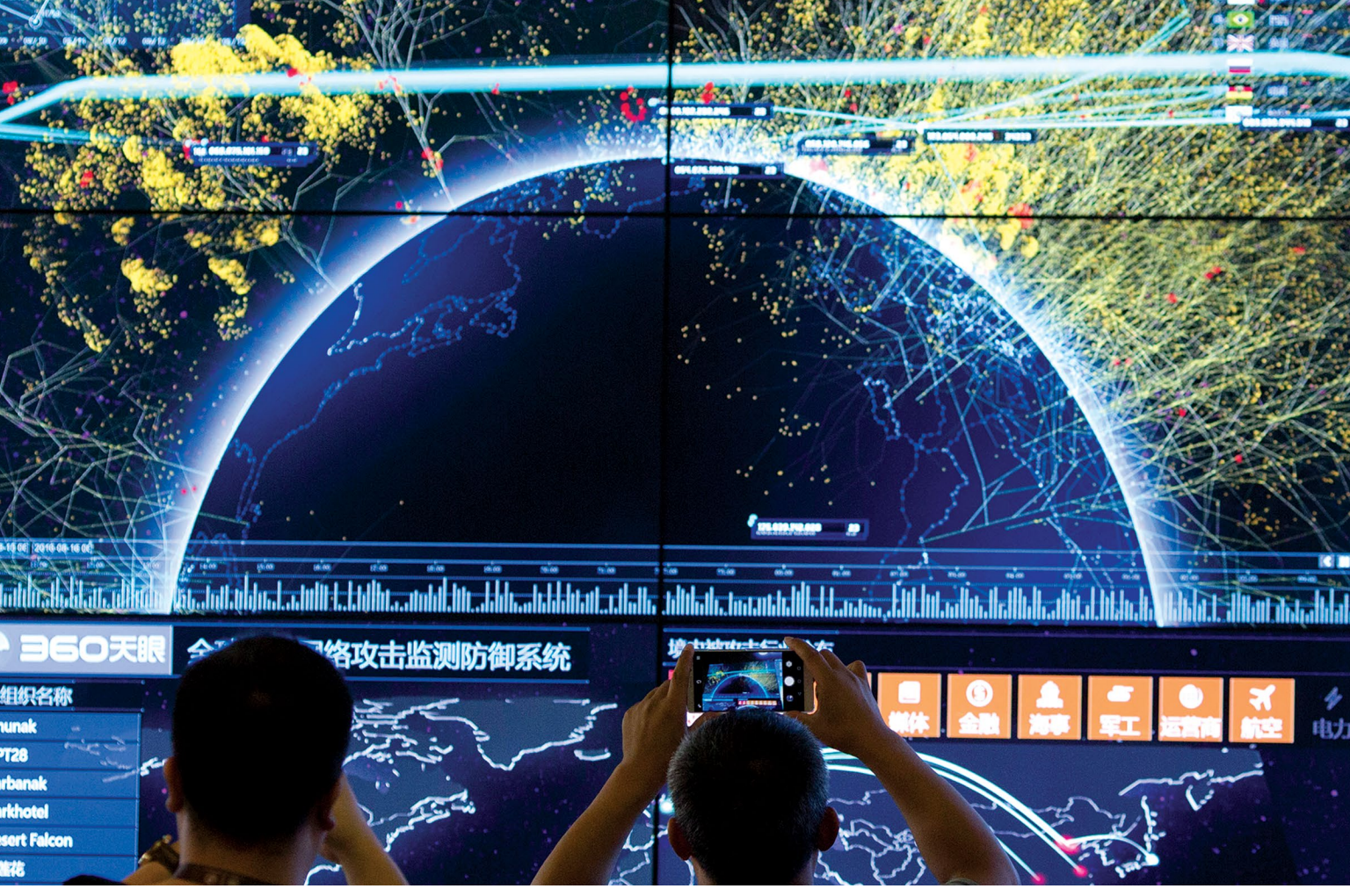


Un asistente a la conferencia fotografía una imagen que muestra los ataques globales a Internet el 16 de agosto de 2016 durante la 4ª Conferencia de Seguridad de Internet de China (ISC) en Pekín. Habiendo alcanzado hoy un nivel de sofisticación que hace que incluso los sistemas de protección de Internet más avanzados sean vulnerables a los continuos ataques de hackers informáticos, el robo en Internet patrocinado por el Gobierno chino de información patentada de todo tipo (por ejemplo, industrial, científica, militar, económica y personal) de Estados Unidos y otras naciones ha alcanzado proporciones pandémicas. (Foto: Ng Han Guan, Associated Press)

Robar la leña de debajo de la olla

El papel del robo de la propiedad intelectual en la estrategia global china

Capitán Scott Tosi, Ejército de EUA

En septiembre de 2015, Estados Unidos y China llegaron a un acuerdo en principio que especificaba, entre otras cosas, que «ni el Gobierno de Estados Unidos ni el de China llevarán a cabo o apoyarán a sabiendas el robo cibernético de propiedad intelectual [PI]»[1]. Sin embargo, menos de dos años después, el uso por parte de China del robo de PI habilitada por el ciberespacio se describió sin rodeos en la Estrategia de Seguridad Nacional de 2017, en la que se afirmaba que «cada año, competidores como China roban propiedad intelectual estadounidense valorada en cientos de miles de millones de dólares»[2]. Este resumen del robo de PI cibernético representa un tema más amplio del robo de PI por parte de China que abarca una amplia gama de métodos y medios. De acuerdo con las estimaciones, la cantidad total anual de robos de PI por China oscila entre 225 000 y 600 000 millones de dólares; además, China es responsable del 50 al 80 por ciento de todos los robos de PI que ocurren contra Estados Unidos[3].

El robo de PI por China tiene amplias implicaciones para el Ejército de EUA y el Departamento de Defensa (DOD), especialmente cuando el enfoque estratégico de EUA cambia de la contrainsurgencia a las operaciones de combate a gran escala entre las grandes potencias[4]. El robo de PI de recursos e investigación y desarrollo del Ejército y el Departamento de Defensa amenaza la superioridad tecnológica militar de EUA en las próximas décadas, ya que China afirma que «mejorará sus capacidades militares», de modo que «a mediados del siglo 21 sus Fuerzas Armadas serán completamente de clase mundial»[5].

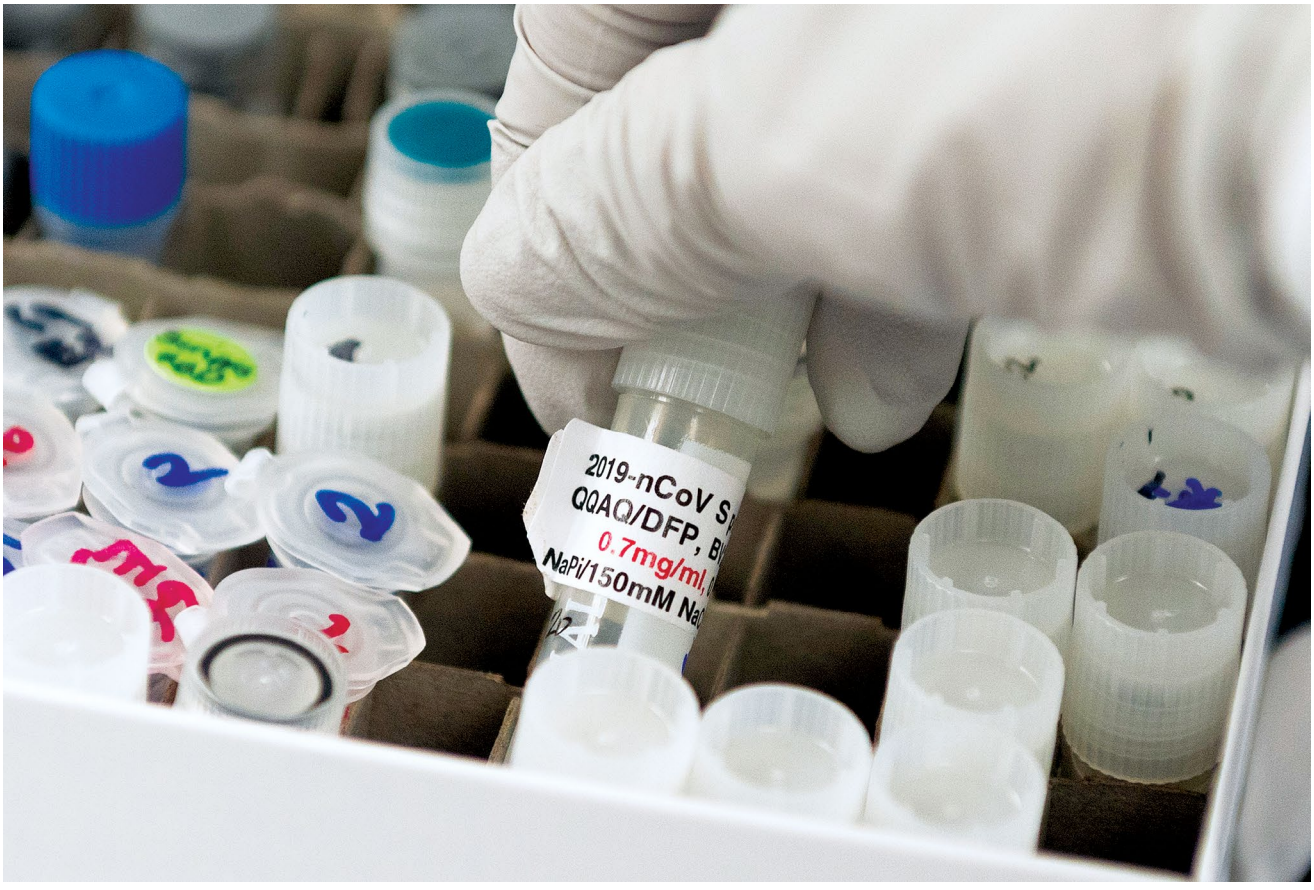
El robo de PI por China al principio: Ocultar nuestras capacidades y esperar el momento oportuno

La explotación sistemática de China de PI extranjero comenzó al principio de su modernización bajo Deng Xiaoping en 1978, cuando implementó las Cuatro Modernizaciones (agricultura, industria, ciencia y tecnología y defensa). Ese mismo año, China obtuvo ayuda económica y tecnológica del Programa de las Naciones Unidas para el Desarrollo y del Banco Mundial, y en el plazo de una década comenzó a enviar millones de estudiantes chinos al extranjero para estudiar.

Las Cuatro Modernizaciones incluyeron dos grandes esfuerzos diseñados para establecer industrias de ciencia y tecnología dentro de China. La primera, el Programa Nacional de Investigación y Desarrollo de Alta Tecnología, procuró hacer hincapié en la ciencia y tecnología en las universidades chinas bajo la dirección de un comité del Gobierno central y el Ejército Popular de Liberación (EPL). El segundo, el Programa Antorcha, buscaba traer de vuelta a miles de académicos chinos entrenados en Occidente[6]. Juntos, estos programas sirvieron como el primer intento del Gobierno para centralizar la investigación y desarrollo de ciencia y tecnología dentro del Partido Comunista de China (PCCh) y el Ejército Popular de Liberación (EPL) a fin de establecer las primeras formas de empresas estatales (SOE) que trabajan junto con el PCCh, el EPL y las empresas privadas extranjeras para adquirir tecnología.

Ya en 1998, el robo por parte de China de PI de EUA se había vuelto lo suficientemente problemático como para justificar el establecimiento del Comité Selecto de la Cámara de Representantes sobre la Seguridad Nacional y Preocupaciones Militares/Comerciales con la República Popular de China. En 1999, el comité publicó un informe en el que se destacaban los esfuerzos realizados por China, ya en la década de 1970, para explotar los laboratorios nacionales de EUA y adquirir tecnología sensible[7]. En el informe también se destacaban los principales medios de adquisición en ese momento: la transferencia ilegal de tecnología de terceros países, la explotación de productos de doble uso, la utilización de empresas ficticias para adquirir ilegalmente la tecnología, la utilización de empresas comerciales como fachada para la adquisición de tecnología y la adquisición de intereses en empresas de tecnología de EUA[8]. Sin embargo, a medida que China entraba en el siglo XXI, buscaba un medio más agresivo de adquisición de tecnología sensible.

El capitán Scott Tosi, Ejército de EUA, es el comandante de la compañía del Cuartel General de la 501ª Brigada de Inteligencia Militar en el Campamento Humphreys, Corea del Sur. Recibió una licenciatura en Historia y Educación en Ciencias Sociales de la Universidad Estatal de Illinois y una MPA de la Universidad de Illinois-Springfield. Sus asignaciones incluyen Yongsan, Corea del Sur; Fort George G. Meade, Maryland y Campamento Lemonnier, Djibouti.



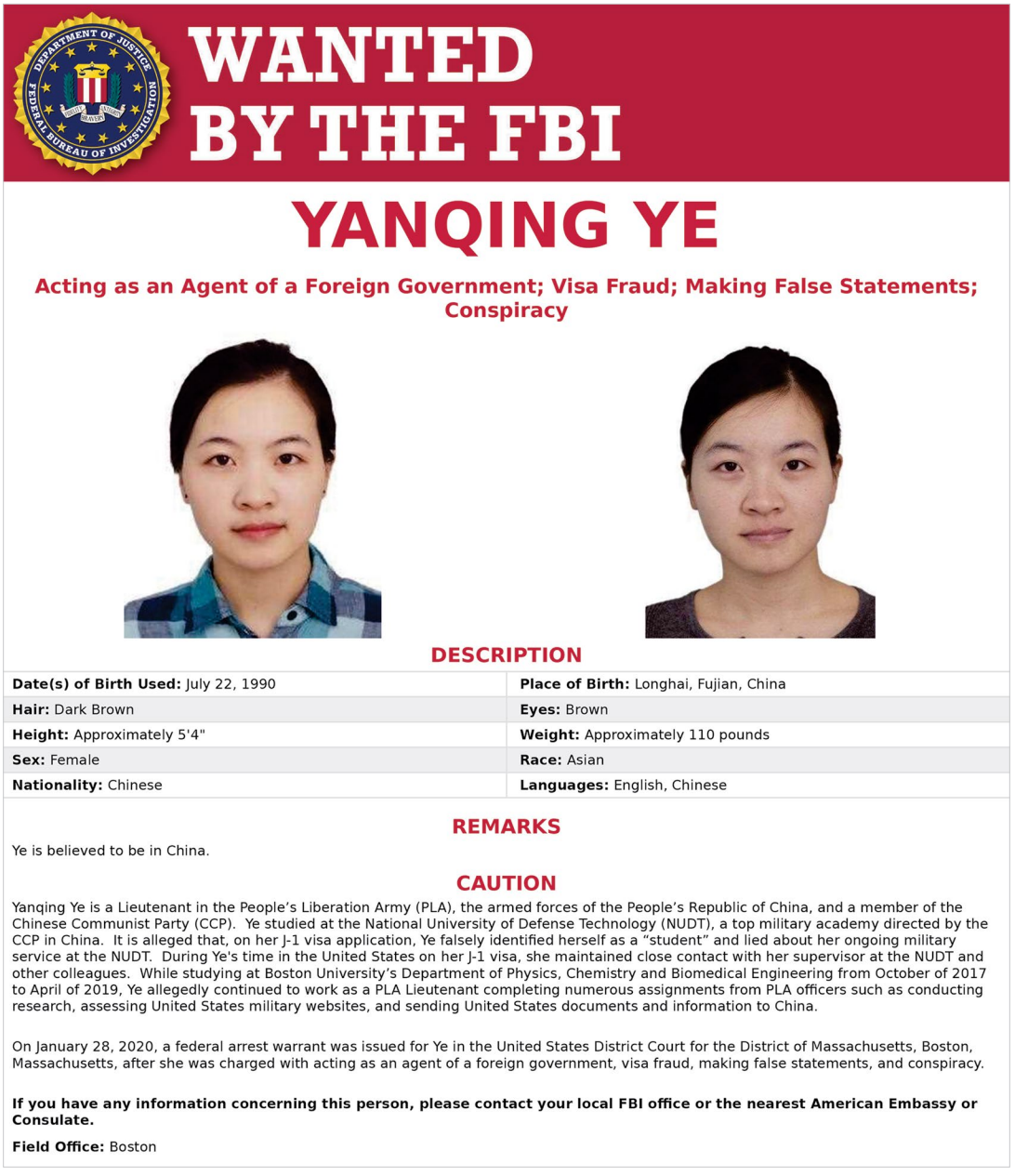
La Dra. Nita Patel, directora de descubrimiento de anticuerpos y desarrollo de vacunas, levanta un vial que contiene una posible vacuna para el COVID-19 el 20 de marzo de 2020 en los laboratorios Novavax en Gaithersburg, Maryland. El FBI ha declarado que el actual esfuerzo dirigido por el Gobierno chino para robar investigación relacionada con el desarrollo de una vacuna contra el coronavirus, así como otras investigaciones industriales y militares a través de la piratería informática, ha alcanzado un nivel sin precedentes. (Foto: Andrew Caballero-Reynolds, Agence France-Presse)

En 2006, bajo la dirección del presidente Hu Jintao, China puso en marcha el «Plan nacional a mediano y largo plazo para el desarrollo de la ciencia y tecnología (2006-2020)», o la política de «innovación autóctona». Esta política aplicaba normas de adquisición que obligaban a las empresas extranjeras a entregar la PI a cambio de acceso a los mercados chinos[9]. Además, la innovación autóctona aumentó la financiación nacional de la investigación y desarrollo tecnológicos, mientras impulsaba «el fomento de innovación original mediante la innovación cooperativa y la nueva innovación basada en la asimilación de tecnologías importadas»[10]. Entre las medidas adicionales dentro de la política figuraban las pruebas estatales de productos orientadas al estudio de los métodos de diseño y producción extranjeros, las políticas de adquisición del Gobierno que bloqueaban los productos no diseñados y producidos en China para alentar a las empresas extranjeras a divulgar los métodos de producción dentro de las fronteras chinas, y las leyes antimonopolio que protegían a las empresas estatales que cooperaban ya sea bajo el control directo o en estrecha coordinación con el PCCh y el EPL[11]. En conjunto, estas políticas promovieron la adquisición legal e ilegal de PI de exportación controlada de Estados Unidos y de terceros países como compensación por realizar negocios dentro de la China continental.

Un cambio en la política china: Pensamientos de Xi Jinping sobre el socialismo con características chinas para una nueva era

En su discurso ante el 19º Congreso Nacional del PCCh, el 18 de octubre de 2017, Xi describió su plan para que China se convierta en «un líder mundial en términos de fuerza nacional compuesta e influencia internacional» para 2050, superando a Estados Unidos y a Occidente como la potencia mundial dominante

tanto económica como militarmente[12]. Este tono contrasta mucho con la «Estrategia de 24 caracteres» de Deng de la década de 1990, que afirmaba «observar con calma; garantizar nuestra posición; manejar los asuntos con calma; esconder nuestras capacidades y esperar el momento oportuno; ser buenos en mantener un perfil bajo; y nunca afirmar el liderazgo»[13]. Si bien el objetivo general de China de alcanzar la prominencia en el escenario mundial no ha cambiado desde la época de Deng hasta la de Xi, el tono y la agresividad con que se persiguen los objetivos económicos, tecnológicos y militares ha cambiado radicalmente.



WANTED BY THE FBI

YANQING YE

Acting as an Agent of a Foreign Government; Visa Fraud; Making False Statements; Conspiracy

DESCRIPTION

Date(s) of Birth Used: July 22, 1990	**Place of Birth:** Longhai, Fujian, China
Hair: Dark Brown	**Eyes:** Brown
Height: Approximately 5'4"	**Weight:** Approximately 110 pounds
Sex: Female	**Race:** Asian
Nationality: Chinese	**Languages:** English, Chinese

REMARKS

Ye is believed to be in China.

CAUTION

Yanqing Ye is a Lieutenant in the People's Liberation Army (PLA), the armed forces of the People's Republic of China, and a member of the Chinese Communist Party (CCP). Ye studied at the National University of Defense Technology (NUDT), a top military academy directed by the CCP in China. It is alleged that, on her J-1 visa application, Ye falsely identified herself as a "student" and lied about her ongoing military service at the NUDT. During Ye's time in the United States on her J-1 visa, she maintained close contact with her supervisor at the NUDT and other colleagues. While studying at Boston University's Department of Physics, Chemistry and Biomedical Engineering from October of 2017 to April of 2019, Ye allegedly continued to work as a PLA Lieutenant completing numerous assignments from PLA officers such as conducting research, assessing United States military websites, and sending United States documents and information to China.

On January 28, 2020, a federal arrest warrant was issued for Ye in the United States District Court for the District of Massachusetts, Boston, Massachusetts, after she was charged with acting as an agent of a foreign government, visa fraud, making false statements, and conspiracy.

If you have any information concerning this person, please contact your local FBI office or the nearest American Embassy or Consulate.

Field Office: Boston

Una captura de pantalla de un cartel «se busca» para una presunta agente china, publicado en 2020 por el FBI.

Los cambios en la política y legislación nacional complementaron este cambio de tono a partir de 2016 con su Ley de Ciberseguridad. Entre otros numerosos cambios y restricciones, esta ley exige que todas las empresas comerciales que produzcan «datos importantes durante las operaciones dentro del territorio continental de la República Popular de China, los almacenen dentro de la China continental»[14]. Si se requiere que los datos se transfieran fuera de China con fines comerciales, deben ser examinados y aprobados por las autoridades chinas antes de su difusión, lo que abre la posibilidad de una amplia recopilación y robo de datos privados entre las empresas extranjeras que operan en China[15].

En 2007, China también promulgó la Ley de Inteligencia Nacional, que estableció un nivel de cooperación sin precedentes entre los organismos estatales (como el Ministerio de Seguridad del Estado [MSE] y el EPL), las organizaciones privadas

y personas. El artículo 7 de la ley establece la cooperación privada con la seguridad del Estado, declarando que «cualquier organización o ciudadano debe cooperar con la labor del aparato de inteligencia del Estado de conformidad con la ley, y mantener los secretos de la labor de inteligencia nacional conocidos por el público. El Estado protege a las personas y organizaciones que apoyan, ayudan y cooperan con la labor de inteligencia nacional»[16]. En el artículo 12 se establece un tono de cooperación similar entre la recopilación de información de inteligencia del Estado y empresas privadas, declarando que «la organización de trabajo de inteligencia del Estado podrá, de conformidad con los reglamentos estatales pertinentes, establecer relaciones de cooperación con personas y organizaciones pertinentes y encomendarles el trabajo correspondiente»[17].

El cambio de tono bajo Xi marca una transformación en la política exterior china cada vez más beligerante económica, tecnológica y militarmente que ha reflejado el aumento del robo de PI de tecnologías de EUA. El robo de PI complementa directamente el objetivo del PLA de modernizarse en una potencia global para mediados del siglo XXI. La Oficina de Información del Consejo del Estado delineó los objetivos futuros del EPL en el nuevo rol global de China en un libro blanco de 2015 titulado «La estrategia militar de China». En el libro blanco, se declaró que el EPL «acelerará la modernización de la defensa nacional y las Fuerzas Armadas [...] para lograr el objetivo estratégico nacional de los "dos centenarios" y para realizar el Sueño Chino de lograr el gran rejuvenecimiento de la nación china»[18].

Simultáneamente con la innovación militar, el Ministerio de Industria y Tecnología de Información (MIIT), bajo la dirección del primer ministro Li Keqiang, anunció su campaña «Hecho en China 2025» en 2015. Hecho en China 2025 hizo hincapié en el desarrollo de la tecnología emergente, la innovación interna y el cambio de una producción basada en la cantidad a una producción basada en la calidad para permitir que China se convierta en el principal fabricante mundial innovador para 2049[19]. El objetivo general es disminuir la dependencia de China de las naciones extranjeras para la tecnología avanzada y los bienes de alta calidad, produciendo el 70 por ciento de los materiales de alta tecnología a nivel nacional para el año 2025[20]. De acuerdo con la Oficina de Política de Comercio y Fabricación de la Casa Blanca de 2018, la inversión en tecnología extranjera de China ha estado en línea con las indicadas en la campaña Hecho en China 2025[21].

Aunque los expertos sostienen que las industrias de defensa de las empresas estatales chinas están intentando la innovación y la producción autóctonas, China continúa teniendo dificultades con el desarrollo de tecnología crítica[22]. Por consiguiente, la modernización del EPL aún requiere la adquisición de tecnología sensible y la investigación y desarrollo, que es mucho más difícil de adquirir mediante leyes comerciales legales en el marco del programa de «innovación autóctona» que otras tecnologías comerciales. Por lo tanto, el PCCh y el EPL dependen en gran medida del robo ilegal de PI para adquirir toda o parte de la tecnología crítica para realizar ingeniería inversa para las armas de producción interna.

Los métodos de robo de PI chinos: Robar la leña de debajo de la olla

Las Treinta y Seis Estratagemas, una colección de proverbios que se cree que son del período de los Tres Reinos de China, describe una estrategia para derrotar a un enemigo superior: «Roba la leña de debajo de la olla»[23]. Este proverbio describe el enfoque indirecto de eliminar la fuente de fuerza del enemigo, en este caso, la superioridad tecnológica de EUA y los ejércitos occidentales. Este método se resumió en la revisión de 2013 de La Ciencia de Estrategia Militar, publicada por la Academia de Ciencias Militares del EPL, que decía: «Tras el estallido de la Guerra del Golfo, el Comité Central del Partido y la Comisión Militar Central previeron que la situación de guerra causó grandes cambios y la política estratégica militar de defensa activa se ha ajustado de manera oportuna, aumentando el uso de la alta tecnología»[24]. Los autores continúan delineando la futura necesidad de paridad tecnológica o superioridad sobre Occidente, declarando: «El desarrollo de la ciencia y tecnología ha abierto el camino para la evolución de la forma de la guerra»[25].

Bajo la dirección de Hu en 2004 y actualmente bajo la dirección de Xi, y destacado en La Ciencia de Estrategia Militar, el EPL ha hecho hincapié en los esfuerzos para igualar a Occidente en alta tecnología

militar[26]. Sin embargo, como antes mencionado, la ciencia y tecnología autóctonas chinas no se consideran lo suficientemente avanzadas para competir de forma independiente con la base industrial de defensa (BID) de EUA y Occidente, lo que hace necesario el robo de las tecnologías actuales y en desarrollo. Para lograrlo, China utiliza varios medios, tanto legales como ilegales, para socavar la tecnología militar, la investigación y desarrollo de EUA y Occidente, y los métodos de producción de la BID. En la Estrategia de Seguridad Nacional, se describen los métodos básicos que China utiliza para robar la PI de EUA: «Los rivales han utilizado medidas sofisticadas para debilitar nuestros negocios y nuestra economía como facetas de la guerra económica cibernética y otras actividades maliciosas. Además de estas actividades ilegales, algunos agentes utilizan transferencias y relaciones, en gran medida legales y legítimas para acceder a los campos, los expertos y las proveedores de confianza»[27]. Los cuatro métodos de robo de PI por China son: de fuente abierta, comercial, académico y cibernético.

> La ciencia y tecnología autóctonas chinas no se consideran lo suficientemente avanzadas para competir de forma independiente con la base industrial de defensa de EUA y Occidente.

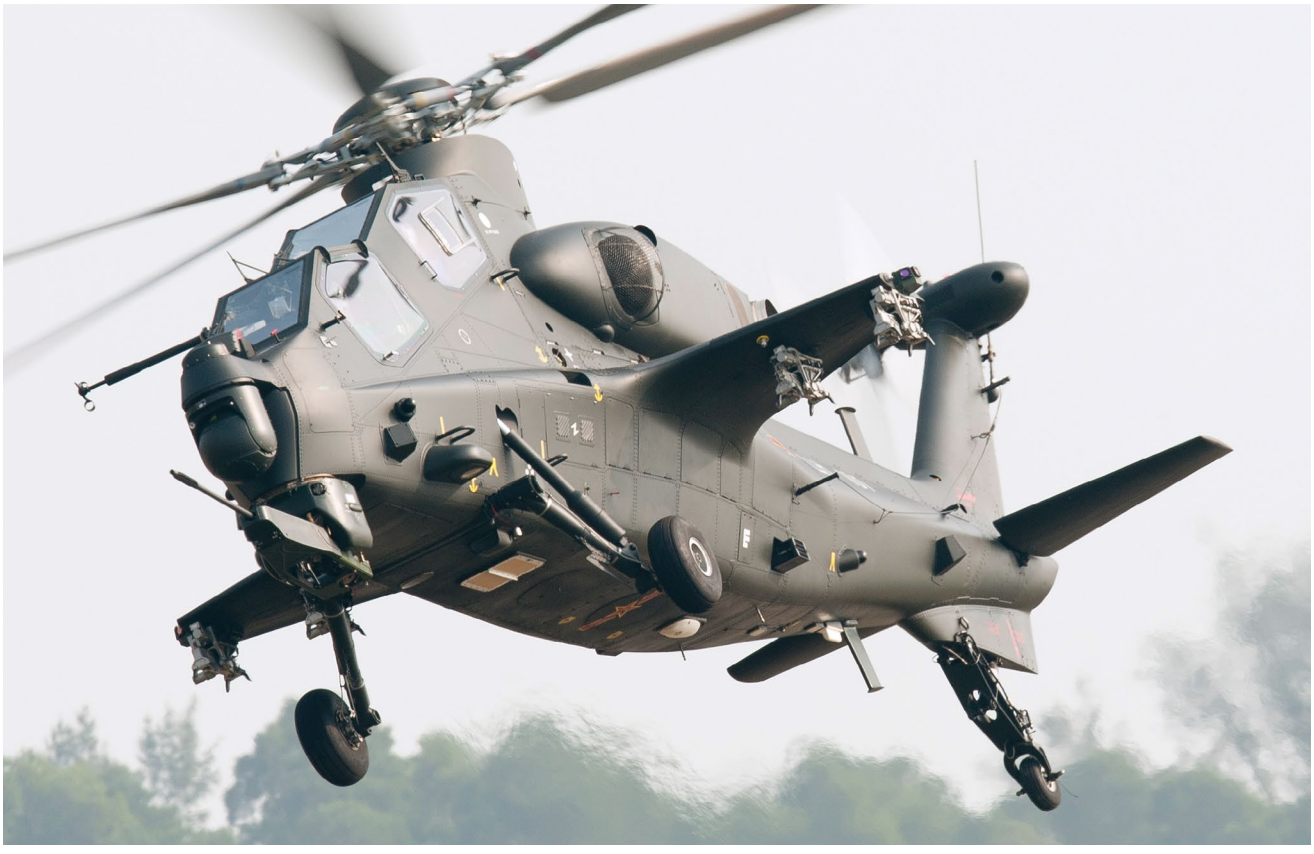
Método 1. Fuente abierta

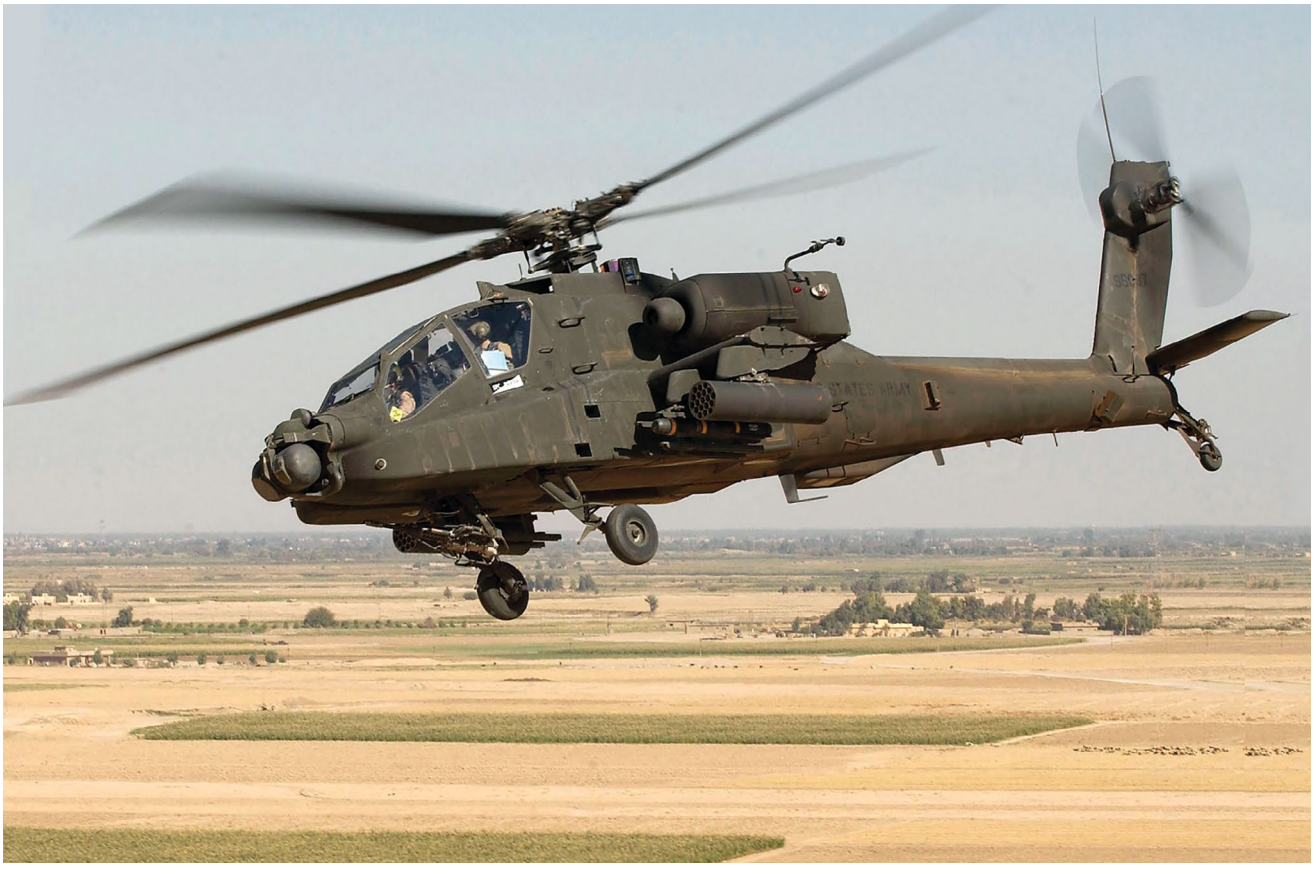
Según James Mulvenon, la recopilación de fuentes abiertas y el desarrollo de bases de datos de información públicamente disponible es el recurso clave de la innovación científica y tecnológica, afirmando que «la innovación en China está impulsada por los acontecimientos en el extranjero, rastreados a través de fuentes abiertas»[28]. Como es el caso con todos los organismos burocráticos chinos, la estructura de recopilación de datos de fuentes abiertas es compleja y redundante. Las organizaciones como el Instituto de Información Científica y Técnica de China operan bajo el disfraz de desarrollar bases de datos y catalogación inocuas, pero en realidad buscan documentación técnica de ciencia y tecnología disponible al público para la ingeniería inversa y la producción nacional; información disponible públicamente sobre organizaciones de investigación y sus empleados que los órganos de inteligencia del Estado utilizan, e información clasificada que ha sido incorrectamente desclasificada o publicada por error[29]. Si bien el sistema funciona de manera similar a un catálogo basado en una biblioteca, está dirigido y administrado por expertos chinos en inteligencia que trabajan para el PCCh, sirviendo como un atajo para que la industria china desarrolle la investigación y tecnología, y se cataloga y difunde en coordinación con desarrolladores y fabricantes privados o de empresas públicas[30].

El programa de fuente abierta ha extraído y catalogado, hasta 2013, más de 4.700 millones de títulos y resúmenes, 644 millones de documentos de texto completo, 1.2 millones de documentos de conferencias, 1.8 millones de informes científicos y tecnológicos extranjeros y 9.8 millones de productos microfilmados[31]. Esta vasta colección de información no clasificada pública y privada e incorrectamente clasificada reduce el costo, el tiempo y el riesgo para el desarrollo militar y civil de China. El programa de fuente abierta ha tenido tanto éxito que el exdirector del Instituto de Información Científica y Técnica de China, He Defang, se jactó de que, gracias a la recolección de datos de fuentes abiertas, «los investigadores de China redujeron sus costos en un 40-50 % y su tiempo en un 60-70 %»[32].

Las implicaciones de una recolección de datos tan completa y específica de fuentes abiertas para el Ejército y el Departamento de Defensa son profundas.

Página siguiente: Una variedad de aviones y helicópteros militares chinos se parecen extrañamente similares en su diseño a los desarrollados por Estados Unidos y otros países, incluidos muchos fabricados por Rusia. Por ejemplo, se cree que el helicóptero chino Z-10 (arriba), que se asemeja mucho al helicóptero Apache AH-64 de Estados Unidos (abajo), se ha desarrollado a partir de información obtenida mediante una combinación de espionaje, piratería informática y transferencia de información secreta comercial clasificada a través de acuerdos engañosos con empresas legítimas que trabajan bajo la presunción de cooperación con China para desarrollar un helicóptero de «doble uso». (Arriba: Peng Chen a través de Wikimedia Commons, CC BY-SA 2.0. Abajo: Ejército de EUA, Sargento Técnico Andy Dunaway)





La responsabilidad pública y la transparencia en Estados Unidos y en los países occidentales pueden permitir que el desarrollo de tecnología militar y las personas que trabajan en ese ámbito se conviertan en blancos. Por ejemplo, las adjudicaciones de contratos gubernamentales que se publican casi a diario en la página de noticias «Contratos» del Departamento de Defensa ofrecen información sobre la tecnología que se está desarrollando, los costos, los contratistas, los subcontratistas, la duración de los contratos, las ubicaciones, las instituciones militares a las que se presta servicio, etcétera[33]. Además, los sitios web de los adjudicatarios de contratos suelen proporcionar información sobre la estructura organizativa, el personal, la ubicación de las instalaciones y la información no clasificada sobre la investigación y desarrollo. Esta información, junto con otros datos de innumerables sitios web gubernamentales y privados de carácter público, proporcionan a China un panorama claro de las prioridades de investigación y desarrollo de Estados Unidos, las intenciones a largo plazo, las estrategias, las prioridades para la fuerza y las oportunidades de recolección por otros medios que se discuten a continuación.

Método 2. Comercial

Si bien China ha pasado de ser una nación comunista maoísta durante el Gobierno de Nixon a una economía de mercado mixto en la actualidad, la distinción entre lo privado, lo público y lo académico es mucho menos profunda que en Estados Unidos. Hoy en día, las SOE que son propiedad o están financiadas directa o indirectamente por el PCCh o el EPL constituyen aproximadamente entre el 23 y el 28 por ciento del producto interno bruto (PIB) de China[34]. Algunas SOE y empresas privadas de China trabajan a instancias o en nombre del PCCh o el EPL, ya sea directa o indirectamente, para buscar y adquirir tecnología de EUA para la importación, ingeniería inversa y producción nacional que apoye los objetivos de investigación y desarrollo del PCCh o el EPL[35]. Los subcontratos adjudicados a empresas chinas por contratistas principales a los contratos del Gobierno de EUA ofrecen una visión de los métodos de producción y la capacidad para compilar e hacer la ingeniería inversa de la tecnología para producir internamente tecnología de alta calidad.

Las SOE están vinculadas a las empresas de EUA y otras empresas occidentales por la Asociación China de Ciencia y Tecnología a través de centros nacionales de transferencia de tecnología. Estos centros establecen relaciones de cooperación con corporaciones e institutos académicos de EUA para fomentar la transferencia de tecnología[36]. El PCCh y el EPL financian a las SOE para que empleen a expertos en ciencia y tecnología de Estados Unidos y de Occidente, que representan alrededor de la mitad de los 440 000 extranjeros que trabajan actualmente en China[37]. Otros programas estatales, como el Programa 863, financiado y dirigido por el Ministerio de Ciencia y Tecnología para desarrollar y adquirir tecnologías de alto nivel, han estado implicados en la comisión de espionaje, como la condena en 2011 de Kexue Huang por robar secretos comerciales de AgroSciences y Cargill Inc[38].

Como se indica en Hecho en China 2025, China ha cambiado el enfoque industrial de los bienes baratos y de baja calidad a la innovación de alta calidad impulsada por la tecnología[39]. Para lograrlo, China ha cambiado la financiación respaldada por el Gobierno de la adquisición de «recursos naturales básicos» antes de la publicación de la política para «adquirir áreas de alta tecnología de la economía de Estados Unidos en particular»[40]. China utiliza SOE, empresas privadas chinas vinculadas al Gobierno chino y fondos de inversión respaldados por el Estado para llevar a cabo fusiones, adquisiciones, inversiones y financiación de empresas, para adquirir alta tecnología de EUA[41]. Estas prácticas consisten en medios legales, ilícitos o a veces ilegales para solicitar, coaccionar o abiertamente robar información y tecnología de empresas privadas de EUA y otras naciones. Según un informe de la FBI (Oficina Federal de Investigación) sobre los enjuiciamientos relacionados con China desde 2018, «alrededor del 80 por ciento de todos los enjuiciamientos por espionaje económico iniciados por el Departamento de Justicia de Estados Unidos (DOJ) alegan conductas que beneficiarían al Estado chino, y existe por lo menos algún nexo con China que es alrededor del 60 por ciento de todos los casos de robo de secretos comerciales»[42].

Además, las empresas chinas, incluidas las SOE, se han insertado en las cadenas de suministro de las instituciones militares de EUA, por lo general mediante subcontratos de bajo nivel, y han producido y vendido a Estados Unidos piezas de repuesto ilegales y de calidad inferior[43]. Entre los ejemplos recientes figuran las piezas de componente de la aeronave de transporte C-130J, la aeronave de transporte C-27J, el helicóptero multimisión SH-60B de la Marina de Guerra, el sistema de defensa antiaérea de gran altura (Terminal High Altitude Area Defense – THAAD) y la aeronave marítima multimisión P-8A Poseidon[44]. A

medida que las fuerzas militares de EUA dependen cada vez más del equipamiento de tecnología de información comerciales disponibles en el mercado, se agrava el riesgo de que las empresas chinas produzcan componentes comprometidos, como lo demuestra un informe de Bloomberg de 2018 en el que se destacan los esfuerzos de China por utilizar microchips comerciales para infiltrarse y establecer una puerta trasera en el equipamiento de tecnología de información que se venden a los organismos gubernamentales[45]. La preocupación con esta cuestión es tan grande que en 2018 el presidente de EUA, Donald Trump, firmó un proyecto de ley por el que se prohibía la tecnología de Huawei y ZTE (principales proveedores de teléfonos celulares a los miembros militares en el extranjero) en los contratos gubernamentales[46].

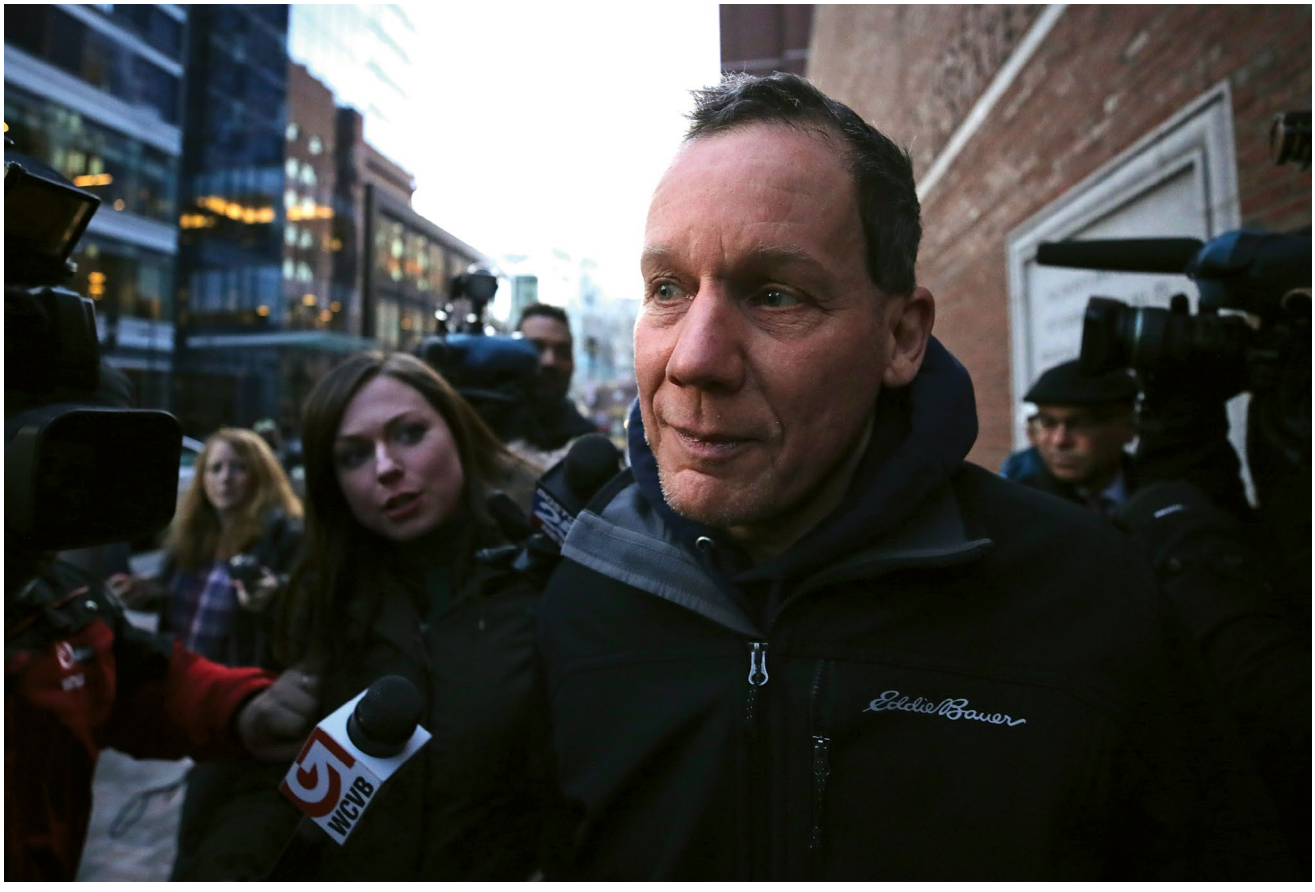
Sello del Programa de Mil Talentos

Método 3. El mundo académico

Además del robo de PI de fuentes abiertas y comerciales, China ha empleado a académicos para cometer robos de PI desde el comienzo de las «cuatro modernizaciones» de Deng[47]. A partir de 1978, con Deng, China cambió a un enfoque más pragmático de modernización, enviando un número cada vez mayor de estudiantes y científicos al extranjero para que aprendieran de las naciones occidentales (algo que se consideró peligroso bajo Mao después de la Revolución Cultural), así como atraer talento extranjero a China[48]. El planteamiento de China para adquirir PI a través del mundo académico tiene dos enfoques distintos: a través de organizaciones abiertas y establecidas patrocinadas por el Gobierno y a través del uso abierto y encubierto de poblaciones de estudiantes y profesores en el extranjero para adquirir ilegalmente PI. Ambos métodos convierten efectivamente a los estudiantes y profesores en recolectores de IP patrocinados por el Estado bajo la dirección del PCCh o el EPL.

En las secuelas del Movimiento de Democracia en 1989, que culminó con la masacre de la Plaza de Tiananmen, el PCCh trató de enfocar en los estudiantes chinos en el país y el extranjero para garantizar la lealtad al partido. Para lograrlo, el PCCh amplió las existentes Asociaciones de Estudiantes y Becarios Chinos (CSSA) en el extranjero para garantizar la lealtad de los estudiantes en el exterior a la ideología del PCCh. Además, en 2004, el PCCh fundó el primer Instituto Confucio, cuyo propósito declarado es «enseñar el idioma, cultura e historia chinos a nivel primario, secundario y universitario en todo el mundo»[49]. Actualmente, China opera más de 140 CSSA y 110 Institutos Confucio, todos bajo la dirección del Departamento de Trabajo del Frente Unido del PCCh[50]. Según la Comisión de Revisión Económica y de Seguridad EUA-China de 2018, en realidad, las CSSA «reciben orientación del PCCh a través de las embajadas y consulados chinos [...] y están activos en la realización de trabajos chinos en el extranjero consistentes con la estrategia del Frente Unido de Pekín»[51]. Del mismo modo, se ha acusado a los Institutos Confucio de «influencia impropia sobre la enseñanza e investigación, espionaje industrial y militar, vigilancia de chinos en el extranjero y socavar la influencia de Taiwán como parte del plan de reunificación»[52]. Ambas organizaciones sirven para garantizar que las poblaciones estudiantiles chinas en el exterior actúen de acuerdo con la orientación y los deseos del PCCh y el EPL.

El Programa de Mil Talentos, establecido en 2008 tanto para reclutar científicos no chinos como para atraer a personas chinas educadas en el extranjero para que regresen al continente, ha sido criticado abiertamente por las agencias de EUA por cometer el robo de PI. En 2018, el subdirector de la División de Contrainteligencia de la FBI declaró que el Programa



El profesor de la Universidad de Harvard Charles Lieber rodeado de reporteros el 30 de enero de 2020 cuando sale de la Corte Federal de Justicia de Estados Unidos John Joseph Moakley en Boston, Massachusetts. Lieber, presidente del Departamento de Química y Biología Química, fue acusado de mentir a los funcionarios acerca de su participación en un programa de reclutamiento dirigido por el Gobierno chino a través del cual recibió decenas de miles de dólares. (Foto: Charles Krupa, Associated Press)

de Mil Talentos y otros programas similares patrocinados por el Gobierno chino «ofrecen salarios competitivos, instalaciones de investigación de última generación y títulos honoríficos, atrayendo tanto al talento chino en el extranjero como a los expertos extranjeros para que aporten sus conocimientos y experiencia a China, incluso si eso significa robar información patentada o violar los controles de exportación para hacerlo»[53]. En enero de 2020, Charles Lieber, el presidente del Departamento de Química y Biología Química de la Universidad de Harvard, fue acusado de aceptar el pago y los gastos de manutención de la Universidad Tecnológica de Wuhan después de aceptar una beca de investigación del Departamento de Defensa y de falsificar declaraciones relativas a su participación en el Programa de los Mil Talentos[54]. El Programa de Mil Talentos y otros programas similares financieramente atractivos permiten a China aprovechar los sistemas educativos y el desarrollo de tecnología extranjeros atrayendo a los científicos e investigadores que trabajan en tecnologías sensibles y controladas para transferir las PI extranjeras a China de forma barata y, a menudo, de forma ilegal.

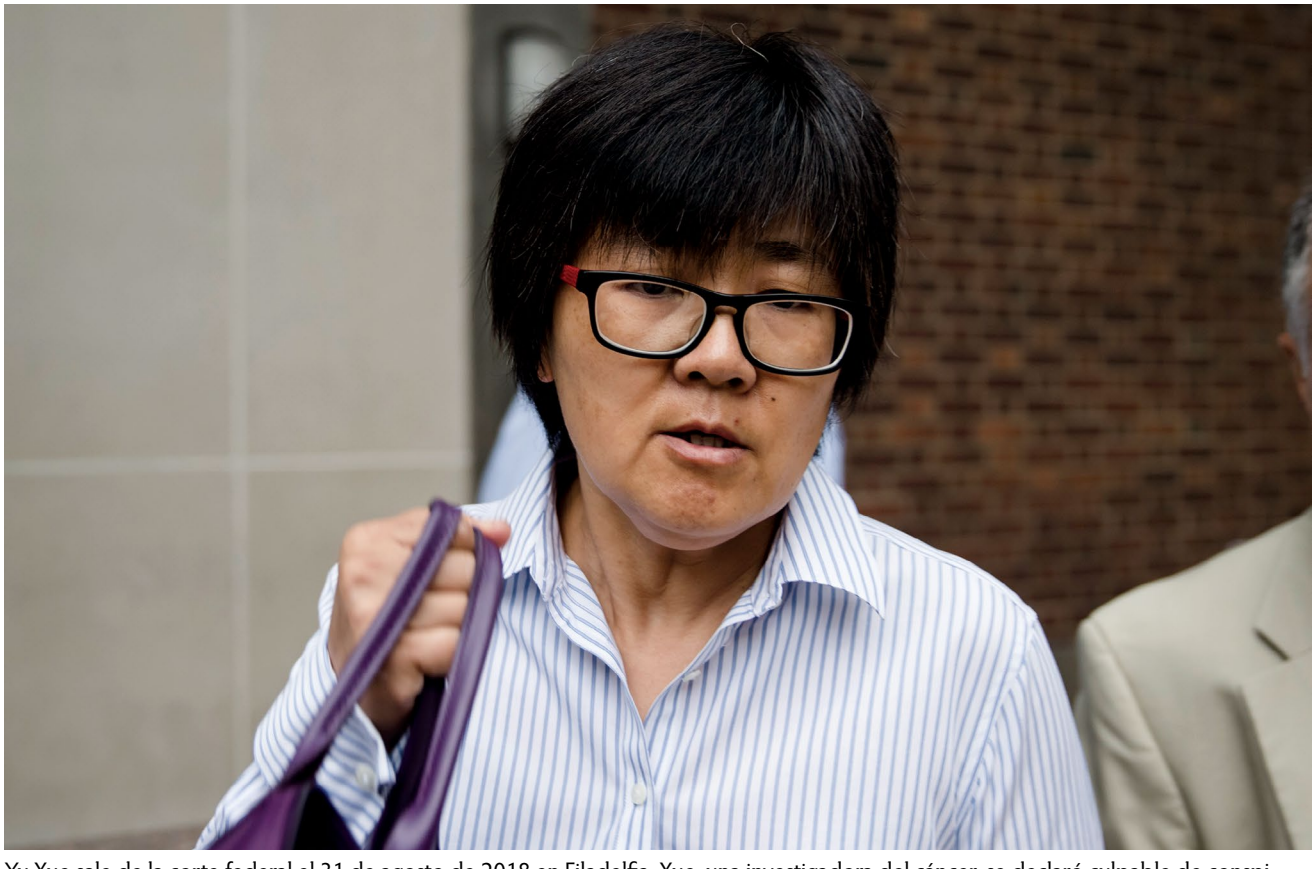
Además de las organizaciones patrocinadas por el Gobierno, se ha acusado a China de considerar a todos los estudiantes chinos como posibles conductos para la transferencia de tecnología extranjera. Las organizaciones chinas han abogado abiertamente por «ampliar el papel de los científicos chinos que viven en el extranjero en la realización de investigaciones en nombre de los institutos de investigación chinos y facilitar la transferencia de tecnología»[55]. Los estudiantes chinos que regresan del extranjero suelen ser interrogados por funcionarios del Gobierno sobre las tecnologías, investigación y personal científico a los que han tenido acceso como parte de la recopilación general de información de inteligencia y para evaluar el potencial de cooptación o reclutamiento de

estudiantes. Además, se ha acusado al MSE de China de acercarse a estudiantes y científicos chinos que se preparan para viajar al extranjero para asignarles la tarea de adquirir información o «realizar otras actividades operacionales» mientras están en el extranjero, como el establecimiento de relaciones encubiertas con personal académico[56]. El uso de estudiantes y profesores chinos en el extranjero como recolectores de IP plantea un gran desafío a la apertura y transparencia de las instituciones académicas fuera de China, que deben esforzarse por equilibrar la protección de la IP y la promoción del intercambio y la colaboración en la investigación científica.

Método 4. Cibernético

China utiliza medios cibernéticos para llevar a cabo el robo de PI, tanto directamente mediante intrusiones en la red y el robo de datos, como indirectamente a través de otros medios, como la recopilación de fuentes abiertas o en apoyo del espionaje tradicional[57]. El ciberespacio vincula los métodos antes mencionados porque proporciona un medio barato y fácil de llevar a cabo el robo de PI en un entorno de bajo riesgo con relativamente pocas repercusiones en acciones que de otro modo tendrían importantes consecuencias, como sanciones económicas, detenciones y expulsión de agentes estatales (conocidos como persona non grata en la diplomacia internacional) si se llevan a cabo en territorio extranjero.

El robo de IP mediante intrusiones en la red y la extracción de datos de la BID, los subcontratistas, el mundo académico y las redes gubernamentales ofrece un medio barato, fiable y de bajo riesgo para adquirir tecnología militar sensible tanto en desarrollo como ya existente para la ingeniería inversa y la producción nacional en China. Según el informe anual del Departamento de Defensa al Congreso en 2019, «China utiliza sus capacidades cibernéticas no solo para apoyar la recolección de inteligencia [...] sino también para extraer información sensible de la BID para obtener una ventaja militar. La información deseada puede beneficiar a la industria de alta tecnología



Yu Xue sale de la corte federal el 31 de agosto de 2018 en Filadelfia. Xue, una investigadora del cáncer, se declaró culpable de conspirar para robar secretos comerciales biofarmacéuticos de GlaxoSmithKline en lo que los fiscales dijeron que era un plan para establecer empresas en China para comercializarlos. (Foto: Matt Rourke, Associated Press)

de defensa de China [y] apoyar la modernización militar de China»[58]. El informe continúa, destacando la gravedad del problema así: «Estas campañas cibernéticas amenazan con erosionar las ventajas militares de EUA y poner en peligro la infraestructura y la prosperidad de la que dependen esas ventajas»[59].

En 2013 se puso de relieve la cúspide del volumen de la actividad cibernética china, ya que FireEye, una empresa privada de seguridad cibernética, identificó una marcada reducción de incidentes de espionaje cibernético en China en los años siguientes. Si bien esto se debió en gran parte a la orden del gran jurado de 2014 y al Acuerdo Cibernético entre EUA y China de 2015 en principio, FireEye también atribuyó la reducción a la profesionalización y reorganización de los agentes cibernéticos chinos[65]. Según Elsa Kania y John Costello, la reducción de la cantidad de ataques coincide con la reorganización de los medios cibernéticos chinos bajo la Fuerza de Apoyo Estratégico del EPL, que centralizó el cibernético del EPL como una rama de servicio separada bajo un solo comando y cambió el enfoque hacia un cibernético orientado al combate. Además, el MSE parece haber tomado una posición delantera en el espionaje cibernético comercial y en la dirección de actores no estatales en ataques centrados en los intereses comerciales de los EUA[66]. Según un informe anual presentado al Congreso en 2016, la actividad cibernética china en general ha pasado de los ataques torpes de gran escala, como los realizados por el EPL antes de 2014, a una fuerza más centralizada y profesionalizada, lo que implica que el ciberespionaje chino será más difícil de detectar en el futuro, ya que el MSE y otros organismos de inteligencia chinos, en lugar del EPL, tienen como objetivo las redes comerciales vulnerables[67]. En lugar de una reducción de los incidentes de ciberespionaje en China, que representa un éxito en la política de EUA, en realidad pone de relieve un posible aumento de las capacidades de los actores cibernéticos chinos y una reducción de la capacidad de EUA para detectar amenazas.

« China utiliza agentes cibernéticos estatales, empresariales y privados para comprometer y robar entre 180 000 y 540 000 millones de dólares de propiedad intelectual y secretos comerciales anualmente, o entre el 1 y el 3 por ciento del PIB de EUA. »

Según un informe de Verizon de 2013, el 96 por ciento de todos los casos de violación de datos de espionaje cibernético se atribuyeron a agentes en China[60]. China utiliza agentes cibernéticos estatales, empresariales y privados para comprometer y robar entre 180 000 y 540 000 millones de dólares de PI y secretos comerciales anualmente, o entre el 1 y el 3 por ciento del PIB de EUA[61]. El general Keith Alexander, entonces director de la Agencia de Seguridad Nacional y luego comandante del Comando Cibernético de EUA, declaró en 2012: «En mi opinión, [el robo de propiedad intelectual cibernética] es la mayor transferencia de riqueza de la historia»[62].

En 2014, el Departamento de Justicia de EUA acusó a cinco oficiales de la Unidad 61398 del EPL, entre otros cargos, de «espionaje económico» y de «acceder (o intentar acceder) a una computadora protegida sin autorización para obtener información por el propósito de obtener ventajas comerciales y ganancias financieras privadas»[63]. Esta ocasión se convirtió en una primera instancia histórica de agentes estatales extranjeros acusados de infiltrarse en objetivos comerciales de EUA mediante el ciberespionaje[64]. En un intento de avergonzar y disuadir futuras acciones de los agentes chinos, las acusaciones del gran jurado representaron un reconocimiento abierto y público por parte del Gobierno de EUA de los agentes estatales chinos que procuran adquirir activa y agresivamente la tecnología militar crítica. Sin embargo, a pesar de las acusaciones, las ramificaciones y las represalias del Gobierno de EUA siguieron estando dirigidas a personas concretas y pusieron de relieve el bajo riesgo y la naturaleza de alto rendimiento del espionaje cibernético.

Además de la intrusión directa en la red y robo de PI, China utiliza las redes de información para dirigirse a personas en línea para llevar a cabo los medios más tradicionales de robo de PI antes mencionados. Los agentes de inteligencia del Estado chino utilizaron

LinkedIn para seleccionar y reclutar clandestinamente a un ex empleado de la Agencia Central de Inteligencia y de la Agencia de Inteligencia de Defensa, y el Departamento de Justicia de EUA acusó a un agente de inteligencia chino en octubre de 2018 de reclutar a un ingeniero de General Electric Aviation con el que establecieron un contacto inicial en LinkedIn[68]. Los perfiles que contienen el historial de trabajo, los títulos y las áreas de especialización ofrecen una lucrativa fuente de información para los agentes chinos que buscan adquirir PI de sectores tecnológicos específicos.

El robo de PI con medios cibernéticos, al igual que todos los demás métodos de robo de PI en China, abarca un amplio espectro de medios y métodos y se superpone a los métodos tradicionales de robo de PI ya mencionados. El robo de PI con apoyo cibernético se destaca entre otros métodos por el volumen y la facilidad con que se puede llevar a cabo. Sin embargo, cabe señalar que los datos técnicos en bruto tienen poco valor si no se dispone de los métodos, medios y conocimientos técnicos necesarios para realizar la ingeniería inversa y producir tecnología internamente en China, lo cual se logra principalmente mediante el robo de PI comerciales y académicas.

Cómo mitigar el robo de PI chino: Detener la marea

Mientras que las políticas y procedimientos internos del Ejército y el Departamento de Defensa pueden mitigar algunos robos de PI, el robo de PI cubre un amplio espectro en todas partes del Gobierno, el sector privado y el mundo académico y, por lo tanto, el problema no puede ser resuelto por el Ejército o el Departamento de Defensa por sí solos. Para mitigar y prevenir el robo de PI, el Departamento de Defensa debe fortalecer las asociaciones, comités y políticas gubernamentales, privados y académicos existentes. En primer lugar, las políticas, organizaciones y autoridades gubernamentales existentes pueden ser aprovechadas para combatir el robo de PI de tecnología militar. Sin embargo, el Ejército y el Departamento de Defensa deben aprovechar el sector privado y enmendar sus políticas y reglamentos de contratación para mitigar los robos mediante la aplicación de normas de protección de información más estrictas a los contratistas y subcontratistas. Además, el Ejército y el Departamento de Defensa deben asociarse con institutos académicos que realicen investigaciones sobre tecnología crítica para proteger tanto las tecnologías clasificadas como las no clasificadas en desarrollo o emergentes.

Dentro del Gobierno federal, se debe analizar un enfoque integral para priorizar las altas tecnologías críticas. Una tecnología que tiene un ciclo de vida más corto antes de volverse obsoleta es menos crítica de defender que una tecnología que seguirá siendo relevante durante décadas sin un reemplazo previsible. Además, el Departamento de Defensa y otras agencias gubernamentales deben garantizar la protección de las tecnologías desde «la cuna hasta la tumba», un término que se utiliza para describir la protección de las tecnologías críticas desde el momento de su inicio hasta su puesta en marcha, su ciclo de vida y su eventual sustitución por una nueva tecnología. Al defender únicamente las tecnologías en desarrollo, el Departamento de Defensa corre el riesgo de retrasar simplemente el eventual robo de la tecnología y la producción interna por parte de los adversarios.

Además, el DOD y el Gobierno federal en general deben aprovechar las políticas y organizaciones existentes para reforzar la protección de la PI del sector privado. Dos ejemplos incluyen el Comité de Inversión Extranjera en Estados Unidos, que puede revisar las adquisiciones y fusiones extranjeras de tecnología crítica de EUA; y el Programa Nacional de Seguridad Industrial, que estableció una política a través del DOD 5220.22-M, un manual de operaciones del DOD que describe los procedimientos para las empresas privadas que trabajan en contratos gubernamentales clasificados[69]. Al aprovechar comités como el Comité de Inversiones Extranjeras en Estados Unidos, el Departamento de Defensa podría abordar las preocupaciones sobre las fusiones o adquisiciones de empresas de contratación o subcontratación de alta tecnología por parte de empresas chinas con vínculos directos o indirectos con el PCCh o el EPL. Las políticas existentes, como la 5220.22-M del Departamento de Defensa, el Reglamento de Adquisiciones Federales y el Suplemento del Reglamento de Adquisiciones Federales del Departamento de Defensa (DFARS) proporcionan marcos sobre los cuales mejorar las prácticas de seguridad del sector privado y reforzar la reglamentación sobre el acceso de los subcontratistas a la tecnología crítica y en desarrollo[70]. Al

aprovechar las autoridades de organismos y departamentos externos como el FBI, el Departamento del Tesoro o el Departamento de Estado, el Ejército y el Departamento de Defensa imponen medidas reglamentarias, financieras o penales a las empresas que no cumplen con las normas dentro de Estados Unidos y ejercen presión internacional a través de los organismos reguladores internacionales.

Actualmente, cualquier universidad con un contrato de defensa federal que trabaje con información no clasificada controlada bajo el DFARS 525.204.7012 debe cumplir con la Publicación Especial 800-171 del Instituto Nacional de Estándares y Tecnología (NIST), Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, para proteger la información no clasificada controlada[71]. En el DFARS 252.204.7012, se estableció el cumplimiento reglamentario de las normas de la NIST 800-171 para todos los contratos adjudicados después del 1º de octubre de 2017. Sin embargo, la aplicación de la norma del DFARS 252.204.7012 se basa principalmente en la notificación del contratista al jefe de información del Departamento de Defensa de cualquier deficiencia en el cumplimiento de la NIST 800-171, pero no en las inspecciones o controles reglamentarios de ningún organismo de aplicación. Además, solo se exige a los subcontratistas que informen de las deficiencias en el cumplimiento de la NIST 800-171 al contratista principal y no al Gobierno federal, con lo que se corre el riesgo de que el cumplimiento por parte de los subcontratistas de la información no clasificada controlada sea deficiente[72]. Esta dependencia de los informes propios de los contratistas y subcontratistas promueve que se ignoren las deficiencias en la orientación normativa federal requerida y pone a las empresas y al Departamento de Defensa en peligro de la vulnerable tecnología crítica de los sistemas de información. Enmendar la guía regulatoria federal para las universidades, contratistas y subcontratistas que trabajan con información no clasificada controlada para permitir inspecciones regulatorias federales y controles de cumplimiento de las compañías protegería contra el robo de PI.

La adición de 2019 al DFARS 252.204-7018, que prohibía las ventas de contratistas o subcontratistas al Gobierno de Estados Unidos de artículos o componentes finales producidos por Huawei y ZTE o cualquier filial de estos, estableció un precedente para la promulgación de medidas reglamentarias contra el robo de PI. Además, el DFARS 252.204-7018 exige que los contratistas principales incluyan la cláusula en los «subcontratos para la adquisición de artículos comerciales» para impedir las ventas prohibidas de equipo de Huawei y ZTE a los contratistas por medio de subcontratos[73].

Ningún planteamiento o método contrarrestará el robo de tecnología militar relacionado con la PI crítica por parte de los chinos. Sin embargo, al asociarse con otras agencias y departamentos federales y estatales, empresas privadas y universidades, así como promulgar una guía regulatoria más estricta y herramientas de aplicación, el Ejército y el Departamento de Defensa prevendrán más eficazmente el robo de PI y tomarán represalias contra los robos después de que ocurran. Mediante un planteamiento público-privado, puede ser posible disuadir el robo de PI mediante una combinación de prevención, incentivos y represalias, que hacen que el robo ilegal de PI sea financieramente insostenible.

Conclusión

Las implicaciones del robo de PI por China son fácilmente aparentes en las acciones, declaraciones oficiales y doctrina del PCCh y el EPL. Mientras que los métodos y técnicas utilizadas para llevar a cabo el robo de PI no son exclusivos del PCCh, el alcance y la frecuencia del robo sí lo son. A pesar del Acuerdo en Principio de 2015 y las subsecuentes acciones de represalia del Gobierno federal de EUA, China ha mostrado poca propensión a frenar su robo de PI de alta tecnología. El robo de PI combinado con el aumento de gastos militares de China amenaza con cerrar la brecha con la superioridad tecnológica militar de EUA y desafiar el dominio militar norteamericano. Aunque China no pueda ser capaz de producir armas y sistemas de alta tecnología de calidad superior por muchas décadas por venir, la amenaza de la paridad en incluso pocas áreas de alta tecnología militar amenaza la superioridad general de EUA en el campo de batalla y lleva a una disminución de su estatus en el escenario mundial.

Los desafíos presentados por el robo de PI chinos son numerosos y pueden requerir que el Ejército y

el Departamento de Defensa salgan de su entorno operativo normal para contrarrestar la amenaza y trabajar con agencias, departamentos y socios que no se asocian frecuentemente con la acción militar. Si bien los incidentes aislados de robo de PI pueden parecer intrascendentes en el presente, las consecuencias de no tomar medidas pueden amenazar las vidas futuras en el campo de batalla y el dominio militar de EUA. Solo a través de la prevención proactiva del robo de PI por China puede el Ejército y el Departamento de Defensa proteger su dominio tecnológico y el futuro de la superioridad militar de EUA. ■

Notas

1. Barack Obama, «Remarks by President Obama and President Xi of the People's Republic of China in Joint Press Conference», The White House, 25 de septiembre de 2015, accedido 13 de mayo de 2020, https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/remarks-president-obama-and-president-xi-peoples-republic-china-joint.

2. The White House, *National Security Strategy of the United States of America* (Washington, DC: The White House, 2017), 21, accedido 14 de mayo de 2020, https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

3. Commission on the Theft of American Intellectual Property, *Update to the PI Commission Report: The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy* (Seattle: National Bureau of Asian Research, febrero de 2017), 1, accedido 14 de mayo de 2020, http://ipcommission.org/report/IP_Commission_Report_Update_2017.pdf; Commission on the Theft of American Intellectual Property, *The PI Commission Report: The Theft of American Intellectual Property: Reassessments of the Challenge and United States Policy* (Seattle: National Bureau of Asian Research, mayo de 2013), 3, accedido 12 de junio de 2020, http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf.

4. Field Manual 3-0, *Operations* (Washington, DC: U.S. Government Publishing Office, 2017), 1-1–1-2.

5. Xi Jinping, «Garantizar una Victoria decisiva en el establecimiento de una sociedad moderadamente próspera en todos los aspectos y esforzarse por el gran éxito del socialismo con características chinas para una nueva era» (discurso, ante el 19º Congreso Nacional del Partido Comunista de China, Pekín, 10 de octubre de 2017), 25, accedido 16 de junio de 2020, http://www.xinhuanet.com/english/download/Xi_Jinping's_report_at_19th_CPC_National_Congress.pdf.

6. William C. Hannas, James Mulvenon y Anna B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernization* (New York: Routledge, 2013), 12.

7. Select Committee on U.S. National Security and Military/Commercial Concerns with the People's Republic of China, H. Rep. No. 105-851, at x–xi (1999), accedido 14 de mayo de 2020, https://www.govinfo.gov/content/pkg/GPO-CRPT-105hrpt851/pdf/GPO-CRPT-105hrpt851.pdf.

8. *Ibid*., 20–21.

9. James McGregor, *China's Drive for «Indigenous Innovation»: A Web of Industrial Policies* (Washington, DC: U.S. Chamber of Commerce, 2010), 2–5, accedido 14 de mayo de 2020, https://www.uschamber.com/report/china%E2%80%99s-drive-indigenous-innovation-web-industrial-policies.

10. *Ibid*., 4.

11. *Ibid*., 5.

12. Xi, «Garantizar una Victoria decisiva», 25.

13. Chuang Meng, «Deng Puts Forward New 12-Character Guiding Principle for Internal and Foreign Policies», *Ching Pao*, nro. 172 (1991): 84–86, citado en Office of the Secretary of Defense, *Annual Report to Congress: Military Power of the People's Republic of China 2006* (Washington, DC: Department of Defense [DOD], 2007), 7, accedido 14 de mayo de 2020, https://fas.org/nuke/guide/china/dod-2006.pdf.

14. Rogier Creemers, Paul Triolo y Graham Webster, «Translation: Cybersecurity Law of the People's Republic of China [Effective June 1, 2017]», Cybersecurity Initiative (blog), New America, 29 de junio de 2018, accedido 14 de mayo de 2020, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.

15. Ministry of Foreign Affairs and Trade and New Zealand Trade and Enterprise, «Understanding China's Cybersecurity Law: Information for New Zealand Businesses» (Wellington, Nueva Zelanda: National Cyber Security Centre, septiembre de 2017), accedido 14 de mayo de 2020, https://www.ncsc.govt.nz/assets/NCSC-Documents/Understanding-Chinas-cybersecurity-law.pdf.

16. National Intelligence Law of the People's Republic of China (promulgado por el Comité permanente del Congreso Popular Nacional, 27 de junio de 2017, vigente el 28 de junio de 2017), art. 7, accedido 16 de junio de 2020, https://cs.brown.edu/courses/csci1800/sources/2017_PRC_NationalIntelligenceLaw.pdf.

17. *Ibid*., art. 12.

18. Information Office of the State Council, «China's Military Strategy (texto completo)» (Pekín: The State Council, 27 de mayo de 2015), accedido 14 de mayo de 2020, http://english.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm. Los «dos centenarios» es una política implementada bajo el presidente Xi Jinping que se refiere al centenario del establecimiento del Partido Comunista de China en 2021, en el momento cuando los chinos establecerán una gran base económica y una clase media, y la fundación de la República Popular de China en 2049, cuando China se convertirá en un «país socialista fuerte, democrático, civilizado, armonioso y moderno». Esto generalmente se refiere

a la restauración de China como la potencia preeminente en el mundo.

19. Information Office of the State Council, «"Made in China 2025" Plan Issued», The State Council, 19 de mayo de 2015, accedido 14 de mayo de 2020, http://english.www.gov.cn/policies/latest_releases/2015/05/19/content_281475110703534.htm.

20. «Notice of the State Council on Printing and Distributing "Made in China 2025"», The State Council, 8 de mayo de 2015, accedido 14 de mayo de 2020, http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm.

21. White House Office of Trade and Manufacturing Policy, *How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World* (Washington, DC: The White House, junio de 2018), 16, accedido 14 de mayo de 2020, https://www.whitehouse.gov/wp-content/uploads/2018/06/FINAL-China-Technology-Report-6.18.18-PDF.pdf.

22. Meia Nouwens y Helena Legarda, «China's Pursuit of Advanced Dual-Use Technologies», International Institute for Strategic Studies, 18 de diciembre de 2018, accedido 10 de marzo de 2020, https://www.iiss.org/blogs/research-paper/2018/12/emerging-technology-dominance; Mike Yeo, «China's Military Capabilities are Booming, but Does Its Defense Industry Mirror That Trend?», Defense News, 14 de agosto de 2018, accedido 10 de marzo de 2020, https://www.defensenews.com/top-100/2018/08/14/chinas-military-capabilities-are-booming-but-does-its-defense-industry-mirror-that-trend/.

23. Stefan H. Verstappen, *The Thirty-Six Strategies of Ancient China* (San Francisco: China Books and Periodicals, 1999), 91–95.

24. Shou Xiaoson, ed., *The Science of Military Strategy*, trad. Chinese Academy of Military Science (Pekín: Military Science Press, 2013), 17.

25. *Ibid*., 3.

26. *Ibid*., 247–48.

27. The White House, *National Security Strategy*, 21.

28. Hannas, Mulvenon y Puglisi, *Chinese Industrial Espionage*, 25.

29. *Ibid*., 23–28.

30. *Ibid*., 24.

31. *Ibid*.

32. He Defang, «As for Indigenous Innovation, Information Should Go Ahead of Rest», *China Information Review* 10 (2006): 12-13, citado en Hannas, Mulvenon y Puglisi, *Chinese Industrial Espionage*, 38.

33. «Contracts», DOD, accedido 15 de mayo de 2020, https://DOD.defense.gov/News/Contracts/.

34. Chunlin Zhang, *How Much do State-Owned Enterprises Contribute to China's GDP and Employment* (Washington, DC: World Bank, 15 de julio de 2019), 10, accedido 15 de mayo de 2020, http://documents.worldbank.org/curated/en/449701565248091726/pdf/How-Much-Do-State-Owned-Enterprises-Contribute-to-China-s-GDP-and-Employment.pdf.

35. Office of Trade and Manufacturing Policy, *How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World*, 17–19.

36. Hannas, Mulvenon y Puglisi, *Chinese Industrial Espionage*, 93–94, 111.

37. *Ibid*., 79–80, 95.

38. «National High-tech R&D Program (863 Program)», Ministry of Science and Technology of the People's Republic of China, accedido 15 de mayo de 2020, http://en.most.gov.cn/eng/programmes1/200610/t20061009_36225.htm; «Chinese Scientist Huang Kexue Jailed for Trade Theft», BBC News, 22 de diciembre de 2011, accedido 15 de mayo de 2020, https://www.bbc.com/news/business-16297237.

39. «Made in China 2025», The State Council, 8 de mayo de 2015, accedido 15 de mayo de 2020, http://www.gov.cn/zhengce/content/2015-05/19/content_9784.htm.

40. Office of Trade and Manufacturing Policy, *How China's Economic Aggression Threatens the Technologies and Intellectual Property of the United States and the World*, 16.

41. *Ibid*., 17–20.

42. «Information About the Department of Justice's China Initiative and a Compilation of China-Related Prosecutions Since 2018», U.S. Department of Justice, accedido 15 de junio de 2020, https://www.justice.gov/opa/page/file/1223496/download.

43. Senate Comm. on Armed Services, Inquiry into Counterfeit Electronic Parts in the Department of Defense Supply Chain, S. Rep. No. 112-167, en vi–viii (2012), accedido 15 de mayo de 2020, https://www.armed-services.senate.gov/imo/media/doc/Counterfeit-Electronic-Parts.pdf.

44. *Ibid*., ii–iv.

45. Jordan Robertson y Michael Riley, «The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies», Bloomberg Businessweek, 4 de octubre de 2018, accedido 15 de mayo de 2020, https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies.

46. Jacob Kastrenakes, «Trump Signs Bill Banning Government Use of Huawei and ZTE Tech», The Verge, 13 de agosto de 2018, accedido 15 de mayo de 2020, https://www.theverge.com/2018/8/13/17686310/huawei-zte-us-government-contractor-ban-trump.

47. Hannas, Mulvenon y Puglisi, *Chinese Industrial Espionage*, 12.

48. *Ibid*., 136–37.

49. Alexander Bowe, *China's Overseas United Front Work: Background and Implications for the United States* (Washington, DC: U.S.-China Economic and Security Review Commission, 2018), 12, accedido 10 de junio de 2020, https://www.uscc.gov/sites/default/files/Research/China%27s%20Overseas%20United%20Front%20Work%20-%20Background%20and%20Implications%20for%20US_final_0.pdf.

50. *Ibid*., 10, 12.

51. *Ibid*., 10.

52. Michael Barr, *Who's Afraid of China?: The Challenge of Chinese Soft Power* (Londres: Zed Books, 2011), 67.

53. China's Non-Traditional Espionage against the United States: The Threat and Potential Policy Responses, Before the Senate Judicary Committee, 115th Cong. (2018) (declaración de E. W. «Bill» Priestap, Assistant Director of Counterintelligence Division, Federal Bureau of Investigation), accedido 18 de mayo de 2020, https://www.fbi.gov/news/testimony/chinas-non-traditional-espionage-against-the-united-states.

54. U.S. Department of Justice, «Harvard University

Professor and Two Chinese Nationals Charged in Three Separate China Related Cases», comunicado de prensa nro. 20-99, 28 de enero de 2020, accedido 15 de junio de 2020, https://www.justice.gov/opa/pr/harvard-university-professor-and-two-chinese-nationals-charged-three-separate-china-related.

55. Hannas, Mulvenon y Puglisi, *Chinese Industrial Espionage*, 156–57.

56. *Ibid*., 157.

57. *Ibid*., 188.

58. Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2019* (Washington, DC: DOD, 2019), 65, accedido 18 de mayo de 2020, https://media.defense.gov/2019/May/02/2002127082/-1/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf.

59. *Ibid*.

60. Verizon RISK Team, *2013 Data Breach Investigations Report* (Nueva York: Verizon, 2013), 21, accedido 18 de mayo de 2020, https://cybersecurity.idaho.gov/wp-content/uploads/sites/87/2019/04/data-breach-investigations-report-2013.pdf.

61. National Bureau of Asian Research, *Update to the PI Commission Report*, 11.

62. «Gen. Alexander: Greatest Transfer of Wealth in History», video en YouTube, publicado por «American Enterprise Institute», 9 de julio de 2012, 1:27, accedido 18 de mayo de 2020, https://www.youtube.com/watch?v=JOFk44yy6IQ.

63. U.S. Department of Justice, «U.S. Charges Five Chinese Military Hackers for Cyber Espionage Against U.S. Corporations and a Labor Organization for Commercial Advantage», comunicado de prensa nro. 14-528, 19 de mayo de 2014, accedido 18 de mayo de 2020, https://www.justice.gov/opa/pr/us-charges-five-chinese-military-hackers-cyber-espionage-against-us-corporations-and-labor.

64. *Ibid*.

65. FireEye iSight Intelligence, *Red Line Drawn: China Recalculates its Use of Cyber Espionage* (Milpitas, California: FireEye, junio de 2016), 3 y 15, accedido 18 de mayo de 2020, https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf.

66. Elsa Kania y John Costello, «The Strategic Support Force and the Future of Chinese Information Operations», *The Cyber Defense Review* 3, nro. 1 (Primavera de 2018): 106–7.

67. U.S.-China Economic and Security Review Commission, *2016 Report to Congress of the U.S.-China Economic and Security Review Commission* (Washington, DC: U.S. Government Publishing Office, 2016), 57, accedido 10 de junio de 2020, https://www.uscc.gov/sites/default/files/annual_reports/2016%20Annual%20Report%20to%20Congress.pdf.

68. Edward Wong, «How China Uses LinkedIn to Recruit Spies Abroad», *New York Times* (sitio web), 27 de agosto de 2019, accedido 18 de mayo de 2020, https://www.nytimes.com/2019/08/27/world/asia/china-linkedin-spies.html.

69. DOD 5220.22-M, *National Industrial Security Program Operating Manual* (Washington, DC: DOD, 2006, incorporating change 2, 18 de mayo de 2016), accedido 18 de mayo de 2020, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/DODm/522022M.pdf.

70. *Ibid*.; «FAR [Federal Acquisition Regulation]», Acquisition.gov, actualizado por última vez el 15 de mayo de 2020, accedido 18 de mayo de 2020, https://www.acquisition.gov/browse/index/far; «Defense Federal Acquisition Regulation Supplement [DFARS]», Acquisition.gov, actualizado por última vez el 18 de mayo de 2020, accedido 18 de mayo de 2020, https://www.acquisition.gov/dfars.

71. Ron Ross et al., *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*, NIST Special Publication 800-171, rev. 2 (Gaithersburg, Maryland: National Institute of Standards and Technology, febrero de 2020), accedido 18 de mayo de 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf.

72. «DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting (Dec 2019)», Office of the Under Secretary of Defense for Acquisition, 31 de diciembre de 2019, 252.204-7012(m)(2), accedido 10 de marzo de 2020, https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012.

73. «DFARS 252.204-7018 Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services (Dec 2019)», Office of the Under Secretary of Defense for Acquisition, 31 de diciembre de 2019, 252.204-7018, accedido 18 de mayo de 2020, https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7018.