THE NEW YORK TIMES

Espías, hackeos y agencias de seguridad: la otra cara de las vacunas contra el coronavirus

Las guerras de los servicios de inteligencia por la investigación de vacunas se han intensificado a medida que China y Rusia amplían sus esfuerzos para robarse el trabajo estadounidense, tanto en institutos de investigación como en empresas.

El F.B.I. ha advertido a los funcionarios de la Universidad de Carolina del Norte en Chapel Hill sobre los intentos de China de piratear sus proyectos de investigación sobre el virus.Credit...Gerry Broome/Associated Press

Por Julian E. Barnes y Michael Venutolo-Mantovani

WASHINGTON — Los piratas cibernéticos del servicio de inteligencia china pretendían robar la información sobre la vacuna para el coronavirus, así que se enfocaron en lo que creían que sería un objetivo fácil. En vez de ir tras las empresas farmacéuticas, hicieron una incursión digital en la Universidad de Carolina del Norte y en otras instituciones que realizan investigaciones de vanguardia.

Pero no eran los únicos espías que estaban en acción. El servicio de inteligencia más importante de Rusia, el SVR, se enfocó en las redes de instituciones que realizan trabajos de investigación sobre las vacunas en Estados Unidos, Canadá y el Reino Unido, un intento de espionaje que fue detectado por una agencia británica de espionaje que monitorea los cables internacionales de fibra óptica.

Irán también ha intensificado sus intentos de robar información relacionada con las investigaciones para desarrollar vacunas, y Estados Unidos ha reforzado sus propias iniciativas para rastrear las labores de espionaje de sus adversarios y robustecer sus defensas.

En pocas palabras, todos los servicios importantes de espionaje intentan averiguar qué están haciendo los demás.

Según entrevistas con agentes y exagentes de inteligencia, y con personas que analizan los trabajos de espionaje, la pandemia del coronavirus ha provocado uno de los cambios más rápidos de los

últimos tiempos para las agencias mundiales de inteligencia —en cuanto a las misiones en tiempos de paz—, lo que ha hecho que se enfrenten en una nueva dinámica de espionaje mutuo.

Casi todos los adversarios de Estados Unidos intensificaron sus intentos de robar las investigaciones estadounidenses mientras que Washington, a su vez, ha implementado una estrategia de protección de las universidades y las empresas cuyos proyectos van más avanzados. Según un funcionario occidental que conoce las tareas de inteligencia, el servicio de inteligencia de la OTAN, que por lo general vigila el movimiento de los tanques rusos y las células terroristas, se ha expandido con el fin de detectar las maniobras del Kremlin para robar las investigaciones sobre las vacunas.

Esta competencia nos recuerda la carrera espacial, en la que la Unión Soviética y Estados Unidos dependían de sus servicios de inteligencia para saber cuándo era probable que el otro alcanzaría sus objetivos. Pero a diferencia de la competencia por llegar a la órbita terrestre y a la luna que se desarrolló durante décadas en la Guerra Fría, el plazo para conseguir la información sobre los tratamientos para el coronavirus es excesivamente limitado puesto que, con el paso de los días, la necesidad de poseer una vacuna se vuelve cada vez más urgente.

“Lo sorprendente sería que no estuvieran tratando de robar las investigaciones biomédicas más valiosas que se están llevando a cabo en este momento”, dijo el mes pasado durante un evento organizado por el Centro de Estudios Estratégicos e Internacionales, John C. Demers, un alto funcionario del Departamento de Justicia, refiriéndose a China. “Valiosas desde un punto de vista económico, e invaluables desde un punto de vista geopolítico”.

Según un funcionario que conoce los servicios de inteligencia, la ofensiva de China es compleja. Sus agentes también han usado de manera subrepticia los datos de la Organización Mundial de la Salud en sus intentos de hackear la información concerniente a las vacunas, tanto en Estados Unidos como en Europa.

No se sabía exactamente cómo es que China estaba usando su posición privilegiada en la OMS para recabar información sobre los proyectos de vacunas en todo el mundo. La organización reúne información acerca de los proyectos que se están desarrollando y, aunque en determinado momento se da a conocer al público la mayor parte de esos datos, los piratas cibernéticos chinos podrían haber obtenido, de manera anticipada, información sobre los trabajos de investigación para las vacunas contra el coronavirus que la OMS veía como más prometedores, según asegura un exfuncionario de inteligencia.

Según exfuncionarios y funcionarios actuales de Estados Unidos, los agentes de ese país se enteraron sobre las intenciones de China a principios de febrero, cuando el virus estaba ganando terreno en Estados Unidos. La CIA y otras agencias vigilaron atentamente los movimientos de China dentro de los organismos internacionales, incluyendo la OMS.

Las conclusiones del servicio de inteligencia hicieron que la Casa Blanca adoptara en mayo una postura firme con respecto a la OMS, según el exagente de inteligencia.

Los funcionarios estadounidenses afirmaron que, además de la Universidad de Carolina del Norte, los atacantes chinos también se han enfocado en otras universidades de todo el país, y es posible que hayan vulnerado algunas de sus redes. En su discurso, Demers señaló que China había realizado

“múltiples hackeos” que van más allá de los que reveló el Departamento de Justicia en una denuncia que hizo en julio, donde acusaba a dos piratas informáticos de trabajar para el servicio de espionaje del Ministerio de Seguridad Pública de China y estar buscando información sobre las investigaciones de las empresas de biotecnología estadounidenses.

De acuerdo con dos personas que conocen la situación, en las últimas semanas el FBI advirtió a los directivos de la Universidad de Carolina del Norte sobre los intentos de ataques informáticos. Los equipos de piratas cibernéticos chinos estaban tratando de ingresar en las redes informáticas del departamento de epidemiología de la institución, pero no lo lograron.

Leslie Minton, una vocera de esa institución, señaló que la universidad “recibe con frecuencia alertas por parte de los organismos de seguridad de Estados Unidos”. Las demás preguntas las canalizó al gobierno federal, pero dijo que ese centro de estudios ha invertido en “equipos de monitoreo permanente” para “ayudar a proteger contra amenazas avanzadas y persistentes de organizaciones auspiciadas por otros gobiernos”.

Además de hackear, China ha hecho incursiones en las universidades de otras maneras. Algunos funcionarios del gobierno creen que trata de aprovecharse de los acuerdos de investigación que las universidades estadounidenses han establecido con algunas instituciones chinas.

Otros han advertido que agentes de inteligencia chinos en Estados Unidos y en otros lugares han intentado recabar información sobre los investigadores. El 22 de julio, el gobierno de Trump ordenó que China cerrara su consulado en Houston en parte debido a que, según el FBI, los agentes chinos lo usaron como un puesto de avanzada para hacer incursiones con los expertos médicos de la ciudad.

En buena medida, los agentes de inteligencia chinos se enfocan en las universidades porque creen que la protección de datos de esas instituciones es menos sólida que la de las empresas farmacéuticas. Pero el espionaje también se ha intensificando a medida que los investigadores someten las vacunas, y tratamientos antivirales, a la evaluación de los expertos, lo que les proporciona a los adversarios mayores posibilidades de tener acceso a las fórmulas y estrategias para el desarrollo de las vacunas, comentó un funcionario del gobierno estadounidense que conoce el trabajo de inteligencia.

Hasta ahora, los agentes creen que los espías extranjeros han obtenido poca información de algunas de las empresas de biotecnología estadounidenses que espiaron como Gilead Sciences, Novavax y Moderna.

Investigadores de un laboratorio en Shenyang, China, que trabajan en una vacuna contra el coronavirus.Credit...Noel Celis/Agence France-Presse — Getty Images

Al mismo tiempo que la agencia británica de investigación en seguridad electrónica, GCHQ, se enteraba de los intentos de Rusia y que el servicio de inteligencia estadounidense detectaba el hackeo de China, el Departamento de Seguridad Nacional y el FBI mandaron a sus equipos a trabajar con las instituciones de biotecnología estadounidenses con el fin de reforzar la protección de sus redes informáticas.

Los intentos de Rusia, denunciados en julio por las agencias de inteligencia británicas, estadounidenses y canadienses, se concentraban principalmente en reunir información sobre las investigaciones de la Universidad de Oxford y de su socio empresarial farmacéutico, AstraZeneca.

Los rusos que atraparon tratando de obtener la información relacionada con la vacuna formaban parte del grupo conocido como Cozy Bear, un conjunto de hackers afiliados al SVR. Este fue uno de los grupos de piratas informáticos que ingresó en los servidores del Partido Demócrata en 2016.

Los funcionarios de seguridad nacional alertaron a las empresas farmacéuticas y a las universidades sobre los ataques y han ayudado a las instituciones para que verifiquen su seguridad. En su mayoría, los agentes han observado que los posibles atacantes usan las vulnerabilidades conocidas que tienen que corregirse, no las armas cibernéticas sofisticadas que atacan las deficiencias desconocidas en los círculos de seguridad informática.

Ninguna empresa ni universidad ha denunciado algún robo de información como resultado de los hackeos reconocidos públicamente. Pero, de acuerdo con un funcionario gubernamental estadounidense, algunos de los intentos de hackeo tuvieron éxito al menos desde el punto de vista de violar los blindajes e introducirse a las redes informáticas. Además, según los agentes de inteligencia, los piratas informáticos chinos y rusos hacen pruebas de vulnerabilidades todos los días.

“En verdad es una carrera contra el tiempo para que los buenos encuentren las vulnerabilidades, las corrijan e implementen esas correcciones antes de que el adversario las encuentre y las aproveche”, señaló Bryan S. Ware, director adjunto de seguridad informática en la Agencia de Ciberseguridad e Infraestructura del Departamento de Seguridad Nacional. “La competencia está más cerrada que nunca”.

Aunque solo se ha reconocido públicamente la existencia de dos equipos de piratas informáticos, uno de Rusia y otro de China, de acuerdo con agentes de los servicios de inteligencia y de las fuerzas policiales, varios equipos de hackeo de casi todas las agencias de inteligencia de esos países han tratado de robar información relacionada con las vacunas.

El 11 de agosto, Rusia anunció que había aprobado una vacuna, una declaración que levantó sospechas de que, como mínimo, a sus científicos los había ayudado el trabajo de sus agencias de espionaje con el robo de información a otros países.

Los funcionarios estadounidenses insisten en que los esfuerzos de sus servicios de espionaje son defensivos y que no se ha ordenado robar la investigación del coronavirus. Pero otros funcionarios de inteligencia actuales, y algunos agentes retirados, dijeron que la realidad no era en blanco y negro. Mientras las agencias de inteligencia estadounidenses intentan averiguar qué pueden haber robado Rusia, China e Irán, podrían encontrar información sobre la investigación de esos países y recopilarla.

Los funcionarios expresaron su preocupación ante la posibilidad de que nuevos intentos de piratería podrían afectar los esfuerzos de desarrollo de vacunas. Los piratas informáticos que extraen datos podrían dañar los sistemas de investigación de manera inadvertida o intencionada.

“Cuando un adversario ejecuta un ataque es muy probable que no solo robe información, sino que de alguna manera también interrumpa las redes operativas de la víctima”, dijo Ware.

Aunque es posible que parte del espionaje de Rusia y China se enfoque en verificar sus propias investigaciones o buscar atajos, algunos funcionarios actuales y anteriores plantearon la posibilidad de que los países intenten sembrar la desconfianza en una eventual vacuna de los países occidentales.

Tanto Rusia como China ya han difundido desinformación sobre el virus, sus orígenes y la respuesta estadounidense. Los servicios de inteligencia rusos, en particular, están sentando las bases para un esfuerzo más agresivo que busca intensificar el movimiento contra las vacunas en Occidente y podrían usar las acusaciones de espionaje para darle mayor tracción a su narrativa.

Desde hace mucho tiempo, Rusia ha tratado de acrecentar las divisiones de la sociedad estadounidense. Tanto los exagentes de seguridad nacional, como los que actualmente están en servicio, dijeron que creían que en algún momento Rusia divulgaría desinformación acerca de la vacuna aprobada en Occidente.

“Parece que estamos ante un caso de retroceso a la antigua Unión Soviética”, comentó Fiona Hill, una exfuncionaria del Consejo de Seguridad Nacional y experta en Rusia que testificó en las audiencias del juicio político contra el presidente Donald Trump. “Los rusos y los chinos han lanzado campañas de desinformación. ¿Qué mejor forma de crear confusión y debilitar aún más a Estados Unidos que promover el movimiento antivacunas? Pero asegúrense de que toda su gente esté vacunada”.

David E. Sanger y Ronen Bergman colaboraron con este reportaje.

Julian E. Barnes es un reportero de seguridad nacional radicado en Washington, donde cubre la labor de las agencias de inteligencia. Antes de unirse a The New York Times en 2018, escribió sobre asuntos de seguridad para The Wall Street Journal.@julianbarnes Facebook

---

Julian E. Barnes is a national security reporter based in Washington, covering the intelligence agencies. Before joining The Times in 2018, he wrote about security matters for The Wall Street Journal. @julianbarnes • Facebook