Associació per a les Nacions Unides a Espanya
United Nations Association of Spain

Novembre 2024

Espionatge Econòmic de la Xina: Un Desafiament per a la Innovació i la Seguretat Empresarial

Aquests últims anys, s'ha presenciat un creixement sense precedents de l'espionatge xinès en tot occident. Després de molts casos d'infiltració d'espies xinesos en empreses, serveis d'intel·ligència i ciberatacs en diferents països, els agents de seguretat i els ministres de defensa han advertit que l'espionatge procedent del gegant asiàtic representa una de les majors amenaces per a la seguretat del món occidental.

En els 80, occident va decidir obrir les seves portes a la Xina i deixar-la participar en el sistema internacional multilateral al costat de les altres superpotències mundials, les quals governaven l'ordre. Occident va pensar que, després d'integrar a la Xina en l'ordre mundial, aquesta adoptaria els estàndards i els valors corresponents. No obstant això, la Xina mai es va adaptar al sistema multilateral ni va acceptar la seva narrativa de drets humans, pau i seguretat. Segons John Demers, un advocat del Departament de Justícia dels Estats Units, estem presenciant una Xina cada vegada més letal, amb majors recursos i una metodologia més rigorosa per a dur a terme el robatori d'informació.

Les relacions econòmiques que ha mantingut Xina amb Occident aquests últims anys, s'han desenvolupat sota un halo d'aparent respecte, honestedat i transparència. No obstant això, segons adverteixen els serveis d'intel·ligència, el que hi ha darrere de cada interacció és molt diferent del que es percep des de la superfície. A través de la cooperació acadèmica, comercial i tecnològica amb empreses i governs occidentals, la Xina va aconseguir accedir a dades confidencials i informació secreta d'alt nivell en múltiples àrees, especialment en els sectors tecnològics i de telecomunicacions.

Des que la Xina es va incorporar al sistema internacional, els casos de robatori d'informació sensible en empreses occidentals per part d'espies xinesos no han fet més que augmentar. Un dels casos més famosos és el de Cao Guangzhi, qui va ser denunciat per robar el codi font de les funcions “Autopilot” dels cotxes Tesla per a una companyia xinesa, Xiaopeng Motors. Aquestes transferències no autoritzades de tecnologia avançada suposen una gran pèrdua de diners per a l'empresa afectada. Segons Tesla, van invertir centenars de milions de dòlars i cinc anys de treball a desenvolupar-la.

Aquests robatoris són extremadament nocius, ja que es duen a terme en sectors estratègics per a obtenir avantatges en els mercats internacionals. Això comporta que l'empresa perjudicada perdi el seu avantatge competitiu en el mercat, el seu posicionament estratègic dins d'ell, la seva independència, la confiança dels clients i talent. Però aquests robatoris no sols afecten les empreses, sinó que també suposen un alt risc per a la seguretat dels seus països i per als drets fonamentals dels seus ciutadans.

La Xina ha estat responsable en moltes ocasions del robatori de tecnologies d'alt risc pertanyents a altres països, particularment en sectors clau com la IA, les telecomunicacions i la biotecnologia. Aquesta situació és alarmant perquè

l'absència de regulacions està permetent violacions sistemàtiques de drets humans. A través de plataformes digitals com Linkedin els agents xinesos violen els drets de privacitat i protecció de dades dels empleats en recol·lectar informació sensible - sobre ells i sobre la seva empresa - sense el seu consentiment. D'altra banda, no sols adquireixen aquest coneixement de manera il·lícita, sinó que a més sotmeten a xantatge i a extorsió a empleats amb dificultats econòmiques o personals, deixant-los en una situació més vulnerable i amb menor autonomia.

Aquestes transferències il·legals no sols afecten els empleats de les empreses afectades, sinó que també afecten els ciutadans del país que les duu a terme. Atès que la Xina és un país autoritari que ha comès, i encara continua cometent, moltes violacions de drets humans, l'accés a tecnologia avançada que podria utilitzar-se per a controlar a la seva ciutadania és motiu de gran preocupació. la Xina pot usar aquesta tecnologia per a rastrejar, monitorar i recopilar de manera massiva informació sobre la seva població i utilitzar-la després com a arma per a controlar-la i reprimir-la.

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

Fionnuala Ní Aoláin, ex-relatora especial de l'ONU sobre la promoció i protecció dels drets humans, va afirmar que "en absència de regulació, el cost per als drets humans només pot augmentar sense que hi hagi un final a la vista". Des de Nacions Unides s'ha fet un anomenat a tots els països per a demanar que estableixin mètodes de defensa adequats amb la finalitat de protegir-se d'aquesta mena d'espionatge.

Aquest ús de tecnologia avançada no sols planteja serioses preocupacions per als drets humans, sinó que també és un component clau de l'estratègia global de la Xina. Mentre persegueix la consolidació del seu poder intern, la Xina també utilitza l'espionatge com una eina per a aconseguir les seves metes geopolítiques.

L'espionatge xinès té com a objectiu, a més de l'estabilitat del règim comunista, consolidar la seva hegemonia global. Per a

aconseguir-ho, és necessari generar creixement econòmic, i per això, la Xina vol adquirir alta tecnologia per a enfortir la seva economia, reduir la seva dependència d'altres països i, sobretot, posicionar-se com a líder mundial. Una de les diferències clau entre l'espionatge xinès i l'occidental és que Pequín dona informació recopilada pels seus serveis d'intel·ligència a les empreses nacionals xineses, per a així proporcionar-los més competitivitat econòmica en el mercat internacional. A la Xina, el govern involucra a tota la societat - ciutadans, empreses i altres organismes - perquè col·laborin amb ells amb l'objectiu de recopilar informació sensible sobre altres països. Això es deu al fet que l'estat està profundament relacionat amb les empreses, i les lleis xineses obliguen les empreses a cooperar amb el govern, la qual cosa implica participar en activitats d'espionatge o col·laborar amb el MSS, el servei d'intel·ligència Xinès.

Una de les tàctiques emprades per la Xina per a obtenir informació confidencial d'empreses occidentals consisteix a establir contacte amb els seus empleats a través de plataformes digitals com Linkedin. Els empleats solen ser abordats per individus que es fan passar per empresaris xinesos, els quals són en realitat espies. La seva missió té com a objectiu establir una relació pròxima amb l'empleat, aparentment inofensiva, oferint oportunitats laborals per grans quantitats de diners. Progressivament, aquests individus comencen a demanar informació sensible relacionada amb la tecnologia o les estratègies comercials de l'empresa. En molts casos, la majoria dels empleats no perceben les intencions dels agents estrangers fins que la informació ja ha estat compromesa.

Els serveis d'intel·ligència no van aconseguir veure la gran amenaça que representava aquest espionatge, ja que durant molt de temps van estar centrats en altres assumptes. Nigel Inkster, qui va ser el segon al comandament de la MI6 fins al seu retir en 2006, va declarar que, en els anys que la Xina estava emergint com una gran superpotència mundial, els serveis d'intel·ligència es trobaven distrets, tractant de combatre el terrorisme. Encara que els serveis d'intel·ligència no sempre detectaven l'activitat d'espionatge, moltes empreses occidentals eren conscients de les amenaces a les quals s'enfrontaven. No obstant això, sovint optaven per romandre en silenci, ja que tenien por d'arriscar les seves relacions comercials amb la Xina i de perdre el seu lloc en el seu mercat.

Avui dia, molts funcionaris d'alt nivell continuen advertint que se segueixen sense prendre les mesures necessàries per a combatre aquest espionatge. Europa i els Estats Units estan decidits a respondre a aquests atacs; no obstant això, segons un article publicat per la BBC, se sosté que aquests han quedat en gran desavantatge amb la Xina pel que fa a la seva xarxa d'intel·ligència. Ara es mostren vulnerables i en risc molt alt de possibles infiltracions, robatoris, ciberatacs massius i més.

Ariadna Moré Andrés
Blanquerna URL
Grau en Relacions Internacionals

Fonts de referència:

Associació per a les Nacions Unides a Espanya
United Nations Association of Spain

Novembre 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-infiltro-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/*

Associació per a les Nacions Unides a Espanya
United Nations Association of Spain

Novembre 2024

Publicat per

Associació per a les Nacions Unides a Espanya
United Nations Association of Spain

Amb el suport de

Generalitat de Catalunya