LA ÚLTIMA OLA DE ATAQUES NOS ACERCA AÚN MÁS A LA 'CIBERGUERRA FRÍA'

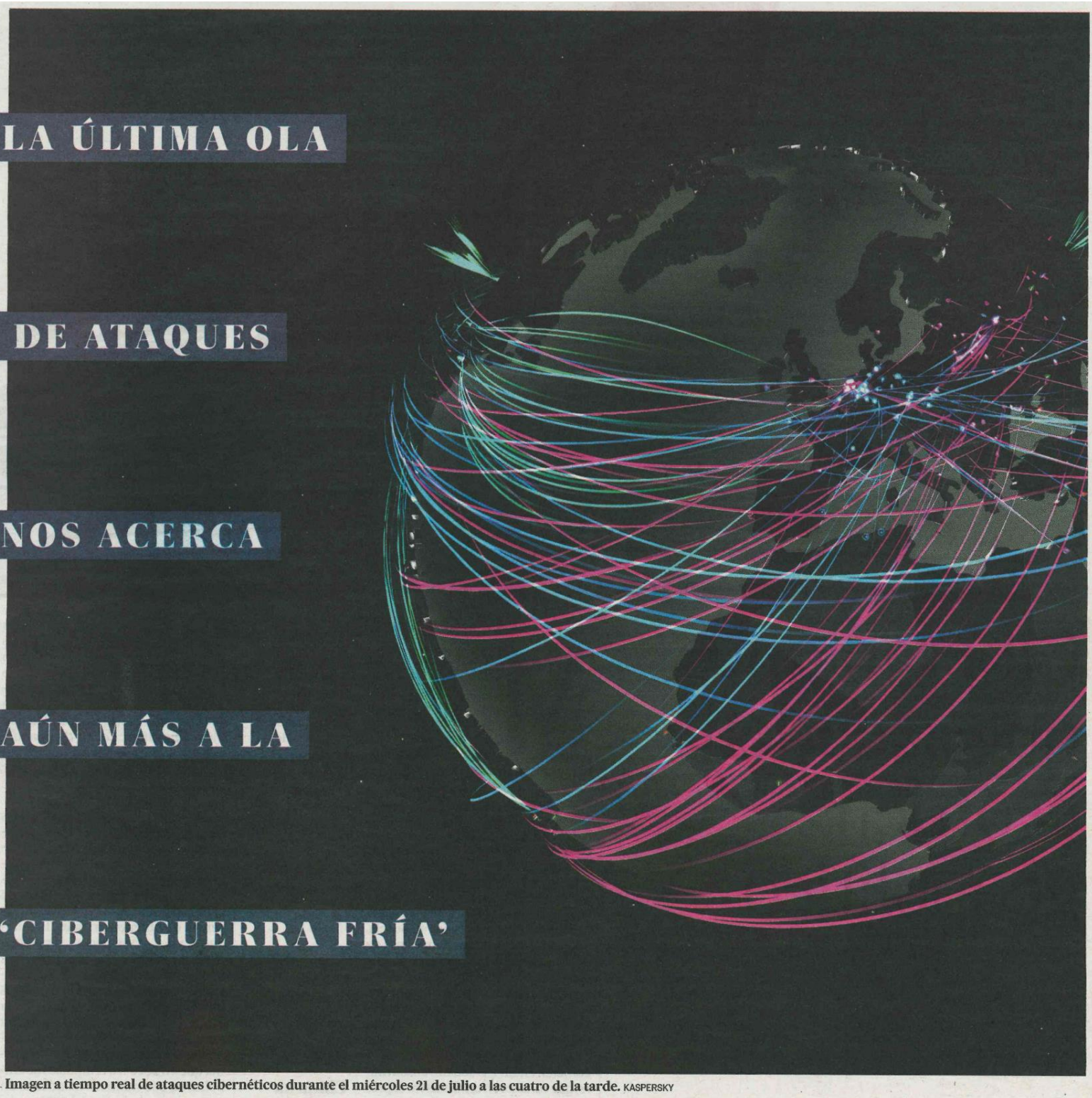
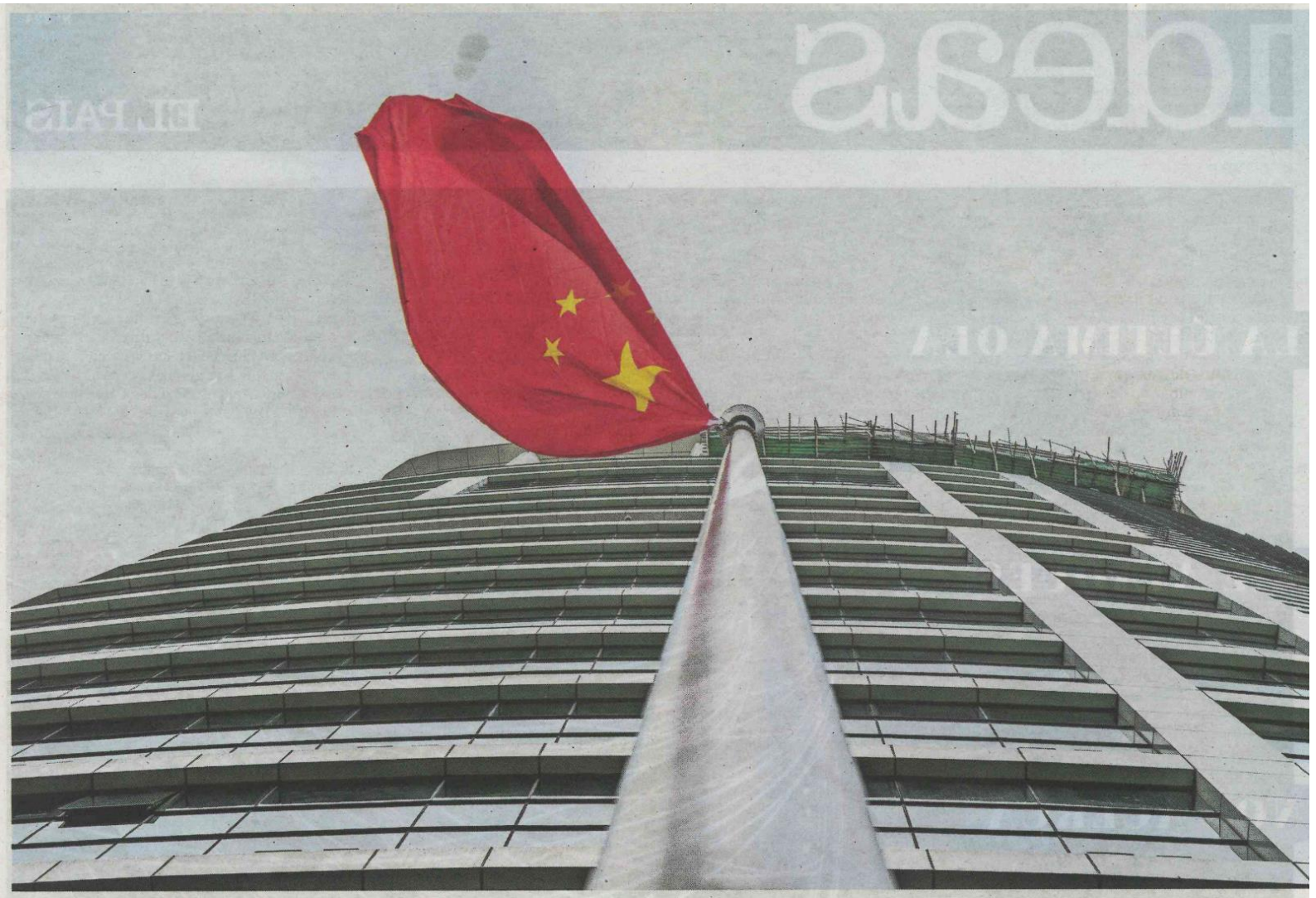


Imagen a tiempo real de ataques cibernéticos durante el miércoles 21 de julio a las cuatro de la tarde. KASPERSKY

Los ciberataques viven días álgidos. EE UU sufrió a principios de julio uno colosal que afectó a cerca de 200 empresas. Los servicios de inteligencia de las grandes potencias vigilan con inquietud a *hackers* que atacan tanto grandes infraestructuras de naciones rivales como compañías y comercios mediante extorsiones en línea. Los presidentes Joe Biden y Vladímir Putin abordaron el problema en su reciente encuentro en Ginebra. Y esta semana, Estados Unidos, la Unión Europea y el Reino Unido señalaban a China por la ola global de ataques. ¿Se puede frenar esta deriva hacia una *ciberguerra fría?*

● **Textos de Luis Pablo Beauregard y Marta Peirano**



Ciberataques que sacuden el orden geopolítico

El presidente de EE UU está creando un bloque de aliados para frenar la última ola de ataques cibernéticos. ¿Son estos, como dijo el exsenador McCain, "un acto de guerra"?

POR **LUIS PABLO BEAUREGARD**

Mientras Estados Unidos festejaba su independencia el fin de semana del 4 de julio, un grupo de *hackers* rusos llevó a cabo uno de los más grandes y coordinados ciberataques de los últimos años. Los piratas, agrupados bajo las siglas REvil (Ransomware Evil), aprovecharon una falla en un programa de tecnología de la información utilizado por unas 40.000 compañías en todo el mundo. Esa fue la puerta de entrada para hacerse con el control de los sistemas de 1.500 comercios e instituciones tan diversos como 11 colegios en Nueva Zelanda o una cadena de supermercados en Suecia. Los criminales exigían 70 millones de dólares para enviar el desencriptador que permitía recuperar la información. Esta ha sido una de las últimas muestras de la democratización de los operativos de extorsión cibernética, una reiterada arma en el juego geopolítico.

El 30% de los ciberataques que se cometen en EE UU son de *ransomware*, que consiste en un secuestro exprés de datos por los que se pide un rescate. Estos ataques se han duplicado entre 2019 y 2020, un periodo que coincide con la campaña y salida de Donald Trump, quien llegó a la presidencia auxiliado por operaciones de desinformación promovidas por piratas rusos. Barack Obama fue el primero que lidió con el problema después de que *hackers* penetraran en los sistemas del Departamento de Estado, de la Casa Blanca y en el correo electrónico de su jefe de Gabinete. Su Gobierno preparó un plan de respuesta que incluía agentes sobre el terreno en varios países, pero no actuaron a fondo ante el temor de que los rusos contraatacaran afectando a la red eléctrica, detalla el capitán de la Armada Scott Jasper en *Russian Cyber Operations: Coding the Boundaries of Conflict*. Se apostó por un paquete de sanciones que, con los años y el desinterés de la Administración de Trump, resultarían insuficientes.

La oficina de inteligencia de Seguridad Nacional del Gobierno chino, en Hong Kong, tras su inauguración, el 8 de julio de 2020. ANTHONY WALLACE (AFP)

> **China ha dado muestras de jugar con el mismo manual que Moscú, que no ha destacado por el control de sus 'hackers'**

El Gobierno de Joe Biden siente los aires de la ciberguerra. Los grupos criminales han puesto a prueba su capacidad de reacción con una serie de ataques desde el extranjero y por grupos rebeldes que en ocasiones cuentan con el respaldo de los servicios de inteligencia de potencias rivales. Los ataques ya no solo se ponen como objetivo a las grandes empresas, sino que han afectado masivamente a comercios de barrio. De los 65.000 ataques contabilizados el año pasado por la agencia de ciberseguridad Recorded Future, el 75% afectó a negocios pequeños. El Departamento de Justicia afirma que en 2020 los criminales se embolsaron 350 millones de dólares en rescates, un aumento del 300% comparado con 2019. ¿Cómo debe responder EE UU a este desafío que supera los límites de las leyes internacionales?

Cada hora, siete personas se dan cuenta de que su ordenador ha sido tomado. Un correo electrónico o un bloque de texto entre el código detalla las instrucciones para recuperar los datos. Un cronómetro en pantalla marca el tiempo para conseguir el dinero, que usualmente es pactado entre

el 10% y el 40% del valor del producto raptado, que es pagado en la gran mayoría de los casos en bitcoins para hacer su rastreo más difícil. "Esto no ha sido tan grave como puede llegar a ser", señala Trey Herr, analista del Atlantic Council. "Una cosa es que un oleoducto cierre unos días y otra que grupos como Boko Haram o el denominado Estado Islámico puedan armarse a sí mismos con fondos conseguidos mediante *ransomware*. Y los cárteles de la droga", añade.

Los atacantes han afinado sus objetivos. Disminuyen las ofensivas contra instituciones sanitarias o educativas y se concentran en industrias más rentables que afectan más a los gobiernos, según un informe de 2021 sobre filtración de datos de Verizon. En un año ha habido un aumento del 159% de casos de *ransomware* en comercio al por mayor y menudeo; en la industria del transporte, de más del 300%.

Dos grandes campañas han sacudido a los estadounidenses en 2021. En mayo, la empacadora de carne más grande del mundo, JBS, pagó 301 bitcoins (11 millones de dólares) para evitar la filtración de información sensible. El FBI responsabilizó del ataque a REvil. Antes había sido víctima Colonial Pipeline, un gasoducto que distribuye diésel y la gasolina al este del país. La compañía pagó 4,4 millones de dólares. Fueron recuperados 2,3 millones gracias al Departamento de Justicia. Biden publicó después de esto un decreto de ciberseguridad que exige estándares más altos para los programas de *software* comercial, como los que vende Microsoft, cuyo servicio de correo electrónico fue atacado en marzo, y para el utilizado por el Gobierno federal, que ha sido clasificado como crítico. La ciberseguridad fue uno de los puntos que, a mediados de junio, trataron el presidente estadounidense y el ruso en la cumbre que mantuvieron en Ginebra en un intento de descongelar sus relaciones. EE UU está viendo con intensidad la llegada a su territorio de una actividad que lleva 15 años dejando cuantiosos daños en Europa. Rusia ha perfeccionado estos ataques como herramienta de influencia.

El ejemplo más conocido es el de Ucrania en 2017. Un ataque con el virus NotPetya, una modificación del código más popular del *ransomware*, dejó en negro durante siete minutos 12.500 computadoras, afectando tanto a cajeros automáticos como a las terminales que miden la radioactividad en Chernóbil. También afectó a la red eléctrica. Maersk, la mayor empresa de contenedores del mundo, perdió 300 millones. La farmacéutica Merck, 870 millones. Ucrania culpó a Moscú, un señalamiento validado por la CIA, que pudo rastrear el origen en la inteligencia militar rusa. Reconocieron la herramienta, que fue robada a la Agencia Nacional de Seguridad y filtrada en internet meses antes del ataque, dejando a EE UU sin su poderoso código de defensa ante ciberataques.

Es solo cuestión de tiempo que pase algo mucho más grave", afirma Nina Jankowicz, analista del Wilson Center y autora de *How to Lose the Information War: Rusia, Fake News and the Future of Conflict* (Cómo perder la guerra de la información: Rusia, noticias falsas y el futuro del conflicto). La especialista señala que el actual clima de ofensiva presenta una ventaja para Moscú. "Entra en la estrategia de guerra asimétrica de Putin, que puede tener al teléfono a Biden o negociaciones de alto nivel en Suiza con representantes estadounidenses. Si los ataques no estuvieran sucediendo, quizá no tendría este nivel de atención", apunta.

La llegada de Biden a la Casa Blanca ha facilitado un retorno a los bloques geopolíticos tradicionales. La cumbre de Ginebra mostró que el estadounidense es capaz de estrechar la mano a sus adversarios y dibujar una raya roja ante el Kremlin. "Biden considera a Rusia una distracción. La gran amenaza para la influencia estadounidense en el escenario mundial es China. No quiere ser distraído por los rusos si cree que puede encontrar un tipo de arreglo que pueda traer un poco de paz a Europa, asegurar la soberanía de Ucrania y que deje de entrometerse en nuestras elecciones y en las de nuestros aliados europeos. Esa fue su oferta", añade Jancowicz, que cree que la pelota está en tejado ruso. El 13 de julio, un mes después del encuentro en Suiza, REvil se desintegró. No se sabe si fue obra de los servicios de inteligencia rusos o estadounidenses. O si los criminales repartieron el botín y se esfumaron. El misterio crece.

China ha dado muestras de jugar con el mismo manual que Moscú, que no ha destacado por el control de sus *hackers*, muchos relacionados con su servicio de inteligencia. Esta semana, EE UU responsabilizó por primera vez a Pekín de estar tras un ataque cibernético, el de marzo contra Microsoft. El mensaje tuvo un altavoz importante: se hizo junto a la OTAN y la UE, que habían mostrado antes reticencias a señalar a China, importante socio comercial. "Se está cimentando una coalición que puede dar una respuesta política a este conflicto. Se ha atribuido a un actor en particular, pero la gran pregunta es cuál será la respuesta", se cuestiona Safa Shahwan, subdirectora de la iniciativa de ciberasuntos de Estado del Atlantic Council. La acusación de la Administración estadounidense no estuvo acompañada de ninguna represalia para China, pero la creación de un bloque de aliados puede ser un paso previo a la imposición de castigos. "Las sanciones solo funcionan cuando se aplican con una coalición", añade Shahwan. La política de *name and shame* (nombrar y avergonzar) será insuficiente en un creciente ambiente de ciberhostilidad. La respuesta que debe dar EE UU es materia de profundos debates. Analistas como Jancowicz creen que es hora de que Washington revise el sistema de sanciones y afine los objetivos, entre ellos los altos funcionarios del Kremlin, así como sus familias e hijos, pues suelen estudiar en el extranjero o tener casas en Miami o Londres. Otras voces han pedido lo mismo para miembros de la cúpula del Partido Comunista Chino.

En 2017, el senador John McCain dijo a la televisión ucrania que el ciberataque ruso a los servidores demócratas debía ser considerado "un acto de guerra". Un año después, la Administración de Trump amplió por primera vez la posibilidad del uso de armas nucleares como respuesta a "importantes ataques estratégicos no nucleares" que afectaran a población o a infraestructuras nacionales o de sus aliados. El Gobierno de Biden está revisando la política nuclear. De momento, parece bastarle una solución diplomática con ayuda de aliados. Una salida improbable en la era de Trump.

El negocio de la extorsión en un mundo sin cortafuegos

La inteligencia estadounidense y el Ejército israelí desarrollaron Stuxnet, un programa muy utilizado por los ciberpiratas

POR **MARTA PEIRANO**

Stuxnet fue diseñado y ejecutado por la inteligencia estadounidense y el Ejército israelí en 2010 para sabotear de forma remota una planta de enriquecimiento de uranio a 180 kilómetros al sur de Teherán. Fue el primer ciberataque contra una infraestructura crítica, y tuvo éxito porque la planta usaba el estándar en sistemas de automatización industrial: Microsoft Windows y CLP de Siemens. Los atacantes pudieron encontrar vulnerabilidades, testarlas sin riesgo en su laboratorio y perfeccionar su estrategia antes de atacar. Una vez suelto, Stuxnet pudo propagarse y prosperar atacando cientos de sistemas idénticos en Irán y el resto del mundo. Todos los monocultivos degradan el sistema y comprometen su inmunidad, pero la falta de diversidad en el mercado del *software* es solo una de las muchas condiciones que han convertido el negocio de los rescates *online* en un lucrativo sector de baja inversión, poco riesgo y explosiva rentabilidad.

El imperio global de soluciones como Microsoft Exchange, Kaseya o SolarWinds ofrece un terreno uniforme para la propagación de los virus, que son "liberados" en busca de puntos débiles y siempre los encuentran. Son el sistema linfático de la Red, un universo de trabajadores estresados, administradores remotos, ejecutivos irresponsables y *drivers* sin actualizar. Otro foco de infección es la galaxia de miles de millones de objetos presuntamente inteligentes diseñados por empresas sin presupuesto de seguridad. Después hay otros incentivos, que favorecen el crecimiento del crimen organizado.

Para empezar, se denuncia poco. A las multinacionales y grandes infraestructuras privadas les sale más rentable pagar un rescate que reconstruir el sistema y ocultan los ataques para proteger su reputación. La nobleza feudal del capitalismo prefiere quemar dinero que admitir debilidad. Segundo, la estructura descentralizada de las criptodivisas permite que se puedan mover grandes sumas de dinero sin burocracia ni alarmas, sin el riesgo de una intervención policial.

Tercero, no es fácil atribuir los delitos, porque se trata de un mercado altamente colaborativo de servicios para la extorsión *online* (Ransomware as a Service o RaaS). Los grupos como REvil o DarkSide no sólo venden su código para atacar y encriptar sistemas, sino también una infraestructura de comunicaciones segura para negociar el rescate y acceso a foros y medios de noticias para volcar los datos cuando la víctima no paga. Hay quien cobra por devolver el acceso al sistema y quien cobra por no compartir los datos con otros o volcarlos en la Red. Cuando hacen las dos cosas, se llama una doble extorsión.

Otro motivo es que los principales cárteles operan en países cuyo gobierno hace la vista gorda, a condición de que no ataquen dentro de sus fronteras y estén disponibles para operaciones patrióticas. "Los *hackers* son espíritus libres, como artistas que se levantan una mañana de buenas y se ponen a pintar", explicaba Vladímir Putin en una rueda de prensa con medios internacionales en 2017. "Hay días que se levantan, leen las noticias y, si se sienten patrióticos, tratan de hacer la contribución que consideran justa contra los que maldicen a Rusia". Por eso es tan difícil distinguir los ciberataques militares o estatales de los genuinamente pecuniarios, o atribuir el ataque a un grupo criminal que alquila sus servicios a cambio de un porcentaje del botín.

> **La falta de diversidad en el mercado del *software* ha convertido el negocio de los rescates *online* en un lucrativo sector**

Biden y Putin, en Ginebra, el pasado 16 de junio. PETER KLAUNZER (EFE)

Finalmente, es habitual que un grupo utilice herramientas robadas a otro grupo, especialmente si trabaja para la inteligencia estadounidense, como el FBI o la NSA, y que luego las vuelque en la Red para borrar sus huellas. Sea como sea, sin atribución no hay denuncia y sin denuncia no hay orden de registro ni investigación.

Kaspersky advirtió que Stuxnet sería el comienzo de una nueva carrera armamentística mundial y tenía razón. Pero no hace falta que un ataque sea tan sofisticado para conseguir su objetivo. Según un estudio de HP, solo el 20% de los ataques de la última década han utilizado herramientas a medida diseñadas por equipos de élite, tanto de criminales como de servicios de inteligencia. La mayor parte son ataques realizados por *hackers* inexpertos con programas de *software* que se pueden comprar en la Red. En otras palabras, el enemigo casi nunca es excepcional, pero nosotros somos excepcionalmente débiles. Necesitamos desarrollar inmunidad de grupo, y ese proyecto solo puede ser deliberado, colectivo y sistémico.

Marta Peirano es periodista. Es autora de 'El enemigo conoce el sistema: Manipulación de ideas, personas e influencias después de la Economía de la atención" (Ed. Debate).