريكي[67] وتتبعها، وتحديد المواقع العسكرية الحساسة *في الوقت نفسه*،[68] ويمكن كذلك استخدامها لتوفير الراحة. وتوفر نتائج بحث Google معلومات عن الأوقات الرائجة وأوقات الانتظار ومدد الزيارة لكل المستخدمين الذين يبحثون عن نشاط تجاري محلي من خلال استخدام "بيانات مجمعة غير محددة الهوية من المستخدمين الذين يستخدمون خدمة سجل المواقع الجغرافية التي يوفرها Google".[69]

يمكن أن يؤدي استخدام تحليلات البيانات الضخمة لمراقبة عمليات المدن الذكية إلى تحقيق نتائج أكثر فعالية للعمليات، وتسهيل مشاركة البيانات، والمساعدة على اتخاذ القرارات، وزيادة الوعي بالأوضاع السائدة بشكل عام. وعلى الرغم من ذلك، فإن وقوع هذه البيانات نفسها في أيدي الخصوم قد يوفر لهم رؤى شاملة كان من الصعب التوصل إليها من دون هذه البيانات. وإذا كانت هذه الأنظمة تخضع لسيطرة الخصوم، فإن المخاوف لا تقتصر على قدرة الآخرين على الوصول إلى البيانات فحسب، بل أيضًا على قدرة الخصوم على التحكم في البيانات أو تعديلها. ونتيجةً لذلك، فإن المعلومات المُستخدَمة لتوفير الراحة وتحسين الكفاءة وزيادة الوعي بالأوضاع السائدة هي المعلومات نفسها التي يمكن أن يستخدمها الخصوم.

لدى بعض شركات التكنولوجيا الكائنة في جمهورية الصين الشعبية إمكانات كافية لمعالجة البيانات الضخمة. وطبقًا للتقارير الواردة في مجلة *Foreign Policy*، فقد تم استخدام هذه الإمكانات من قِبل دولة الحزب لتنفيذ مهام استخباراتية. ووفق ما ذكره "المسؤولون الحاليون والسابقون" المشار إليهم في التقرير، فقد تضمنت هذه المهام الاستحواذ على قواعد بيانات تم الوصول إليها من خلال عمليات اختراق البيانات الكبيرة، مثل عملية الاختراق السيبراني لمكتب إدارة شؤون العاملين في الولايات المتحدة في عام 2014 [70] وتعتقد وكالة الاستخبارات المركزية الأمريكية أن تحليل البيانات الضخمة على هذا النحو هو ما

أدى إلى الكشف عن ضُبَّاطها السريين في إفريقيا وأوروبا.[71] ويتمثل السؤال الذي يتطلب مزيدًا من البحث والتحليل في معرفة السبب وراء اختيار هذه الشركات الموجودة في جمهورية الصين الشعبية. فعلى سبيل المثال، هل تم اختيارها ليس فقط من أجل قدرتها على معالجة البيانات، لكن أيضًا لقدرتها على إثراء المعلومات التي يمكن أن تُستمد من البيانات من خلال استيعاب مجموعات البيانات ودمج البيانات مع ممتلكاتها الخاصة؟

إنَّ الشركات التجارية ليست الكيانات الوحيدة التي تقوم بمعالجة البيانات على نطاق واسع في جمهورية الصين الشعبية. إذ تقوم دولة الحزب بذلك أيضًا على المستوى الوطني. ولقد ضم بنك الشعب الصيني "مركز تحليل البيانات الضخمة" بوصفه جزءًا من تصميم نظام "العملة الرقمية/المدفوعات الإلكترونية" في جمهورية الصين الشعبية. وأفاد المسؤولون في البنك أن البيانات التي يتم جمعها من خلال النظام ستُستخدم لتحسين سياسة الاقتصاد الكلي. وسيعمل البنك على "تحليل طريقة استخدام الأموال وتحويلها وتخزينها، ودعم التتبع والمراقبة بالاستعانة بالبيانات الدائمة والفورية، وتوفير مدخلات البيانات والتحليل لأغراض السياسة النقدية، والإبلاغ بالاحتيال المالي".[72]

إنَّ الأهداف المرتبطة بتسخير القوة الإستراتيجية للبيانات تُشكِّل امتدادًا طبيعيًا للأهداف المكرَّسة منذ أمد بعيد في وثائق دولة الحزب الرسمية، وتُعد جزءًا لا يتجزأ من السياسات والخطط الاقتصادية التفصيلية التي يتم وضعها لضمان إحراز تقدم في تحقيق هذه الأهداف.[73] ومع ذلك، فإن تطوير دولة الحزب للنظريات والسياسات هي عملية متكررة، وتضمن دائمًا مرحلة اختبار لضمان إحراز التقدم من دون التعرض للعديد من العواقب غير المرغوب فيها.[74] فالسيطرة على سلطة الحزب الشيوعي الصيني أو الحفاظ عليها لا تُعد هدفًا في حد ذاتها، بل إنها مطلب أساسي لتحقيق هذه الأهداف. وستؤدي عمليات جمع البيانات الضخمة وتخزينها ومعالجتها دورًا رئيسيًا متزايدًا في ما يتعلق ببذل هذه الجهود في المستقبل.

4. التوصيات

إنَّ التقييم المناسب للأخطار المرتبطة بممارسة الأعمال التجارية مع شركات التكنولوجيا التي تتخذ من جمهورية الصين الشعبية مقرًا لها، أو الشركات التي تعتمد على تكنولوجياتها في سلاسل التوريد الخاصة بها يتطلب فهمًا للطريقة التي تكشف بها دولة الحزب الصيني عن نياتها. كما يتطلب هذا التقييم فهمًا لتداعيات الوثائق السياسية والقانونية التي تشير إلى الخطوات التي سيتم اتخاذها لتحقيق النتائج المرجوة، بالإضافة إلى تحليل السلوك الفعلي لدولة الحزب (على المستويين المحلي والعالمي) بطبيعة الحال.

نوصي بما يأتي:

1. **استثمار الموارد لفهم الطريقة التي تُكشَف بها نوايا جمهورية الصين الشعبية والحزب الشيوعي الصيني بشكل أفضل من أجل تحديد الأسلوب اللازم لإجراء مناقشة عامة أكثر استنارة من شأنها أن توفر استجابات موجهة نحو المشكلات المحددة.**

   كثيرًا ما يتم وضع افتراضات غير صحيحة بشأن نوايا دولة الحزب. بالإضافة إلى ذلك، غالبًا ما يتم تجاهل النوايا التي يتم الكشف عنها والإشارة إليها من خلال سياسة جمهورية الصين الشعبية والوثائق القانونية أو لا يتم وضعها في السياق الذي تُكشف أو تتم الإشارة إليها فيه (مثل وضعها في سياق سياسي مناسب) أو السياق التي توصف فيه (على سبيل المثال، حسب وجهة نظر الحزب الشيوعي الصيني المتمثلة في أن أمن البيانات يُعد مشكلة تتعلق بأمن الدولة، وفق تعريف دولة الحزب لـ "أمن الدولة").

2. **إعادة تقويم سياسات أمن البيانات وأُطُر الخصوصية لأخذ استخدام الدولة الصينية للبيانات لتعزيز احتكارها السياسي في الحسبان.**

   كثيرًا ما تفترض الشركات والحكومات أن بيانات الحكومات الأخرى ولوائح الخصوصية تشترك معها في الأهداف نفسها التي تسعى إلى تحقيقها. وهذا غير صحيح عندما يتعلق الأمر بدولة الحزب الصيني والشركات التي تتخذ من جمهورية الصين الشعبية مقرًا لها، حتى لو استُخدِمَت المفردات الشائعة نفسها أو كانت بعض الدوافع السياسية متماثلة. ففي جمهورية الصين الشعبية، على النقيض من المجتمعات الديموقراطية الليبرالية، تعمل مفاهيم أمن البيانات والخصوصية
   (بما في ذلك المشروعات التشريعية) على تعزيز سلطة الاحتكار التي تتمتع بها دولة الحزب. ويتعين على الشركات والحكومات أن تدرك هذه الأخطار وأن تعمل على تقويم سياساتها بحيث تضع ذلك في حسبانها.

3. **التعاون مع الدول ذات التفكير المماثل المتعلق بوضع أنظمة لتحسين النُهُج التي تركِّز على الأخطار من أجل تحسين تنظيم عمليات نقل البيانات.**

   يتعين على المنظمات أن تُقيّم قيمة بياناتها، بالإضافة إلى قيمة بيانات أي طرف محتمل في سلسلة التوريد الخاصة بها الذي قد يتمكن من الوصول إليها أو الذي قد يُمنح حق الوصول إليها. ففي عصرنا الذي يشهد حرب المعلومات وحملاتها المضللة عبر منصات وسائل التواصل الاجتماعي، وهي من بين أكبر الأخطار التي تهدد التماسك الاجتماعي، تُعد البيانات التي تعبر عن المشاعر العامة ذات قيمة إستراتيجية مثل البيانات المتعلقة بالأهداف العسكرية الأكثر تقليدية. ولا بد من فهم الأخطار على النحو الذي يتماشى مع مشهد التهديد الحالي الذي يمكن فيه تجميع البيانات غير الضارة بأي طريقة أخرى لتحمل معنى من شأنه أن يقوض مجتمعًا أو أفرادًا.

4. **اتباع نهج متعدد التخصصات لبذل العناية الواجبة.**

   يتعين على الحكومات والشركات التجارية وغيرها من المنظمات أن تعمل على وضع أُطُر عمل لإجراء مراجعات لسلسلة التوريد مع أخذ الدوافع السياسية الخاصة بكل بلد في الحسبان. ولا ينبغي أن يقتصر وضع هذه الأُطُر على تقييم أخطار البائعين التي تؤدي إلى التعرض للأخطار السياسية. وينبغي أن تتضمن هذه الأُطُر أيضًا تحليلاً مفصلاً للجهات الفاعلة في المراحل النهائية التي تتمتع بإمكانية الوصول إلى بيانات البائعين (ولا بد من أن تتضمن تحليلاً لأمور مثل النظام البيئي للبيانات الأوسع نطاقًا الذي تُشكِّل هذه الجهات جزءًا منه والالتزامات التي يفي بها هؤلاء البائعون تجاه حكوماتهم). فاتباع هذا النهج الأكثر شمولاً لبذل العناية الواجبة سيضمن حماية البيانات بطريقة فعالة وشكل أفضل.

الملحق: مشروع قانون أمن البيانات ومشروع قانون حماية المعلومات الشخصية

القانون	المادة	النص
قانون أمن البيانات	2	在中华人民共和国境内开展数据处理活动及其安全监管,适用本法。在中华人民共和国境外开展数据处理活动,损害中华人民共和国国家安全、公共利益或者公民、组织合法权益的,依法追究法律责任。 ينطبق هذا القانون على أنشطة معالجة البيانات والتنظيمات الأمنية التي تتم داخل أراضي جمهورية الصين الشعبية. وفي ما يتعلق بأنشطة معالجة البيانات التي تتم خارج أراضي جمهورية الصين الشعبية والتي تضر بأمن الدولة، أو المصلحة العامة، أو الحقوق والمصالح المشروعة للمواطنين ومنظمات جمهورية الصين الشعبية، فتجب متابعتها لغرض المسؤولية القانونية وفق القانون.
قانون أمن البيانات	4	维护数据安全,应当坚持总体国家安全观,建立健全数据安全治理体系,提高数据安全保障能力。 يجب أن تخضع عملية الحفاظ على أمن البيانات للنظرة الشاملة لأمن الدولة، وأن تعمل على وضع أنظمة حوكمة لأمن البيانات وإكمالها، وأن تعزّز إمكانات ضمان أمن البيانات.
قانون أمن البيانات	5	国家保护个人、组织与数据有关的权益,鼓励数据依法合理有效利用,保障数据依法有序自由流动,促进以数据为关键要素的数字经济发展。 تحمي الدولة حقوق الأفراد والمنظمات ومصالحهما في ما يتعلق بالبيانات، وتشجع الاستخدام القانوني والمناسب والفعال للبيانات، وتضمن التدفق الحر القانوني والمنظّم للبيانات، وتعزز تنمية الاقتصاد الرقمي باستخدام البيانات بوصفها عاملاً رئيسيًا.
قانون أمن البيانات	6	中央国家安全领导机构负责数据安全工作的决策和统筹协调,研究制定、指导实施国家数据安全战略和有关重大方针政策。 إنَّ الجهاز القيادي المركزي لأمن الدولة هو المسؤول عن اتخاذ القرارات بشأن الأعمال المتعلقة بأمن البيانات والتنسيق الشامل لها، وإجراء الأبحاث، وصياغة إستراتيجيات أمن البيانات الوطنية والمبادئ التوجيهية والسياسات الرئيسية ذات الصلة وتوجيه تنفيذها.
قانون أمن البيانات	7	各地区、各部门对本地区、本部门工作中产生、汇总、加工的数据及数据安全负主体责任。工业、电信、交通、金融、自然资源、卫生健康、教育、科技等主管部门承担本行业、本领域数据安全监管职责。公安机关、国家安全机关等依照本法和有关法律、行政法规的规定,在各自职责范围内承担数据安全监管职责。国家网信部门依照本法和有关法律、行政法规的规定,负责统筹协调网络数据安全和相关监管工作。 تتحمل كل منطقة وإدارة المسؤولية الأساسية عن الجهود التي تبذلها هذه المنطقة أو الإدارة في ما يتصل بإنتاج البيانات وتجميعها ومعالجتها، بالإضافة إلى أمن البيانات. وتتولى الإدارات التنظيمية مثل تلك التابعة لقطاعات الصناعة، والاتصالات السلكية واللاسلكية، والاتصالات العامة، والتمويل، والموارد الطبيعية، والصحة، والتعليم، والعلوم، والتكنولوجيا مهام تنظيم أمن البيانات في القطاع التابعة له. كما تتولى أجهزة الأمن العام وأجهزة أمن الدولة وما إلى ذلك مهام تنظيم أمن البيانات في نطاق التزاماتها التي تنص عليها أحكام هذا القانون والقوانين واللوائح الإدارية ذات الصلة. وتتولى إدارات الأمن السيبراني والحوسبة التابعة للدولة مسؤولية التنسيق الشامل لأمن بيانات الشبكة والجهود التنظيمية ذات الصلة وفق هذا القانون والقوانين واللوائح الإدارية ذات الصلة.
قانون أمن البيانات	11	国家积极开展数据领域国际交流与合作,参与数据安全相关国际规则和标准的制定,促进数据跨境安全、自由流动。 تنفذ الدولة بفاعلية عمليات التبادل والتعاون الدولية في مجال البيانات، وتشارك في صياغة القواعد والمعايير الدولية المتصلة بأمن البيانات، وتعزز التدفق الآمن والحر للبيانات عبر الحدود.
قانون أمن البيانات	14	国家实施大数据战略,推进数据基础设施建设,鼓励和支持数据在各行业、各领域的创新应用。县级以上人民政府应当将数字经济发展纳入本级国民经济和社会发展规划,并根据需要制定数字经济发展规划。 تلتزم الدولة بتنفيذ إستراتيجية للبيانات الضخمة، وتعزيز إنشاء البنية التحتية للبيانات، وتشجيع التطبيقات المبتكرة للبيانات ودعمها في كل صناعة ومجال. وتعمل الحكومات على مستوى المقاطعات أو مستوى أوسع على إدراج تنمية الاقتصاد الرقمي في خطط التنمية الاقتصادية والاجتماعية الوطنية لهذا المستوى، وصياغة خطط التنمية للاقتصاد الرقمي حسب الحاجة.
قانون أمن البيانات	15	国家支持数据开发利用和数据安全技术研究,鼓励数据开发利用和数据安全等领域的技术推广和商业创新,培育、发展数据开发利用和数据安全产品和产业体系。 تدعم الدولة الأبحاث في مجال استخدام البيانات وتطويرها وتكنولوجيات أمن البيانات، وتشجع انتشار الابتكارات التجارية في مجالات مثل استخدام البيانات وتطوير أمن البيانات، كما تعزز وتحسّن استخدام البيانات وتطويرها، ومنتجات أمن البيانات، والنظم الصناعية.

القانون	المادة	النص
قانون أمن البيانات	16	国家推进数据开发利用技术和数据安全标准体系建设。国务院标准化行政主管部门和国务院有关部门根据各自的职责,组织制定并适时修订有关数据开发利用技术、产品和数据安全相关标准。国家支持企业、社会团体和教育、科研机构等参与标准制定。 تُعزّز الدولة إنشاء نظام معايير لتطوير البيانات وتكنولوجيات استخدامها وأمن البيانات. وفي نطاق الالتزامات المتعلقة بكل مجال، تقوم الهيئات الإدارية التابعة لمجلس الدولة المعنية بالتوحيد القياسي وغيرها من الهيئات ذات الصلة بمجلس الدولة بتنظيم صياغة المعايير المتعلقة بالتكنولوجيا والمنتجات وأمن البيانات ومراجعتها بشكل مناسب من أجل تطوير البيانات واستخدامها. وتدعم الدولة المؤسسات والمجموعات الاجتماعية، والهيئات التعليمية أو البحثية، وما إلى ذلك للمشاركة في صياغة المعايير.
قانون أمن البيانات	19	国家支持高等学校、中等职业学校、科研机构和 企业等开展数据开发利用技术和数据安全相关教育和培训,采取 多种方式培养数据开发利用技术和数据安全专业人才,促进人才 交流。 تدعم الدولة مدارس التعليم العالي، والمدارس المهنية الثانوية، ومعاهد البحث العلمي، والمؤسسات، وما إلى ذلك لتوفير التعليم والتدريب المتعلقَين باستخدام البيانات وتطويرها وأمن البيانات، كما تدعمها لاستخدام أساليب متنوعة لتنمية استخدام البيانات المهنية وتطويرها وتنمية المواهب في مجال أمن البيانات وتشجيع التبادلات المهنية.
قانون أمن البيانات	34	公安机关、国家安全机关因依法维护国家安全或者侦查犯罪的需要调取数据,应当按照国家有关规定,经过严格的批准手续,依法进行,有关组织、个人应当予以配合。 تلتزم أجهزة الأمن العام وأجهزة أمن الدولة التي تقوم باسترجاع البيانات عند الضرورة للحفاظ على أمن الدولة أو التحقيق في الجرائم بشكل قانوني بأحكام الدولة ذات الصلة، وتستكمل إجراءات الاعتماد اللازمة للقيام بذلك وفق القانون، وتتعاون مع المنظمات والأفراد ذوي الصلة لتحقيق ذلك.
قانون أمن البيانات	51	开展涉及国家秘密的数据处理活动,适用 《中华人民共和国保守国家秘密法》等法律、行政法规的规定。 开展涉及个人信息的数据处理活动,应当遵守个人信息保护法律、行政法规的规定。 يُطبَّق قانون جمهورية الصين الشعبية بشأن حماية أسرار الدولة وغيره من القوانين واللوائح الإدارية ذات الصلة على ممارسة أنشطة معالجة البيانات التي تتضمن أسرار الدولة. ويتعين أن تمتثل أنشطة معالجة البيانات التي تتضمن معلومات شخصية للقوانين واللوائح الإدارية المتعلقة بحماية المعلومات الشخصية.
قانون حماية المعلومات الشخصية	3	组织、个人在中华人民共和国境内处理自然人个人信息的活动,适用本法。在中华人民共和国境外处理中华人民共和国境内自然人个人信息的活动,有下列情形之一的,也适用本法: (一)以向境内自然人提供产品或者服务为目的; (二)分析、评估境内自然人的行为; (三)法律、行政法规规定的其他情形。 يُطبَّق هذا القانون على أنشطة المنظمات والأفراد القائمين على معالجة المعلومات الشخصية الخاصة بالأفراد المقيمين داخل أراضي جمهورية الصين الشعبية. كما يطبَّق هذا القانون على الأنشطة التي تتم خارج جمهورية الصين الشعبية والتي تتضمن معالجة المعلومات الشخصية للأفراد المقيمين داخل أراضي جمهورية الصين الشعبية لأي من الأغراض الآتية: (1) توفير المنتجات أو الخدمات للأفراد المقيمين داخل أراضي جمهورية الصين الشعبية. (2) تحليل سلوكيات الأفراد المقيمين داخل أراضي جمهورية الصين الشعبية وتقييمها. (3) الأغراض الأخرى التي ينص عليها القانون أو اللوائح الإدارية.
قانون حماية المعلومات الشخصية	4	个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息,不包括匿名化处理后的信息。个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开等。 المعلومات الشخصية هي أي نوع من المعلومات التي تحدد أو يمكن أن تحدد هوية الأفراد المسجّلين إلكترونيًا أو بوسائل أخرى، لكنها لا تتضمن معلومات غير محددة الهوية. وتشمل عملية معالجة المعلومات الشخصية جمع المعلومات الشخصية وتخزينها واستخدامها ومعالجتها ونقلها وتوفيرها والكشف عنها وما إلى ذلك.
قانون حماية المعلومات الشخصية	12	国家积极参与个人信息保护国际规则的制定,促进个人信息保护方面的国际交流与合作,推动与其他国家、地区、国际组织之间的个人信息保护规则、标准等的互认。 تشارك الدولة بنشاط في صياغة القواعد الدولية المتعلقة بحماية المعلومات الشخصية، وتدعم التبادل والتعاون الدوليين بشأن حماية المعلومات الشخصية، وتعزز الاعتراف المتبادل بالقواعد والمعايير لحماية المعلومات الشخصية بين الدول والمناطق والمنظمات الدولية الأخرى.

القانون	المادة	النص
قانون حماية المعلومات الشخصية	19	个人信息处理者处理个人信息,有法律、行政法规规定应当保密或者不需要告知的情形的,可以不向个人告知前条规定的事项。紧急情况下为保护自然人的生命健康和财产安全无法及时向个人告知的,个人信息处理者应当在紧急情况消除后及时告知。 عندما يقوم معالجو المعلومات الشخصية بمعالجة المعلومات الشخصية في الحالات التي تنص فيها القوانين واللوائح الإدارية على سرية المعلومات أو عدم وجوب الكشف عنها، فمن المقبول عدم إخطار الفرد بالأمور المنصوص عليها في المادة السابقة. وإذا تعذَّر إخطار الفرد في الوقت المناسب لحماية حياته وصحته وسلامة ممتلكاته في حالات الطوارئ، فعلى معالج المعلومات الشخصية إخطار الفرد على الفور بعد انتهاء حالة الطوارئ.
قانون حماية المعلومات الشخصية	34	国家机关为履行法定职责处理个人信息,应当依照法律、行政法规规定的权限、程序进行,不得超出履行法定职责所必需的范围和限度。 تقوم أجهزة الدولة المعنية بمعالجة المعلومات الشخصية من أجل الوفاء بالتزاماتها المقررة قانونًا بمعالجة المعلومات وفق السلطة والإجراءات المنصوص عليها في القوانين واللوائح الإدارية، ويجب عليها ألا تتجاوز النطاق والحدود اللازمة للوفاء بالتزاماتها المنصوص عليها بشكل قانوني.
قانون حماية المعلومات الشخصية	35	国家机关为履行法定职责处理个人信息,应当依照本法规定向个人告知并取得其同意;法律、行政法规规定应当保密,或者告知、取得同意将妨碍国家机关履行法定职责的除外。 تقوم أجهزة الدولة المعنية بمعالجة المعلومات الشخصية من أجل الوفاء بالتزاماتها المقررة قانونًا بإخطار الأفراد والحصول على موافقتهم على النحو المنصوص عليه في هذا القانون، باستثناء الحالات التي تنص فيها القوانين واللوائح الإدارية على سرية المعلومات أو الحالات التي يعرقل فيها الإخطار والحصول على الموافقة الوفاء بالتزامات أجهزة الدولة المنصوص عليها قانونًا.

المراجع

1 مشروع ‘Mapping China’s Tech Giants’ عبر الإنترنت.

2 Samantha Hoffman, *Engineering global consent: the Chinese Communist Party’s data-driven power expansion*, ASPI, Canberra, 14 October 2019، عبر الإنترنت.

3 Hoffman, *Engineering global consent: the Chinese Communist Party’s data-driven power expansion*.

4 ‘Two Chinese hackers working with the Ministry of State Security charged with global computer intrusion campaign targeting intellectual property and confidential business information, including COVID-19 research’, news release, US Department of Justice, 21 July 2020، عبر الإنترنت؛ "Chinese military personnel charged with computer fraud, economic espionage and wire fraud for hacking into credit reporting agency Equifax", news release, US Department of Justice, 10 February 2020، عبر الإنترنت.

5 يوفر نموذج الربط بين الأنظمة المفتوحة معيارًا للأنظمة من أجل الاتصال ببعضها البعض. ويحتوي على عدة طبقات لابد أن تمر البيانات عبرها تبدأ بـ "طبقة التطبيقات" التي يواجهها المستخدم و"الطبقة المادية" التي تُمثِّل الوسيلة المادية لربط الأنظمة ببعضها البعض من أجل تبادل البيانات بينها. وفيما بين هذه الطبقات، توجد الطبقات التي تحدد كيفية تقديم البيانات وتعبئتها وتجميعها من أجل التنقل عبر الشبكة.

6 Rebecca Heilweil, ‘Why algorithms can be racist and sexist’, *Vox*, 18 February 2020، عبر الإنترنت.

7 Jenny Darmody, ‘For smart cities to work, they need to be “neutral and objective”’, *Siliconrepublic*, 12 May 2021، عبر الإنترنت.

8 Karen Hao, ‘This is how AI bias really happens—and why it’s so hard to fix’, *MIT Technology Review*, 4 February 2019، عبر الإنترنت. على سبيل المثال

9 Carla Hobbs, *Europe’s digital sovereignty: from rulemaker to superpower in the age of US–China rivalry*, European Council On Foreign Relations, 30 July 2020، عبر الإنترنت.

10 Adam Satariano, Monika Pronczuk, ‘Europe, overrun by foreign tech giants, wants to grow its own’, *New York Times*, 19 February 2020، عبر الإنترنت.

11 Leo Kelion, ‘Huawei patent mentions use of Uighur-spotting tech’, *BBC*, 13 January 2021، عبر الإنترنت؛ ‘Dahua and Hikvision co-author racial and ethnic PRC police standards’, *IPVM*, 30 March 2021، عبر الإنترنت.

12 "China: Police “big data” systems violate privacy, target dissent", *Human Rights Watch*, 19 November 2017، اقرأ عن "كبار الموظفين" في تقرير عبر الإنترنت.

13 ‘国家大数据战略’ [National Big Data Strategy], *People’s Daily*, 12 November 2015، عبر الإنترنت.

14 "中华人民共和国国民经济和社会发展" [Outline of the 13th Five-Year Plan for the National Economic and Social Development of the People’s Republic of China], *Gov.cn*, 17 March 2016، عبر الإنترنت. راجع الفصل 28، القسم 2 في

15 ‘国家大数据战略’ [Outline of the People’s Republic of China 14th Five-Year Plan for National Economic and Social Development and long-range objectives for 2035], PRC Government, 13 March 2021، عبر الإنترنت.

16 ‘习近平与“十三五”十四大战略——国家大数据战略’ [Co-construction, co-governance, and co-sharing: Summary of Central Committee of the China Association for Promoting Democracy’s key investigations on ‘improving the effectiveness of grassroots governance and promoting harmony and stability of the society’], National Committee of the Chinese People’s Political Consultative Conference, 9 September 2020، عبر الإنترنت؛ ‘民进中央“提升基层治理效能，促进社会和谐稳定”重点考察调研综述——共建 共治 共享’ [Xi Jinping and the fourteen grand strategies of the ‘13th five-year-plan Big Data strategy’], *Xinhua*, 12 November 2015، عبر الإنترنت؛ ‘第四届互联网大数据与社会治理南京智库峰会举行’ [The 4th Internet Big Data and Social Governance Nanjing Think Tank Summit was held], *Xinhua*, 13 November 2020، عبر الإنترنت؛ Fengli Wang, Li Zhang, ‘大数据技术提升社会治理能力’ [Big data technology enhances social governance capabilities], *China Social Science Net*, 10 June 2020، عبر الإنترنت.

17 Samantha Hoffman, ‘Programming China: the Communist Party’s autonomic approach to managing state security’, PhD thesis, University of Nottingham, 29 September 2017.

18 Samantha Hoffman, ‘Grasping power with both hands: social credit, “Service-oriented management” and the mass line, and party control’, *China Brief*, 10 October 2018، عبر الإنترنت. لمزيد من المعلومات عن هذا الموضوع، راجع قسم في

19 ,*Human Rights Watch* ,'Maya Wang, 'China's algorithms of repression: reverse engineering a Xinjiang police mass surveillance app
May 2019، عبر الإنترنت.

20 على سبيل المثال، وصف نظام معلومات قيادة الدفاع الوطني في مقاطعة قويتشو بأنه يعتمد على منصة البيانات الضخمة "Guizhou Cloud"، التي تُوصف بأنها تشمل العشرات من التقسيمات الإدارية على مستوى القطاعات لكل من السحب العادية و"السحب المواضيعية". '国防动员，再不牵手大数据就晚了' National defence mobilisation, it would be too late to hold hands with big data (if not doing it now)] [Company '公司简介'، عبر الإنترنت؛ [Successful cases], Cinasoft '成功案例'، عبر الإنترنت؛ 6 June 2016 ,*Xinhuanet*
introduction], Cinasoft، عبر الإنترنت؛
Guizhou big data think tank platform: boosting government] '贵州大数据智库平台：助推政府管理和社会治理创新' Cheng Miao, Feng Xinyi, 'Hu Xiao, '"云上贵州"平台上线 建设"7+N"多云'، عبر الإنترنت؛ *Xinhuanet*, 19 January 2018 ,management and social governance innovation] 贵州携阿里云造中国"数'، عبر الإنترنت؛ 20 October 2014 ,Guizhou Cloud' platform was launched, constructed '7+n' clouds], *People's Daily*] '据之都
22 December 2014 ,*People's Daily* ,['Guizhou and Alibaba Cloud jointly build China's 'data capital]، عبر الإنترنت.

21 ,*CPC News* ,Analysis of the development of big data from the perspective of state security]] '透析国家安全视野中的大数据发展问题'
9 November 2016، عبر الإنترنت.

22 Nigel Inkster, *China's cyber power*, Routledge, Adelphi, London, for the Institute of International and Strategic Studies, 2016, 24.

23 Take a look a these three cases: young students must tighten the string] '拍案丨看看这三个案例，青年学子可要绷紧国家安全这根弦'
15 April 2021 ,of state security], *Xinhua*، عبر الإنترنت.

24 Committee member: [Our] computer operating systems rely too much on imports,] '委员：电脑操作系统太依赖进口 威胁国家安全'
专家谈XP退休：严重依赖国外技术 中国信息安全形势严'، عبر الإنترنت؛ 10 March 2009 ,threatening national security], *China News*
Experts discuss XP retirement: relying heavily on foreign technology, China's information security situation is severe], *People's Daily*, 8] '峻 April
2014، عبر الإنترنت؛ '人民日报整版讨论：抓住信息化发展的历史机遇'، *People's Daily* ,informatisation development], 12 April 2019، عبر الإنترنت.

25 Taking self-reliance of science and technology as a strategic support for national] '把科技自立自强作为国家发展的战略支撑' Jianguo Hou,
The Central Committee] "中共中央 国务院印发《国家创新驱动发展战略纲要》"، عبر الإنترنت؛ 16 March 2021 ,*Qstheory* ,development]
,['of the Communist Party of China and the State Council issued the 'Outline of the National Strategy of Innovation-Driven Development
Xinhua,
19 May 2016، عبر الإنترنت.

26 راجع "Notice from the State Council on issuing the action outline for promoting the development of big data" لعام 2015، عبر الإنترنت.

27 'Chinese standards going global an unavoidable trend' ,*Global Times* ,28 April 2020، عبر الإنترنت.

28 يتطابق الرقم الوارد بين قوسين مع الاستشهادات المرجعية للمطالبات المدرجة في نص الرسم التوضيحي:
[1] شارك العديد من أفراد الجيل المؤسس لدولة الحزب مع الإصلاحيين والثوريين الآخرين في جمهورية الصين الشعبية رؤية الصين الحديثة في أن تصبح دولة غنية وقوية على السواء. أطلق شي جين بينغ *Wealth and power: China's long march to the twenty-first century*, Random House, 16 July 2013. ,John Delury, Orville Schell راجع على هذا "التطلع الرئيسي" للحزب. حيث صرَّح شي جين بينغ في خطابه الذي ألقاه خلال المؤتمر الـ 19 للحزب الشيوعي أن "التطلع الرئيسي والمهمة الأساسية للحزب الشيوعي الصيني متمثلان في السعي نحو تحقيق السعادة للشعب الصيني وإنعاش الدولة الصينية". راجع Xi Jinping, 'Secure a decisive victory in building a moderately prosperous society in all respects and strive for the great success of socialism with Chinese characteristics for a new era ,*Xinhua* ,'18 October
2017، عبر الإنترنت.
[2] Liza Tobin, 'Xi's vision for ;Samantha Hoffman, *Engineering global consent: the Chinese Communist Party's data-driven power expansion*
،November 2018, 2(1) ,*Texas National Security Review* ,'transforming global governance: a strategic challenge for Washington and its allies
عبر الإنترنت.
[3] Xinhua international commentary: A new key is needed to solve the problem of] '新华国际时评：破解全球治理赤字难题需要新钥匙'
24 January 2019 ,global governance deficit], *Xinhua*، عبر الإنترنت.
[4] Fengrong Zuo, '全球治理中的国际话语权' *China Worker Net*] ،22 November 2019 ,International discourse power in global governance]
عبر الإنترنت.

[5] Nadège Rolland, *China's vision for a new world order* ,NBR special report no. 83, National Bureau of Asian Research, 27 January 2020، عبر الإنترنت.

29 قانون مكافحة التجسس (2014)، وقانون أمن الدولة (2015)، وقانون إدارة المنظمات غير الحكومية الأجنبية (2016)، وقانون الأمن السيبراني (2016)، وقانون الاستخبارات (2017)، وغيرها من القوانين.

30 ويغطي مركز الأمن السيبراني الأسترالي، في توجيهاته للمنظمات لتحديد أخطار سلاسل التوريد في المجال السيبراني، هذا تحت عنوان "السيطرة الأجنبية، والنفوذ، والتدخل".
راجع *Identifying cyber supply chain risks*، Australian Cyber Security Centre, January 2021، عبر الإنترنت؛ Max Smolaks, 'No backdoor, no backdoor … you're a backdoor! ,'Huawei won't spy for China or anyone else, exec tells MPs *The Register*,
11 June 2019، عبر الإنترنت.

31 全民国家'، عبر الإنترنت؛ 11 December 2017 ,Samantha Hoffman, 'China's state security strategy: "Everyone is responsible"', *The Strategist*
People's ,'National State Security Education Day: Do you understand these 20 legal trivia?]] '个法律知识你懂吗？20安全教育日 这
7 April 2017 ,*Liberation Army Daily*، عبر الإنترنت.

32 Samm Sacks, 'Data security and US–China tech entanglement' ,*Lawfare* ,2 April 2020، عبر الإنترنت.

33 Rob Davies, Helen Davidson, 'The strange case of Alibaba's Jack Ma and his three-month vanishing act' ,*The Guardian* ،23 January 2021
عبر الإنترنت.

34 Karishma Vaswani, 'Alibaba accepts record China fine and vows to change' ,*BBC* ,12 April 2021، عبر الإنترنت.

35 'Jack Ma shows why China's tycoons keep quiet' ,*New York Times* ،22 April 2021، عبر الإنترنت.

36 راجع اللقطات الموضوعية (Thematic snapshots) المنشورة على الموقع الإلكتروني لمشروع Mapping China's Technology Giants ضمن قسم "Analysis"
'Thematic snapshot: Privacy policies' covers the publicly available privacy policies for the 27 companies tracked in the project، عبر
الإنترنت.

37 'Xi Jinping's latest key quotes on the rule of law analyse the reasons why senior cadres commit crimes], *CPC News*, 15 February 2019، عبر الإنترنت؛ Yixin Chen, 'Xi Jinping's thought] '习近平法治思想是全面依法治国的行动指南'
on the rule of law is an action guide for comprehensively relying upon the law to rule the country], National People's Congress of the PRC, 14
Relying upon the law to rule the country to build a socialist] '依法治国，建设社会主义法治国家' Jiafu Wang, ،عبر الإنترنت؛ May 2021
country
The leadership of the party is the fundamental] '党的领导是推进全面依法治国的根本保证'، عبر الإنترنت؛ 1997ruled by law], *Public Law*,
坚持党对全面依法治国' Dalin Fu, ،عبر الإنترنت؛ 30 December 2020 ,guarantee for advancing the rule of law comprehensively], *Legal Daily*
13 January 2021 ,Persist in the party's leadership of comprehensively governing the country relying on law], *Qstheory*] '的领导، عبر الإنترنت؛
Guangming ,Correctly understand and handle the relationship between the party and the law]] '正确认识和把握党和法的关系' Qingshan Qu,
Daily, 16 February 2015,
عبر الإنترنت.

38 中华人民共和国数据安全法（草案）（二次审议稿）[Data Security Law of the People's Republic of China (draft) (second deliberation)],
中华人民共和国个人信息保护法 (草案) (二次审议稿), [Personal Information Protection Law of the ؛عبر الإنترنت، April 2021 ,*NPC.gov.cn*

People's Republic of China (draft) (second deliberation)], *NPC.gov.cn*, April 2021، عبر الإنترنت.

39 'China's top legislature schedules standing committee session', *Xinhua*, 26 May 2021، عبر الإنترنت.

40 راجع الملحق: المواد 2، و5، و6، و7، و14، و15، و16، و19 من مشروع قانون أمن البيانات والمادة 3 من مشروع قانون حماية المعلومات الشخصية؛ وراجع أيضًا Chuanying Lu, 'Lu Chuanying: Data security legislation needs to balance the demands of all parties], [鲁传颖：数据安全立法，需平衡好各方诉求], *Global Times*, 27 May 2020، عبر الإنترنت.

41 مشروع قانون أمن البيانات، المادة 4.

42 مشروع قانون أمن البيانات، المادة 6.

43 يتطابق الرقم الوارد بين قوسين مع الاستشهادات المرجعية للمطالبات المدرجة في نص الرسم التوضيحي.

[1] '[中华人民共和国国家安全法], *Gov.cn*, 1 July 2015، عبر الإنترنت.

[2] '[中华人民共和国国家安全法], *Gov.cn*, 1 July 2015، عبر الإنترنت.

[3] يشمل مفهوم "النظرة الشاملة لأمن الدولة" في وقتنا الحالي العديد من الجهات التي تشكل أمن الدولة، بالإضافة إلى تلك الجهات الموضحة في الرسم البياني. وبدلاً من أن تكون النظرة الشاملة لأمن الدولة جديدة من نوعها في عهد شي جين بينغ، فقد برزت من خلال المحادثة التي أجراها الحزب الشيوعي الصيني بشأن قدرته على الاستجابة للتهديدات المتصورة، التي أصبحت متميزة بشكل كبير منذ مذبحة تيانانمين في عام 1989. وبحلول أواخر تسعينيات القرن العشرين وأوائل العقد الأول من القرن الحادي والعشرين، كانت العديد من جهات أمن الدولة التي تشملها "نظرة" شي جين بينغ تُناقَش بالفعل كجزء من أمن الدولة. على سبيل المثال، أوضحت وثيقة 2001 Science of Military Strategy أن "أمن الدولة" هو "مصلحة وطنية" رئيسية و"مجموعة من المواقف السياسية والاقتصادية والعسكرية والثقافية والإعلامية والمتعلقة بالطاقة والبيئة البيولوجية". وأضافت: "بينما لا يزال الأمن التقليدي قائمًا، لا يمكننا أن نهمل التهديد الذي تُشكِّله المجالات الاقتصادية والسياسية والثقافية. فالأمن في المجالات غير التقليدية مثل "الأمن الاقتصادي"، و"الأمن السياسي"، والثقافة وغيرها من المجالات يُعد من العوامل المهمة أيضًا لأمن الدولة". وتتمثل إحدى المراحل الانتقالية في عهد شي جين بينغ في إزالة أي غموض حول فكرة مسؤولية كل فرد وكل كيان عن أمن الدولة. فقد شدّد شي جين بينغ في اليوم السنوي لزيادة الوعي بأمن الدولة الذي انعقد في 15 إبريل/نيسان 2016، على سبيل المثال، على أنه "يجب أن نكون استباقيين، وأن نتخذ الاحتياطات [أي نتفاعل/نتعلم] من الأدلة التي تكشف عن الاتجاهات، ونحل [المشكلات] في بدايتها، ونتخذ الخطوة الأولى، ونأخذ زمام المبادرة، وأن نكون على استعداد للتعامل مع أي شكل من أشكال الصراع والخطر والتحدي، وأن نكون مستعدين بشكل جيد لمواجهة أي نوع من أنواع الصراع [في] [المجالات] الاقتصادية والسياسية والثقافية والمجتمعية والدبلوماسية والعسكرية. وينبغي أن يتحمل كل الأفراد وكل المستويات مسؤولية [ذلك]". راجع أيضًا '习近平这样谈总体国家安全' Xi Jinping talks about comprehensive state security], *Science and Technology Daily*, 11 April 2020، عبر الإنترنت؛ Dazhi Yang, 'Political security is the foundation of state security], *Qstheory*, 20 April 2018، عبر الإنترنت؛ Xiaofeng Yan, 'The people's security is the cornerstone of state security], *PLA Daily*, 12 June 2020، عبر الإنترنت.

[4] Andrew S Erickson, Adam P Liff, 'Installing a safety on the "loaded gun"? China's institutional reforms, National Security Commission and Sino-Japanese crisis (in)stability', *Journal of Contemporary China*, 26 October 2015, 25(98)، عبر الإنترنت؛ Weixing Hu, 'Xi Jinping's "big power diplomacy" and China's Central National Security Commission', *Journal of Contemporary China*, 8 December 2015, 25(98):163–177، عبر الإنترنت؛ David M Lampton, 'Xi Jinping and the National Security Commission: policy coordination and political power', *Journal of Contemporary China*, 18 March 2015, 24(95):759–777، عبر الإنترنت؛ Joel Wuthnow, 'Decoding China's new "National Security Commission"', *CNA Brief*, November 2013، عبر الإنترنت؛ Joel Wuthnow, 'China's much-heralded NSC has disappeared', *Foreign Policy*, 30 June 2016، عبر الإنترنت.

[5] '林铎在省委国家安全委员会第一次会议上强调全面贯彻落实总体国家安全观 努力推动国家安全工作上台阶唐仁健出席' Lin Duo emphasised at the first meeting of the State Security Committee of the Provincial Party Committee to fully implement the overall state security concept and strive to promote state security work, Tang Renjian attended], *Gansu Daily*, 29 December 2018، عبر الإنترنت؛ '河南省级机构改革：' Henan Provincial Institutional Reform: Set up 18 party committees and 42 government agencies], *Sina News*, 6 November 2018، عبر الإنترنت.

[6] '这20个法律知识你懂吗？20全民国家安全教育日 National State Security Education Day: Do you understand these 20 legal trivia?], *People's Liberation Army Daily*, 7 April 2017، عبر الإنترنت؛ '中共中央印发《中国共产党政法工作条例》' The Central Committee of the Communist Party of China issued the 'Regulations on the Political and Legal Work of the Communist Party of China'], *Xinhua*, 18 January 2019، عبر الإنترنت.

[7] Samantha Hoffman, Peter Mattis, 'Managing the power within: China's Central State Security Commission', *War on the Rocks*, 18 July 2016، عبر الإنترنت.

44 يُستخدم مصطلح "الجهاز القيادي المركزي لأمن الدولة" (中央国家安全领导机构) في الوثائق القانونية للإشارة إلى اللجنة المركزية لأمن الدولة (中央国家安全委员会) لأن CSSC هي هيئة حزبية. راجع 'Do you understand these 20 legal trivia? 20全民国家安全教育日 这个法律知识你懂吗？' State Security Education Day], *People's Liberation Army Daily*, 7 April 2017، عبر الإنترنت.

45 مشروع قانون أمن البيانات، المادة 7.

46 Dominic Meagher, 'Has Hong Kong's national security law created secret police with Chinese characteristics?', *The Strategist*, 14 July 2020، عبر الإنترنت.

47 مشروع قانون حماية المعلومات الشخصية، المادة 3.

48 William Yang, 'Hong Kong: National security law targets overseas activists', *DW News*, 18 August 2020، عبر الإنترنت.

49 مشروع قانون حماية المعلومات الشخصية، المادة 34، راجع أيضًا المادة 35 بشأن متطلبات الإخطار.

50 'Data security business advisory: Risks and considerations for businesses using data services and equipment from firms linked to the People's Republic of China', US Department of Homeland Security, 22 December 2020، عبر الإنترنت.

51 '学习贯彻习近平同志关于标准化工作的重要论述——开创我国标准化事业新局面' [Create a new situation in China's standardisation business—study and implement Comrade Xi Jinping's important exposition on standardisation], *People's Daily*, 6 September 2015، عبر الإنترنت.

52 مشروع قانون أمن البيانات، المادة 16.

53 'Standardisation Law of the People's Republic of China', Standardisation Administration of China, 23 March 2018، عبر الإنترنت. تم تعديل قانون التوحيد القياسي واعتماده في اجتماع اللجنة الدائمة لمجلس الشعب الصيني الذي عُقد في نوفمبر/تشرين الثاني 2017، وتم بدء العمل به في 1 يناير/كانون الثاني 2018.

54 'China—Standards for trade', *Export.gov*, 30 July 2019، عبر الإنترنت.

55 'Dahua and Hikvision co-author racial and ethnic PRC police standards', *IPVM*, 30 March 2021، عبر الإنترنت. راجع أيضًا Samantha Hoffman, 'Double-edged sword: China's sharp power exploitation of emerging technologies', National Endowment for Democracy, April 2021، عبر الإنترنت.

56 '组织机构' [Organisation], Standardisation Administration of China، عبر الإنترنت.

57 مشروع قانون أمن البيانات، المادة 11؛ ومشروع قانون حماية المعلومات الشخصية، المادة 12.

58 على سبيل المثال، راجع تعليقات الرئيس الأمريكي بايدن التي أدلى بها في خطابه المتعلق بتوقيع أمر تنفيذي بشأن أمن سلسلة التوريد: 'Remarks by President Biden at signing of an executive order on supply chains', transcript, The White House, 24 February 2021، عبر الإنترنت.

59 Cyber Security & Infrastructure Security Agency, 'Joint Statement by the Federal Bureau Of Investigation (FBI), the Cybersecurity And Infrastructure Security Agency (CISA), the office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA)', US Government, 5 January 2021؛ Andrew Roth, 'Code deployed in US cyber-attack linked to suspected Russian hackers', *The Guardian*, 11 January 2021، عبر الإنترنت؛ عبر الإنترنت.

60 بلغ عدد المنظمات المعروف أنها قامت بتنزيل التحديثات الخبيثة نحو 18,000 منظمة، لكن من الممكن أن يكون العدد المتضرر أعلى بكثير. وقد استهدفت هذه التحديثات حكومة الولايات المتحدة والشبكات الخاصة والشركات الكبرى مثل Microsoft، التي وصفها مديرها التنفيذي براد سميث، بأنها "الهجوم الأكبر والأكثر تطورًا الذي شهده العالم على الإطلاق".

'Microsoft president :SolarWinds hack was "largest and most sophisticated attack" ever', *Reuters*, 14 February 2021، عبر الإنترنت؛ David E Sanger, Nicole Perlroth, Julian E Barnes, 'As understanding of Russian hacking grows, so does alarm', *New York Times*, 2 January 2021، عبر الإنترنت.

61 تنتج الشركة المُصنِّعة للمعدات الأصلية المنتجات أو المكونات وتبيعها بكميات كبيرة مقابل سعر أرخص إلى شركة أخرى، وتبيعها أحيانًا من دون أن تضع عليها العلامة التجارية الخاصة بها (تضع عليها الملصقات البيضاء). ويمكن بعد ذلك أن تضع الشركة المشترية العلامة التجارية على المنتج. راجع "OEM software", *Looker*, غير مؤرخ، عبر الإنترنت؛ 'Original equipment manufacturer (OEM): introduction, pros & cons', *Intrepidsourcing*, غير مؤرخ، عبر الإنترنت.

62 'Dahua OEM directory', *IPVM*, 5 May 2021، عبر الإنترنت؛ John Honovich, 'Bosch dropping Dahua', *IPVM*, 13 February 2020، عبر الإنترنت؛ 'Honeywell hides selling US Gov banned Chinese video surveillance', *IPVM*, 10 October 2018، عبر الإنترنت؛ Chris Burt, 'Bosch considers dumping Dahua cameras after biometric ethnicity-warning revelations', *Biometric*, 19 February 2021، عبر الإنترنت؛ John Honovich, '3 weeks later, Honeywell still cannot say whether they are vulnerable to Dahua wiretapping [now admits]', *IPVM*, 27 August 2019، عبر الإنترنت.

63 Danielle Cave, Elsa Kania, Tom Uren, Fergus Hanson, Peter Jennings, Michael Shoebridge, Samantha Hoffman, Jessica Clarence, Greg Austin, *Huawei and Australia's 5G network*, ASPI, Canberra, 10 October 2018، عبر الإنترنت.

64 Elsa Kania, 'Danielle Cave, 'Huawei highlights China's expansion dilemma: espionage or profit?', *The Strategist*, 15 June 2018، عبر الإنترنت؛ Samantha Hoffman, 'China's state security strategy: "Much ado about Huawei (Part 2)", *The Strategist*, 28 March 2018، عبر الإنترنت؛ Samantha Hoffman, '"Dangerous love": China's all-encompassing security vision', *The National Interest*, 17 May 2016، عبر الإنترنت.

65 *Identifying cyber supply chain risks*, Australian Cyber Security Centre, January 2021، عبر الإنترنت.

66 Hoffman, *Engineering global consent: the Chinese Communist Party's data-driven power expansion*.

67 Stuart A Thompson, Charlie Warzel, 'How to track President Trump', *New York Times*, 20 December 2019، عبر الإنترنت.

68 Richard Pérez-Peña, Matthew Rosenberg, 'Strava fitness app can reveal military sites, analysts say', *New York Times*, 29 January 2018، عبر الإنترنت.

69 'Popular times, wait times, and visit duration', *Google My Business Help*، عبر الإنترنت.

70 Zach Dorfman, 'How China's tech giants are giving China a vital edge in espionage', *Foreign Policy*, 23 December 2020، عبر الإنترنت.

71 Zach Dorfman, 'China used stolen data to expose CIA operatives in Africa and Europe', *Foreign Policy*, 21 December 2020، عبر الإنترنت.

72 Samantha Hoffman, John Garnaut, Kayla Izenman, Matthew Johnson, Alexandra Pascoe, Fergus Ryan, Elise Thomas, *The flipside of China's central bank digital currency*, ASPI, Canberra, 14 October 2020، عبر الإنترنت.

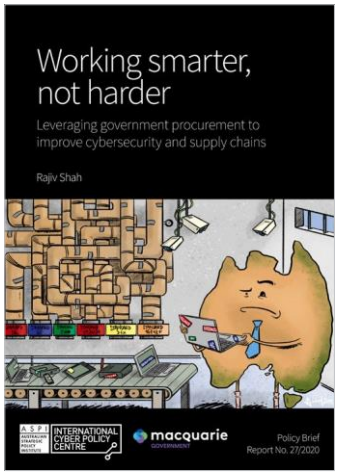
73 Sebastian Heilmann, Oliver Melton, 'The reinvention of development planning in China, 1993–2012', *Modern China*, 24 August 2013، عبر الإنترنت؛ Dan Tobin, *How Xi Jinping's 'New Era' should have ended US debate on Beijing's ambitions*, Center for Strategic and International Studies, 8 May 2020، عبر الإنترنت.

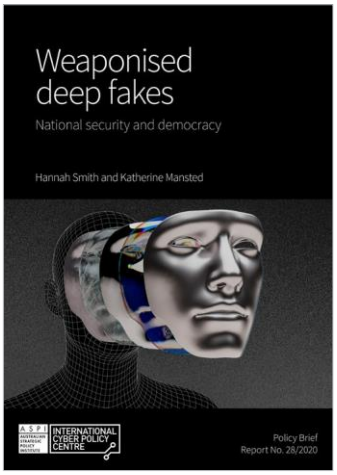
74 Timothy R Heath, *China's new governing party paradigm*, Routledge, 28 February 2019; Sebastian Heilmann, Elizabeth J Perry (eds), *Mao's invisible hand: the political foundations of adaptive governance in China*, Harvard Contemporary China Series 17, Harvard University Press, 1 May 2011.

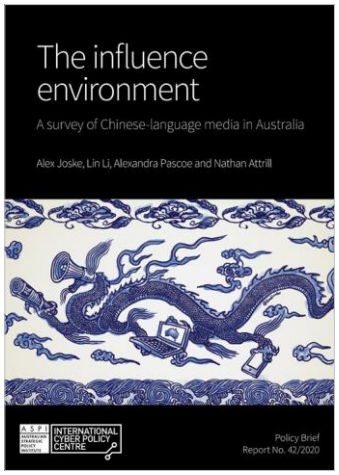
الاختصارات

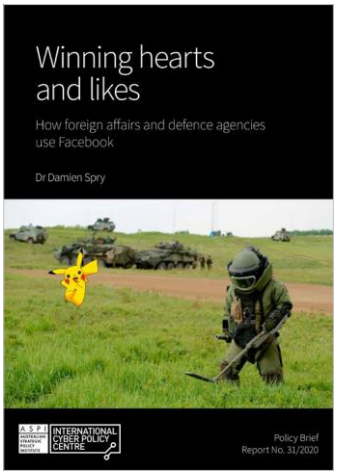
CCP	الحزب الشيوعي الصيني
DSL	قانون أمن بيانات
GTCOM	شركة Global Tone Communication Technology
ICPC Co. Ltd	المركز الدولي للسياسة السيبرانية
OEM	الشركة المُصنِّعة للمعدات الأصلية PIPL
	قانون حماية المعلومات الشخصية PRC
	جمهورية الصين الشعبية
SAC	هيئة التوحيد القياسي الصينية

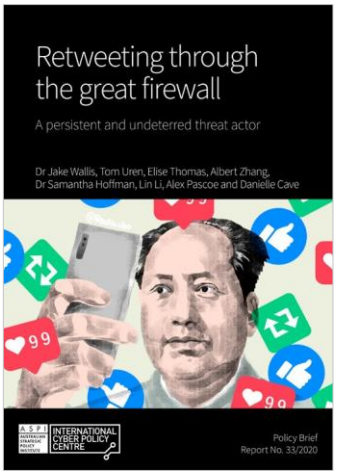
بعض منشورات مركز ICPC السابقة

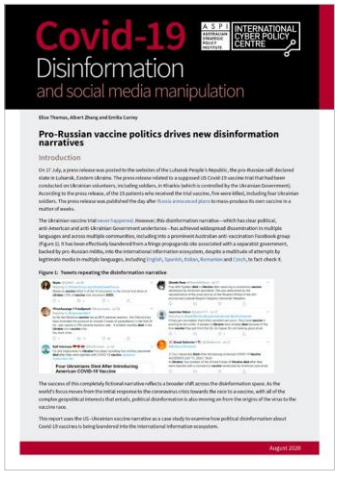


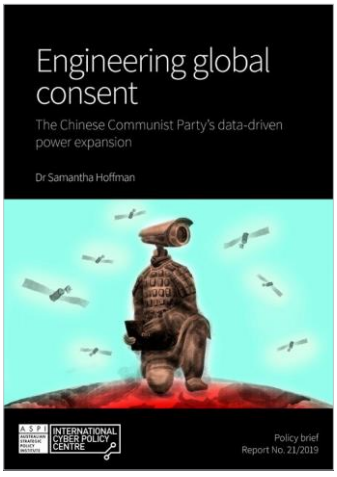


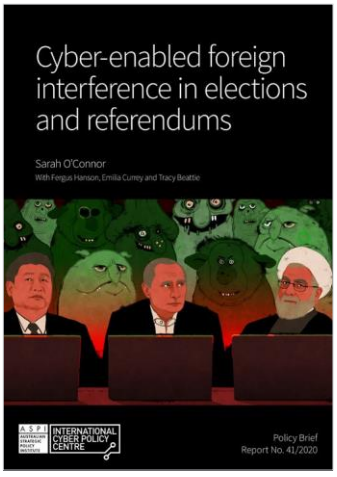












تم ترجمة محتوى ASPI هذا بواسطة SDL، ولا يُعتد إلا بالمحتوى الأصلي باللغة الإنجليزية.

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

TWENTY YEARS OF ASPI STRATEGY 2001 - 2021