التقرير اليومي

2007/5/17

مختارات من الصحف ومراكز الدراسات الدولية

إكتساب التكنولوجيا والتهديد الصيني

بقلم فريد بورتون؛ ستراتفور؛ 2007/5/9

كانت لا تزال هيئة المحلفين التابعة لمحكمة مقاطعة أميركية في سانتا آنا، كاليفورنيا، تقوم بمداولاتها في 9 أيار بخصوص محاكمة تشي ماك، وهو أميركي من أصل صيني، بسبب عمله كعميل للحكومة الصينية وتصدير معلومات عسكرية، وذلك بين تهم أخرى. وتترقب زوجة تشي، أخوه، زوجة أخيه وإبن أخيه المحاكمة المتصلة بالقضية.

إنّ الطبيعة السرية والحساسة جداً للقضايا الجاسوسية، وكذلك الحاجة لحماية المصادر والتكتيكات المستخدمة لإكتشاف عمليات كهذه، تجعل من الصعب إقامة عدوى جرمية ضد الجواسيس المزعومين، حتى عندما تكون الحكومة واثقة من أنّ الفريق المتّهم مذنب. فعلى سبيل المثال، لقد لوحِظَ بأنّ الجاسوس الأميركي المزعوم فيليكس بلوش كان يجتمع مع ضباط من الـ KGB في مقهى باريسي، على الرغم أنه لم يتم مطلقاً إقامة دعوى ضده. أما إقامة دعوى ضد الجواسيس المتّهمين فهو أمر أكثر تعقيداً بكثير في القضايا التي تشمل الحكومة الصينية، المشهورة بصبرها، ومقاربتها الطويلة الأمد لقضايا الجاسوسية. وبسبب هذه العوامل، لم يقم المدّعون الأميركيون بإتهام تشي بالجاسوسية، وإنما بجرائم أقل وكونه عميلاً أجنبياً غير مسجل، وبإنتهاكه قوانين التصدير.

على كل حال، وبصرف النظر عن نتيجة المحاكمة، فإنّ الشهادة والدليل المقدمان في هذه القضية يقدمان نظرة داخلية على الأساليب التي يستخدمها الصينيون في الولايات المتّحدة للحصول على ميزات تكنولوجيا مقتطعة– و على جهود الحكومة الأميركية لمكافحة هذه الأساليب.

مشكلة قديمة

لقد مورست الجاسوسية، التي غالباً ما دُعِيَت بـ"ثاني أقدم مهنة في العالم" منذ بداية التاريخ المعروف. وعلى كل حال، وفي بداية هجمات 9/11 وإطلاق الحرب العالمية على الإرهاب، أعاد جهاز الـ "أف بي آي" توجيه كل ما يقتنيه بخصوص برامج مكافحة الإستخبارات الخارجية (FCI) بإتجاه جهود مكافحة الإرهاب. وهذا كان يعني، ولأول مرة في تاريخ الدائرة، بأنه لم يكن يتم بذل جهود لمكافحة

الإستخبارات تحديداً. وبرغم أنّ نطاق الضرر الذي تسببت به فجوة FCI قد لا يتم تقديرها بالكامل مطلقاً، فإنّ عملية إعتقال عائلة تشي في تشرين الأول 2005 كانت إحدى الإشارات بأنّ بندول الساعة كان قد بدأ يتأرجح بالطريقة الأخرى– أنّ الموارد كان يتم تخصيصها للإنكباب على المشاكل الهائلة للجواسيس الأجانب.

وفي حين أنّ برامج FCI المحدودة للـــ أف بي آي تعتبر تمهيدية ضد جهود الجاسوسية لعشرات البلدان الأجنبية، فلا يوجد بلد يشكّل تهديداً إستخبارياً منتشراً أو أكثر عدائية بالنسبة للولايات المتّحدة من الصين. فالصينيون يستخدمون، بطرق عدة، نسخة الجاسوسية المعدلة لهجمات "الموجة البشرية" التي قاموا بتوظيفها ضد القوات العسكرية الأميركية خلال الحرب الكورية. أما بالنسبة الى حجم الصين وسيطرة الحكومة الشيوعية على المجتمع، فإنّ الصينيين بإمكانهم تكريس قوة بشرية ضخمة وهائلة لجمع المعلومات الإستخبارية. فعلى سبيل المثال، أصدرت الإدارة الأميركية 382,000 تأشيرة دخول غير مخصصة للهجرة، و 37,000 تأشيرة هجرة للمواطنين الصينيين في العام 2006. بالإضافة الى ذلك، كان أكثر من 62,000 طالب صيني يدرسون في الجامعات الأميركية في العام الماضي. ومن المسلّم به أنّ قلة قليلة من هؤلاء كانوا جواسيس، رغم أنّ العدد لا يزال يمثل مجموعة هائلة من المشتبه بهم المحتملين للتدقيق معهم ومراقبتهم، خصوصاً عندما يأخذ المرء بالإعتبار بأنّ هناك ، 12575عميل للـــ "أف بي آي" في الولايات المتّحدة– معظمهم معينون في مهمات غير FCI، كالإرهاب والجريمة المتعلقة بطبقة الموظفين الأنيقين(بحكم الوظيفة).

ولذلك، فإنّ النقطة الجوهرية هي أنه من الصعب تحديد أي واحد من هؤلاء الزائرين المتواجدين في الولايات المتّحدة سيقوم بسرقة الأسرار والتكنولوجيا. وبالواقع، فإنّ كثيراً منهم يعملون بكلا الطاقتين: إنهم طلاب شرعيون "و" جزء من الجهود الإستخبارية. كما أن ليس كل من يجمع المعلومات للحكومة الصينية يدرك أنه يفعل ذلك. فبالدخول في حوارات طبيعية مع الأصدقاء الصينيين أو الأقارب حول كل الأمور، بما في ذلك العمل، فإنّ الشخص العادي بإمكانه تقديم معلومات شديدة الأهمية لهؤلاء الأصدقاء– عملاء الإستخبارات الحقيقيين.

بالإضافة الى ذلك، وفي حالات عدة، فإنّ أنشطة العملاء الصينيين لا تناسب التعريف القانوني للجاسوسية. فالبحث عن مادة مصادر مفتوحة لتكنولوجيا جديدة وناشطة، حضور المؤتمرات التكنولوجية والمعارض التجارية وإستئجار الشركات لإلقاء نظرة على التكنولوجيات الجديدة، كلها أنشطة مشروعة– وتقوم الشركات الأميركية بهذا الأمر طوال الوقت. ومن ثم يعمد بعض العملاء الصينيون الى الدخول في مجال الإستخبارات حول الأعمال أكثر بكثير من مجال التجسس الحقيقي. وعلى كل حال، وبسبب الحدود غير الواضحة بين التكنولوجيا المدنية والحكومية/ العسكرية في الصين، فإنّ المعلومات الملتقطة والمجموعة يمكن أن تجد طريقها بسهولة الى التطبيق العسكرية.

الأسلوب الصيني

إنّ الصينيين مشهورون بسبب صبرهم وأساليبهم التجسسية الثابتة والمستمرة، وبسبب قدراتهم الهندسية التكنولوجية العاكسة. كما أنهم مشهورون بسبب تناولهم رؤية واسعة المدى وبالغة الأثر للغاية لحاجاتهم السياسية والعسكرية وللإستخبارات المطلوبة لتلبيتها. وبسبب ذلك، يشكل الصينيون التهديد الإستخباري الأكبر للتكنولوجيا الأميركية.

إنّ الجهود الهجومية من قِبَل الحكومة الصينية للحصول على تكنولوجيات حساسة، ليست سراً. فعلى سبيل المثال، تصنع وزارة العلوم والتكنولوجيا الصينية قائمة ببرامج إكتساب العلوم والتكنولوجيا كبرنامجها R&D الوطني للتقنية العالية (المعروف ببرنامج 863) على موقعها الإلكتروني الرسمي. ويوفر هذا البرنامج الإرشاد والتمويل للحصول على التكنولوجيا أو تطويرها، والتي سيكون لها "وقع مهم على تعزيز القوة الوطنية الكاملة للصين". إنّ التكنولوجيات المستهدفة تتضمن تلك التي للإستخدام المدني في مجالات مثل تكنولوجيا المعلومات

(IT)، التكنولوجيا الحيوية (تطبيق الهندسة والتكنولوجيا على علوم الحياة)، الزراعة، تصنيع الطاقة، والبيئة. وعلى كل حال، فإنّ عدداً من هذه التكنولوجيات أيضاً لها تطبيقات عسكرية.

وفي حين يدعو برنامج 863 الصينيين للحصول على هذه التكنولوجيات "أو" تطويرها، فإنه من الأرخص والأسرع بكثير الحصول عليها– والصين لديها تاريخ طويل بالقيام بذلك. فعدد كبير من أنظمة السلاح الصيني تم تطويرها إما بسرقة التصميمات والتكنولوجيا، وإما بنسخ تام، ودون أي تحفظ، للنظام بأكمله. وبالإضافة الى نسخ أسلحة صغيرة مثل AK-47 و RPG-7، ومسدس Makarov، قامت المصانع العسكرية الصينية بهندسة عسكرية عاكسة لطائرة مقاتلة. فالمقاتلة Chengdu F-7، على سبيل المثال، هي نسخة عن ميغ– 21 الروسية. فهذا البرنامج التكنولوجي المتقدم يُقصد منه ليس فقط سد الثغرة التكنولوجية للصين مع الغرب، وإنما القفز من فوق ظهره الى الأمام.

ومن ثم، وللحصول على تكنولوجيات حساسة، فإنّ الصينيين لا يعتمدون فقط على التجسس التقليدي، وإنما على جمع المعلومات الضرورية عن طريق مصادر مفتوحة وعلنية. فهذاالجمع من مصادر مفتوحة تعتبر أسرع وأسهل من الدخول في الجاسوسية– كما أنها مشروعة.

وبتأثير ذلك، فإنّ الصينيين يقومون بإستغلال إنفتاح نظام الأبحاث والتطور الأميركي (R&D). إنّ إنفتاحاً كهذا يسمح بتطور أسرع للتكنولوجيات في الولايات المتّحدة لأنّ العلماء والمهندسين من مختلف المؤسسات والشركات يمكنهم تقاسم الأفكار، وبذلك يساهمون بأوجه مختلفة بخصوص المفهوم(R&D). وعلى كل حال، فإنّ الإنفتاح يجعل من السهل، أيضاً، بالنسبة للآخرين القيام بـــ "إستراق السمع" حول المحادثات التكنولوجية الجارية.

وتقوم دول أخرى، بما فيها إسرائيل، فرنسا، الهند وكوريا الجنوبية، بالشيء نفسه، رغم أنه لم يسبق أن شابه أي بلد الصين بمقدار الجهود والموارد المكرسة لهذه العملية. وللحصول على التكنولوجيا المرغوبة والمطلوبة، تقوم الصين بإرسال الطلاب والباحثين للعمل والدراسة في الولايات المتّحدة وفي بلدان صناعية أخرى. ويعود بعض هؤلاء الزائرين الى الصين لاحقاً للعمل في "حدائق حاضنة" للتقنية العالية، حيث تتم عملية الأبحاث والتطوير(R&D). وعلى كل حال، يوجد من بين هذه المجموعة ضباط إستخبارات مُرسلون لسرقة تكنولوجيات حساسة. وتوفر قضية تشي فهماً داخلياً لهذه العملية التي تتم في الولايات المتّحدة. وبحسب الحكومة الأميركية، فقد تم توظيف تشي كمهندس دعم رئيس لـــ Power Paragon، الشركة التابعة لـــ إتصالات L-3/ تكنولوجيا SPD/ مجموعة أنظمة الطاقة في أناهيم بكاليفورنيا. وقد تم منح تشي، الذي ولد في الصين وأصبح مواطناً أميركياً في العام 1985، شهادة براءة ذمة رسمية أمنية من "مستوى سري" في العام 1996، وعمل على أكثر من 200 عقد من العقود الدفاعية والعسكرية الأميركية بصفته مهندساً كهربائياً.

وخلال التحقيق بأنشطة تشي، انجزت الـــ أف بي آي "بحثاً بالقمامة" حوله– وذلك بالتمشيط والبحث في قمامته سعياً وراء دليل– ووجدوا وثيقتين تحتويان على تعليمات لـــ "تشي" لحضور حلقات بحث أكثر وقوائم بالتكنولوجيات التي كان سيحصل عليها. وتم تمزيق القوائم الى قطع صغيرة، إلا أنّ الـــ أف بي آي إستطاع إعادة تجميعها وترجمتها، ومن ثم قام الـــ أف بي آي بأعمال بحث وتقصٍ تحليلي عن إقامة تشي، ووجدوا، على ما قيل، وثائق لعدد من التكنولوجيات الموجودة على قوائم كلا الوثيقتين.

إعادة تعريف "الشركة"

إنّ الجهود المبذولة لجمع التكنولوجيات الحساسة لا يديرها فقط عملاء إستخبارات أفراد، وإنما يديرها أيضاً عدد من الشركات المؤسسة والمسيطر عليها من قِبَل الحكومة الصينية. وإحدى هذه الشركات هي مجموعة Xinshidai Group، التي تم تأسيسها من قِبَل جيش تحرير

الشعب (PLA)، وهي إحدى أكبر شركتين للأجهزة الصناعية العسكرية الصينية. وإحدى شركات التسلح التي تسيطر عليها Xinshidai هي Norinco، المعروفة على نطاق واسع في الولايات المتّحدة بسبب مبيعاتها للأسلحة الخفيفة والذخائر.

وفي حين أنّ هذه الشركات المختلفة الأغراض كـ Xinshidai ليست، رسمياً، جزءاً من الحكومة الصينية، فقد تم تأسيسها لخدمة حاجات PLA والشركات الصناعية العسكرية الصينية، فقط . كما أنّ إحدى الحاجات الهامة للحكومة الصينية هي إكتساب تكنولوجيا الدفاع المتطورة. فعدد من وحدات Xinshidai الثانوية، بما فيها Norinco، والشركات الثانوية المساعدة التابعة لها في الولايات المتّحدة وموظفي هذه الشركات يحضرون المعارض التجارية والمؤتمرات التكنولوجية ويلتقون أيضاً مع ممثلين من شركات أخرى. وبالطبع، ومع معلومات كثيرة متوفرة على الإنترنت، فإنّ كثيراً من المعلومات المتجمعة من المصادر المفتوحة يمكن إنجازها من على مكتب ما في الصين.

ففي أحيان عديدة لا تكون فيها التكنولوجيات السابقة المتصلة بصناعة الدفاع مصنّفة سرية حتى الآن، ولذلك فهي غير محميّة. فهذه التكنولوجيات غالباً ما تصبح مصنفة سرية فقط بعدما تشتريها الحكومة الأميركية. ومن ثم فإنّ المعلومات حول هذه التكنولوجيات الناشئة يمكن الحصول عليها خلال المرحلة الأولى، عندما يتقدم المطورون لهذه التكنولوجيات بطلب الحصول على براءات إختراع أو يبحثون عن رأسمال لمشروع جريء، ولشركاء و/أو زبائن.

إنّ عملية إكتساب التكنولوجيا تعبُر، غالباً، الخط لتصل الى التجسس التقليدي داخل الصين، حيث يقوم ضباط الإستخبارات الصينيين– الذين يعملون دون خوف إقامة دعوى ضدهم– بسرقة وثائق حساسة ، بشكل متكرر، أو نسخ هدف صعب.

وهذا الوضع يعتبر معقداً أكثر عندما يأخذ المرء بالإعتبار بأنّ عدداً من الشركات الكبرى، ومركزها الولايات المتّحدة، تقوم بأعمالها في الصين وتسعى لتوسيع حصة السوق هناك، لديها أيضاً عقوداً مربحة مع وزارة الدفاع الأميركية أو وكالات فيدرالية أخرى. وبعض هذه الشركات تقوم بتخطي الصناعة الصينية، كما تقوم بتأسيس مراكز تطوير Software في البلاد، ما يعني حتى وجوب توفير معلومات تكنولوجية ومملوكة(بحقوق محفوظة) هناك.

إنّ تمدد وتوسع الشركات الأجنبية الى داخل الصين يجلب حشداً من الأهداف المحتملة مباشرة الى أجهزة الإستخبارات الصينية، ما يسمح للصين بتطبيق ضغط أكبر حتى والحصول على نقاط أكثر في سعيها للتكنولوجيا. كما أنّ التقنيات المستخدمة ضد الشركات والمسافرين في الصين يمكن أن تكون أكثر عدائية بكثير من تلك الموظفة ضد أهداف مشابهة في الولايات المتّحدة.

بالإضافة الى التهديد الذي يشكله التجسس للأمن الوطني الأميركي، والسماح للصين بسد ثغرة التكنولوجيا من خلال إكتساب معلومات مملوكة بحقوق محفوظة– بشكل قانوني أو لا– فإنّ ذلك سيؤذي، في النهاية، الشركات الأميركية المتعددة الجنسيات، مع قيام الشركات الصينية بإستخدام المعلومات لتصبح شركات منافسة. وهذا يعني بأنّ الشركات الأميركية الراغبة بأن تبقى منافسة بالعمل في الصين أو بالشراكة مع الشركات الصينية والشركاتهم التابعة لها في الولايات المتّحدة يجب أن تحافظ على مستوى الحذر واليقظة الشديدَيْن.