



Espionaje económico de China: un desafío para la innovación y la seguridad empresarial

Estos últimos años, se ha presenciado un crecimiento sin precedentes del espionaje chino en todo occidente. Después de muchos casos de infiltración de espías chinos en empresas, servicios de inteligencia y ciberataques en diferentes países, los agentes de seguridad y los ministros de defensa han advertido que el espionaje procedente del gigante asiático representa una de las mayores amenazas para la seguridad del mundo occidental.

En los 80, occidente decidió abrir sus puertas a China y dejarla participar en el sistema internacional multilateral junto a las demás superpotencias mundiales, las cuales gobernaban el orden. Occidente pensó que, tras integrar a China en el orden mundial, esta adoptaría los estándares y los valores correspondientes. No obstante, China nunca se adaptó al sistema multilateral ni aceptó su narrativa de derechos humanos, paz y seguridad. Según John Demers, un abogado del Departamento de Justicia de los Estados Unidos, estamos presenciando una China cada vez más letal, con mayores recursos y una metodología más rigurosa para llevar a cabo el robo de información.

Las relaciones económicas que ha mantenido China con Occidente estos últimos años, se han desarrollado bajo un halo de aparente respeto, honestidad y transparencia. Sin embargo, según advierten los servicios de inteligencia, lo que hay detrás de cada interacción es muy diferente a lo que se percibe desde la superficie. A través de la cooperación académica, comercial y tecnológica con empresas y gobiernos occidentales, China logró acceder a datos confidenciales e información secreta de alto nivel en múltiples áreas, especialmente en los sectores tecnológicos y de telecomunicaciones.

Desde que China se incorporó al sistema internacional, los casos de robo de información sensible en empresas occidentales por parte de espías chinos no han hecho más que aumentar. Uno de los casos más famosos es el de Cao Guangzhi, quien fue denunciado por robar el código fuente de las funciones “Autopilot” de los coches Tesla para una compañía china, Xiaopeng Motors. Estas transferencias no autorizadas de tecnología avanzada suponen una gran pérdida de dinero para la empresa afectada. Según Tesla, invirtieron cientos de millones de dólares y cinco años de trabajo en desarrollarla.

Estos robos son extremadamente dañinos, ya que se llevan a cabo en sectores estratégicos para obtener ventajas en los mercados internacionales. Esto conlleva que la empresa perjudicada pierda su ventaja competitiva en el mercado, su posicionamiento estratégico dentro de él, su independencia, la confianza de los clientes y talento. Pero estos robos no solo afectan a las empresas, sino que también suponen un alto riesgo para la seguridad de sus países y para los derechos fundamentales de sus ciudadanos.

China ha sido responsable en muchas ocasiones del robo de tecnologías de alto riesgo pertenecientes a otros países, particularmente en sectores clave como la IA, las telecomunicaciones y la biotecnología. Esta situación es alarmante porque

la ausencia de regulaciones está permitiendo violaciones sistemáticas de derechos humanos. A través de plataformas digitales como LinkedIn los agentes chinos violan los derechos de privacidad y protección de datos de los empleados al recolectar información sensible - sobre ellos y sobre su empresa - sin su consentimiento. Por otra parte, no solo adquieren este conocimiento de forma ilícita, sino que además someten a chantaje y a extorsión a empleados con dificultades económicas o personales, dejándolos en una situación más vulnerable y con menor autonomía. mercats internacionals.

Estas transferencias ilegales no solo afectan a los empleados de las empresas afectadas, sino que también afectan a los ciudadanos del país que las lleva a cabo. Dado que China es un país autoritario que ha cometido, y todavía sigue cometiendo, muchas violaciones de derechos humanos, el acceso a tecnología avanzada que podría utilizarse para controlar a su ciudadanía es motivo de gran preocupación. China puede usar esta tecnología para rastrear, monitorear y recopilar de manera masiva información sobre su población y utilizarla después como arma para controlarla y reprimirla.

Fionnuala Ní Aoláin, ex-relatora especial de la ONU sobre la promoción y protección de los derechos humanos, afirmó que “en ausencia de regulación, el coste para los derechos humanos sólo puede aumentar sin que haya un final a la vista”. Desde Naciones Unidas se ha hecho un llamado a todos los países para pedir que establezcan métodos de defensa adecuados con el fin de protegerse de este tipo de espionaje.

Este uso de tecnología avanzada no solo plantea serias preocupaciones para los derechos humanos, sino que también es un componente clave de la estrategia global de China. Mientras persigue la consolidación de su poder interno, China también utiliza el espionaje como una herramienta para lograr sus metas geopolíticas.



Imatge extreta del reportatge de la BBC "*Looking for China's Spies*", amb crèdits fotogràfics generals a Getty Images, Alamy, Creative Commons i Facebook

El espionaje chino tiene como objetivo, además de la estabilidad del régimen comunista, consolidar su hegemonía global.

Para lograrlo, es necesario generar crecimiento económico, y por ello, China quiere adquirir alta tecnología para fortalecer su economía, reducir su dependencia de otros países y, sobre todo, posicionarse como líder mundial. Una de las diferencias clave entre el espionaje chino y el occidental es que Pekín da información recopilada por sus servicios de inteligencia a las empresas nacionales chinas, para así proporcionarles más competitividad económica en el mercado internacional. En China, el gobierno involucra a toda la sociedad - ciudadanos, empresas y otros organismos - para que colaboren con ellos con el objetivo de recopilar información sensible sobre otros países. Esto se debe a que el estado está profundamente relacionado con las empresas, y las leyes chinas obligan a las empresas a cooperar con el gobierno, lo cual implica participar en actividades de espionaje o colaborar con el MSS, el servicio de inteligencia Chino.

Una de las tácticas empleadas por China para obtener información confidencial de empresas occidentales consiste en establecer contacto con sus empleados a través de plataformas digitales como LinkedIn. Los empleados suelen ser abordados por individuos que se hacen pasar por empresarios chinos, los cuales son en realidad espías. Su misión tiene como objetivo establecer una relación cercana con el empleado, aparentemente inofensiva, ofreciendo oportunidades laborales por grandes cantidades de dinero. Progresivamente, estos individuos empiezan a pedir información sensible relacionada con la tecnología o las estrategias comerciales de la empresa. En muchos casos, la mayoría de los empleados no perciben las intenciones de los agentes extranjeros hasta que la información ya ha sido comprometida.

Los servicios de inteligencia no lograron ver la gran amenaza que representaba este espionaje, ya que durante mucho tiempo estuvieron centrados en otros asuntos. Nigel Inkster, quien fue el segundo al mando de la MI6 hasta su retiro en 2006, declaró que, en los años que China estaba emergiendo como una gran superpotencia mundial, los servicios de inteligencia se encontraban distraídos, tratando de combatir el terrorismo. Aunque los servicios de inteligencia no siempre detectaban la actividad de espionaje, muchas empresas occidentales eran conscientes de las amenazas a las que se enfrentaban. Sin embargo, a menudo optaban por permanecer en silencio, ya que tenían miedo de arriesgar sus relaciones comerciales con China y de perder su lugar en su mercado.

A día de hoy, muchos funcionarios de alto nivel siguen advirtiendo que se siguen sin tomar las medidas necesarias para combatir este espionaje. Europa y Estados Unidos están decididos a responder a estos ataques; sin embargo, según un artículo publicado por la BBC, se sostiene que estos han quedado en gran desventaja con China en lo que respecta a su red de inteligencia. Ahora se muestran vulnerables y en riesgo muy alto de posibles infiltraciones, robos, ciberataques masivos y más.

Ariadna Moré Andrés
Blanquerna URL
Grado en Relaciones Internacionales

Fuentes de referencia:



Asociación para las
Naciones Unidas
en España
United Nations Association of Spain

Noviembre 2024

- Joske, A. (2020). Economic espionage. In *Hunting the phoenix: The Chinese Communist Party's global search for technology and talent* (pp. 22–24). Australian Strategic Policy Institute. <http://www.jstor.org/stable/resrep26119.8>
- Yong, N. (2023, 26 enero). *Cómo China consigue robarle sus secretos tecnológicos a Estados Unidos*. BBC News Mundo. <https://www.bbc.com/mundo/noticias-internacional-64355527>
- Caminiti, S. (2024, 5 junio). *Chinese spies are targeting disgruntled workers within U.S. corporations, warns national counterintelligence head Michael Casey*. CNBC. <https://www.cnbc.com/2024/06/04/china-spies-targeting-disgruntled-us-workers-counterintelligence-head.html>
- De Diego Cerezo, M. (2024, 13 junio). *Guoanbu, la gran herramienta China de espionaje para cambiar el Orden Mundial*. RTVE.es. <https://www.rtve.es/noticias/20240613/guoanbu-gran-herramienta-china-espionaje-para-cambiar-orden-mundial/16120870.shtml>
- Corera, G. (2024, 22 mayo). *Cómo ha aumentado la amenaza del espionaje chino (y por qué Occidente no ha logrado combatirlo)*. BBC News Mundo. <https://www.bbc.com/mundo/articles/c84z9q41zd0o>
- Hawkins, A. (2024, 8 mayo). *'Countries are now forced to confront it': Rise in Chinese espionage arrests alarms Europe*. The Guardian. <https://www.theguardian.com/world/article/2024/may/08/court-chinese-espionage-europe>
- Walton, C. (2023, 28 abril). *China Has Been Waging a Decades-Long, All-Out Spy War on the United States*. Foreign Policy. <https://foreignpolicy.com/2023/03/28/china-has-been-waging-a-decades-long-all-out-spy-war/>
- Anand, A. (2023, 15 febrero). *Global Watch | From 'Guoanbu' to Xinhua, how China's espionage network operates in shadows*. Firstpost. <https://www.firstpost.com/opinion/global-watch-from-guoanbu-to-xinhua-how-chinas-espionage-network-operates-in-shadows-12157062.html>
- Dezenski, E., & Rader, D. (2023, 22 septiembre). *How China Uses Shipping to Spy on the West*. Foreign Policy. <https://foreignpolicy.com/2023/09/20/china-shipping-maritime-logistics-lanes-trade-ports-security-espionage-intelligence/>
- Giglio, M. (2019, 30 agosto). *Inside the U.S.-China Espionage War*. The Atlantic. <https://www.theatlantic.com/politics/archive/2019/08/inside-us-china-espionage-war/595747/>
- Redacción. (2022, 7 julio). *La advertencia sin precedentes del FBI y el MI5 sobre «la inmensa amenaza» que representa China*. BBC News Mundo. <https://www.bbc.com/mundo/noticias-62074574>
- Debusmann, B., Jr. (2022, 12 julio). *Cómo China usa espías para vigilar y desacreditar a disidentes que viven en Estados Unidos*. BBC News Mundo. <https://www.bbc.com/mundo/noticias-internacional-62117259>
- Kobelinsky, F. (2023, 1 julio). *Los espías chinos están en todos lados: cómo se tejió la mega red que nació en los burdeles de Shanghai y se infiltró en el mundo*. Infobae. <https://www.infobae.com/america/mundo/2023/07/01/los-espias-chinos-estan-en-todos-lados-como-se-tejio-la-mega-red-que-nacio-en-los-burdeles-de-shanghai-y-se-infiltra-en-el-mundo/>
- Iriarte, D. (2024, 24 abril). *¿Qué hacemos con los espías de China? El gran desafío de la contrainteligencia europea*. elconfidencial.com. https://www.elconfidencial.com/mundo/2024-04-24/desafio-contrainteligencia-europea-espias-china_3872322/
- Wheeler, T. (2024, 20 noviembre). *Chinese spies and the security of America's networks*. Brookings. <https://www.brookings.edu/articles/chinese-spies-and-the-security-of-americas-networks/>



**Asociación para las
Naciones Unidas
en España**
United Nations Association of Spain

Noviembre 2024

Publicado por



**Asociación para las
Naciones Unidas
en España**
United Nations Association of Spain

Con el apoyo de



**Generalitat
de Catalunya**

ANUE no hace necesariamente como suyas las opiniones expresadas por sus colaboradores.