SPECIAL REPORT

N.º 506 | FEBRERO DE 2022 UNITED STATES INSTITUTE OF PEACE www.usip.org

La acción no violenta en la era del autoritarismo digital: Dificultades e innovaciones

Por Matthew Cebul y Jonathan Pinckney

Refugiados musulmanes rohinyás miran un teléfono en Bangladés en enero de 2018. Las expresiones de odio sin restricciones en Facebook impulsaron la limpieza étnica en Birmania. (Fotografía de Manish Swarup/AP)

Contenidos

Resumen

- Si bien las tecnologías emergentes y el activismo en línea inicialmente empoderaron las campañas no violentas, hoy los activistas se ven desafiados por los regímenes autoritarios armados con tecnologías de represión digital optimizadas.
- Las entrevistas que se realizaron en nueve países revelan cómo los activistas se están adaptando a la nueva realidad del sofisticado autoritarismo digital. Los activistas han realizado importantes innovaciones técnicas y organizativas, desde la sistematización del cifrado de extremo a extremo y las redes privadas virtuales hasta la adopción de estructuras de movimiento descentralizadas.
- Sin embargo, sigue habiendo grandes obstáculos. Los activistas luchan para encontrar una relación de equilibrio entre la seguridad digital y la comodidad, la dificultad en la coordinación en el ámbito del movimiento y la creciente complejidad técnica del panorama digital.
- Además, los activistas no violentos se enfrentan a poderosas empresas tecnológicas internacionales que ayudan, ya sea mediante la indiferencia o incompetencia, a los autócratas digitales en sus esfuerzos represivos.
- Los partidarios internacionales deben acelerar el ritmo de las adaptaciones digitales de los activistas y obstruir la innovación autocrática. Entre los temas prioritarios, se encuentran rectificar las desigualdades geográficas en el acceso a la capacitación, crear redes transnacionales de activistas y endurecer la regulación para evitar una mayor difusión de las tecnologías de represión digital.

United States Institute of Peace
Making Peace Possible

SPECIAL REPORT

N.º 506 | FEBRERO DE 2022

ACERCA DEL INFORME

Este informe analiza cómo los activistas involucrados en la acción no violenta se están adaptando al uso de tecnologías emergentes por parte de los regímenes autoritarios. Basado en entrevistas con veinticinco activistas destacados de nueve países, este informe se financió mediante un acuerdo interinstitucional entre el Instituto de Paz de los Estados Unidos (USIP, en inglés) y el Centro para la democracia, los derechos humanos y la gobernanza de la Agencia de los Estados Unidos para el Desarrollo Internacional (USAID, en inglés).

ACERCA DE LOS AUTORES

Matthew Cebul es investigador del Programa sobre Acción no violenta del USIP, donde realiza investigaciones multimétodo sobre la acción no violenta y sus implicancias. Jonathan Pinckney es investigador sénior del Programa sobre Acción no violenta del USIP y autor de *From Dissent to Democracy: The Promise and Peril of Civil Resistance Transitions* (Del disenso a la democracia: la promesa y el peligro de las transiciones de resistencia civil), publicado por Oxford University Press en 2020.

United States Institute of Peace
2301 Constitution Avenue NW
Washington, DC 20037

Teléfono: (202) 457-1700
Fax: (202) 429-6063
Correo electrónico: usip_requests@usip.org
Sitio web: www.USIP.org

Special Report n.º 506. Publicado por primera vez en 2022.

ISBN: 978-1-60127-887-6

UNITED STATES
INSTITUTE OF PEACE PRESS

Partidarios de la oposición bielorrusa encienden las luces de sus teléfonos inteligentes durante un mitín en la Plaza de la Independencia en Minsk, Bielorrusia, el 20 de agosto de 2020. (Fotografía de Dmitri Lovetsky/AP)

Introducción

Las tecnologías emergentes han transformado la acción no violenta del siglo XXI. Luego de asombrosos avances en la comunicación digital y la expansión global del acceso a Internet, los activistas han adoptado tecnologías emergentes para preparar, organizar y expandir sus demandas. Estas tecnologías han permitido a los activistas coordinar rápidamente movimientos descentralizados y sin líderes vinculados tanto a las periferias nacionales como a públicos internacionales, exponer de manera drástica los abusos contra los derechos humanos antes ocultos en una negación admisible y alimentar vibrantes discursos cívicos en ecosistemas en línea liberados de los guardianes de medios tradicionales.[1] Es difícil identificar una campaña no violenta actual que no tenga una presencia considerable en línea. Desde Hong Kong hasta Sudán del Sur, Venezuela y otros lugares, el espacio virtual es un ámbito determinante para la acción no violenta.

Estas ventajas del activismo en línea fueron especialmente pronunciadas durante período de la Primavera Árabe, donde jóvenes pioneros rápidamente dominaron el campo digital, lo que dejó a los autócratas ingeniándoselas para contener arrebatos inesperados de disidencia.[2] Algunos persisten. Sin embargo, estos días de euforia incipiente días dieron paso a la represión digital, la restricción de libertades en línea y el retroceso democrático. Como se documentó en un informe anterior del Instituto de Paz de los Estados Unidos y en cada vez más publicaciones sobre autoritarismo digital, la mayoría de los activistas ahora enfrentan regímenes inteligentes desde el punto de vista tecnológico armados con censura digital, vigilancia y técnicas de desinformación.[3] Estas autocracias digitales más sofisticadas amordazan a los críticos en línea, se infiltran en foros de oposición, controlan a activistas tanto en línea como fuera de línea, y crean arquitecturas legales y pseudolegales para forzar a las empresas tecnológicas a facilitar la represión.

Los problemas de comodidad, la coordinación en el ámbito de los movimientos y la incertidumbre sobre el siempre cambiante panorama de seguridad digital dejan a los activistas vulnerables a la represión digital. Estos problemas se exacerban por una desigualdad significativa en el acceso a la capacitación en seguridad digital.

Las autocracias del mundo se están adaptando rápidamente a la era digital, como lo demuestra el ritmo continuo de detenciones por activismo en línea y la disminución de los derechos digitales en todo el mundo.[4]

¿Cómo enfrentan este problema los activistas no violentos y qué pueden hacer para salir fortalecidos por otro lado? A partir de entrevistas con veinticinco activistas de nueve países, este informe documenta cómo los activistas se están adaptando a las nuevas formas de represión digital.[5] Estos activistas se están movilizando en torno a una amplia variedad de temas y con diferentes niveles de experiencia (algunos son jóvenes activistas por los derechos digitales, mientras que otros son experimentados defensores de las luchas por la democratización y hay incluso constructores de paz a nivel local).[6] Sus relatos esclarecen los desafíos a los que se enfrentan los activistas en un rango de autocracias digitales, desde regímenes de alta capacidad, como Rusia y China, hasta países como Sudán del Sur o Bangladés, donde el Gobierno adoptó recientemente algunos de los elementos clave de la represión digital.

Las entrevistas destacaron las siguientes tres tendencias clave:

- Los activistas descubrieron muchas adaptaciones creativas a la nueva realidad del autoritarismo digital. Las medidas de seguridad digital son más comunes y mejor comprendidas entre los activistas en la actualidad que incluso hace algunos años. Más activistas han adoptado tecnologías, estructuras organizativas y prácticas comunitarias para comunicarse de manera más segura, mantenerse resilientes frente a la represión digital y seguir impulsando el cambio. Algunos incluso utilizan tecnologías emergentes avanzadas para promover su activismo de maneras innovadoras.

- Sin embargo, enfrentan dificultades persistentes para adaptarse al autoritarismo digital y luchan por seguir el ritmo de los sofisticados regímenes de seguridad. Los problemas de comodidad, la coordinación en el ámbito de los movimientos y la incertidumbre sobre el siempre cambiante panorama de seguridad digital dejan a los activistas vulnerables a la represión digital. Estos problemas se ven agravados por una gran desigualdad en el acceso a la formación sobre seguridad digital: los activistas de los países de alta prioridad y las zonas urbanas disfrutan de un acceso fácil, mientras que, análogamente, aquellos en riesgo en entornos más marginales no son tenidos en cuenta.

- Los activistas están luchando en múltiples frentes, no solo contra regímenes represivos, sino también contra empresas tecnológicas que a menudo son indiferentes o incluso hostiles ante sus necesidades. Las redes sociales son un activo indispensable para los activistas; sin embargo, los requisitos de identidad y la moderación no transparente del contenido algorítmico reprimen el activismo en estas plataformas. Del mismo modo, las empresas tecnológicas se benefician de la venta de tecnología de vigilancia contra el terrorismo, pero eluden con cinismo la responsabilidad cuando los autócratas utilizan estas herramientas para silenciar a los disidentes.

Para enfrentar estos desafíos, los activistas y sus partidarios internacionales necesitan acelerar el ritmo de la innovación activista y obstruir la proliferación de tecnologías de represión digital. Esto ayudará a alejar el equilibrio tecnológico de los autócratas y acercarlo a las campañas de acción no violenta que los desafían; de esta manera, se promoverá la paz, la democracia y la justicia social que esos movimientos pretenden lograr.

Los activistas se adaptan a la represión digital

Los recursos del autoritarismo digital, donde los regímenes autoritarios utilizan tecnologías emergentes para involucrarse en censura, vigilancia y desinformación, inicialmente tomaron por sorpresa a muchos activistas. Llenos de optimismo sobre las formas en las que la tecnología digital los empoderaba para llegar a millones de personas con un clic, la mayoría calificó sus evaluaciones iniciales de estas tecnologías como estrictamente positivas. Como dijo un activista ruso: "Sin Internet, no tendríamos una sociedad civil".

Este aprecio por el activismo digital surgió en gran parte de la falta de experiencia técnica de los regímenes represivos. Muchos se acercaron a Internet no solo con indiferencia, sino también con desdén activo, una actitud que demostró con gracia la incompetencia de parte de su personal de base. Por ejemplo, un activista de Irán contó una historia sobre un amigo que hace una década había sido interrogado durante horas por la policía sobre la identidad de un misterioso conspirador llamado Sarvar sobre el que, supuestamente, había estado hablando con un amigo. Después de mucha confusión, la policía generó los correos electrónicos aparentemente incriminatorios, y el activista arrestado se dio cuenta de que los interrogadores habían confundido el término *server* (servidor) con un nombre persa femenino.

Sin embargo, según documentan una gran cantidad de fuentes, la mayoría de los autócratas aprendieron rápido de sus primeros errores, a menudo después de revueltas masivas impulsadas por las redes sociales.[7] La Revolución verde de 2009 en Irán, las revueltas de la Primavera Árabe en 2010 y 2011, y las protestas en Rusia después de las elecciones legislativas de 2011 fueron llamados de atención especialmente importantes. China, que desarrolló un alto grado de capacidad técnica y control desde el principio, fue la pionera innovadora que otros autócratas de alta capacidad intentaron imitar. Estados como Rusia e Irán han aprovechado las nuevas tecnologías para promulgar regímenes integrales de censura, vigilancia y desinformación. Arrestos de gran repercusión mediática demostraron la necesidad de adaptación de casi todos los activistas de estos países.

En países con infraestructuras de represión digital menos desarrolladas, la necesidad de adaptación ha sido menos evidente. Muchos activistas, despreocupados por la rudimentaria capacidad técnica de sus Gobiernos, siguieron descuidando incluso los fundamentos de la higiene digital en línea, y ni hablar de los protocolos de seguridad digital integral. Sin embargo, incluso en estos países, cambios recientes les han dado motivos para repensar sus prácticas. Un activista ambiental de Bangladés informó que algunos de sus colegas habían pensado seriamente en la seguridad en línea. La aprobación de la Ley de Seguridad Digital del país en septiembre de 2018 y varios casos en los que los regímenes controlaron y publicaron contenido privado bochornoso de destacados activistas han llevado a estos colegas a cambiar radicalmente la forma en que interactúan con la Internet. De manera similar, activistas de Sudán del Sur informaron que hace poco cambiaron a plataformas digitales más seguras después de casos de piratería de teléfonos inteligentes y cuentas de redes sociales.

Importantes revelaciones de las tecnologías avanzadas de vigilancia también dieron forma a la conversación sobre adaptación. En particular, muchos activistas expresaron su preocupación por el proyecto Pegasus, que expuso la venta del software distintivo de la empresa israelí NSO Group a muchos Gobiernos autoritarios, que lo usaron para vigilar a activistas y políticos de la oposición.[8] Mientras que la mayoría de los ataques de *phishing* requieren que el objetivo haga clic en un vínculo o abra un correo electrónico, Pegasus infecta dispositivos electrónicos privados sin ninguna acción del usuario. Muchos activistas mencionaron a Pegasus, y si bien la mayoría dijo que confiaba en que su Gobierno no tenía los recursos para desplegar a escala

este tipo de vulnerabilidades de seguridad, lo señalaron como un ejemplo de las herramientas de represión digital cada vez más malignas que los autócratas tienen a su disposición.

Además, algunos activistas se resistieron a la idea de responder a la represión digital implementando mejores prácticas de seguridad, y algunos rechazaron la idea de contrarrestar la vigilancia gubernamental. Un instructor de seguridad digital señaló una cultura de martirio o la sensación de que evadir la vigilancia era admitir tácitamente que se estaba haciendo algo mal, e hizo hincapié en la necesidad de cambiar la conversación entre los activistas de una centrada en no haber hecho nada malo a otra centrada en cómo la seguridad digital preserva la resiliencia de los activistas a largo plazo. Sin embargo, incluso quienes rechazaron la necesidad de hacer esto indicaron una lenta adopción de herramientas específicas para impedir la represión digital.

El resultado de estos procesos ha sido un gran repunte del interés en la seguridad digital y un conjunto de adaptaciones innovadoras en evolución ante el autoritarismo digital. El alcance de sus cambios de conducta varió de manera significativa, pero todos los activistas reconocieron la importancia de adaptarse a las nuevas herramientas de represión digital e identificaron formas de hacerlo. Una persona entrevistada dijo lo siguiente:

> Supongamos que había un taller para activistas y se organizaban dos sesiones de grupos pequeños, una sobre recaudación de fondos y otra sobre seguridad digital. En ese momento, todos querían participar en la sesión de recaudación de fondos y nadie en la de seguridad digital. Pero ahora, como se trata cada vez más de una cuestión de vida o muerte, las personas realmente están aprendiendo sobre herramientas digitales. Hoy, ese taller podría tener el 70 % de las personas en la sesión de recaudación de fondos y el 30 % en la sesión de seguridad digital.

ADAPTACIONES TÉCNICAS

El primer conjunto de adaptaciones implica cambios técnicos en las herramientas, las plataformas y los dispositivos que los activistas usan para presentar y coordinar sus acciones. Gran parte de este proceso pretende abordar el desafío de la legibilidad, es decir, comunicaciones a las que "el Estado pueda acceder y que pueda interpretar con facilidad".[9] La tecnología emergente facilita la legibilidad del mundo social y político por parte de los regímenes autoritarios, lo que les permite observarlo integralmente con soltura. Por lo tanto, los activistas han intentado cambiar sus prácticas técnicas por vías ilegibles para los posibles observadores del Gobierno.

Un paso clave es pasar de las redes sociales y las plataformas de comunicaciones que pueden censurarse o vigilarse fácilmente a aquellas que se mantienen confidenciales mediante un cifrado sólido. Las formas de comunicación en línea que utilizan cifrado de extremo a extremo (E2EE) son prácticas estándar para la mayoría de los activistas en entornos más complejos, pero siguen siendo relativamente raras en entornos con una represión gubernamental menos extrema. Activistas informaron que la mayoría de las herramientas de E2EE más importantes, como la plataforma de mensajería Signal o el servicio de correo electrónico ProtonMail, son comunes entre los círculos activistas en sus países. Muchos informan que cambian entre estas plataformas para las comunicaciones internas confidenciales y otras más populares como WhatsApp o Facebook Messenger para comunicaciones externas menos confidenciales.

Otra adaptación importante ha sido el uso más uniforme de redes privadas virtuales (VPN). Cuando un usuario se conecta a Internet a través de una VPN, sus datos pasan de la computadora a un servidor externo a través de una conexión cifrada. Luego el servidor externo se conecta al sitio web o servicio al que el usuario desea acceder y vuelve a enviar los datos al usuario a través de esa misma conexión cifrada. De este modo, se evita que partes externas vigilen o censuren el tráfico web de un usuario. Como los servidores VPN suelen estar ubicados en otros países, también pueden ayudar a los usuarios a acceder a sitios web internacionales que su Gobierno censura a nivel nacional.

Manifestantes miran su teléfono inteligente en Hong Kong el 12 de junio de 2019. El espacio virtual es un ámbito determinante para la acción no violenta, y los foros en línea anónimos abiertos como LIHKG han servido como plataformas organizadoras cruciales. (Fotografía de Kin Cheung/AP)

Por ejemplo, todos los activistas rusos entrevistados para este informe consideran el uso de una VPN una práctica estándar básica y lo hacen cada vez que se conectan a Internet. Un activista iraní informó que "dentro de Irán, el 99 % de los activistas usan una VPN".

Una tercera adaptación técnica común es el cambio de las prácticas de almacenamiento de datos. Los activistas dijeron que la vulnerabilidad más grave era que las fuerzas de seguridad los detengan a ellos o a uno de sus colegas activistas y adquieran posesión de su teléfono o computadora. Por lo general, con el dispositivo físico en su poder, las fuerzas de seguridad pueden obligar a los activistas a desbloquearlo y luego acceder a registros de comunicaciones confidenciales y documentos organizativos. Los activistas informaron varias maneras técnicas de abordar esta situación. Un activista en Rusia informó que borraba todos los mensajes y datos que había en su dispositivo cada tres días. Este es un enfoque extremo, pero muchos activistas informaron que utilizan adaptaciones similares, como activar la configuración en aplicaciones de mensajería que elimina los mensajes de manera automática, almacenar datos únicamente en servidores cifrados en la nube en lugar de en dispositivos físicos y borrar toda la información de su dispositivo si sienten peligro inminente de ser arrestados. También es importante el software que permite la eliminación remota o códigos para eliminar rápidamente los datos desde la pantalla de bloqueo.

ADAPTACIONES NO TÉCNICAS

Tal vez incluso más importantes que las adaptaciones técnicas son las adaptaciones no técnicas, es decir, modificaciones de las prácticas en el ámbito del movimiento y los patrones de acción que promueven la resiliencia ante los desafíos que plantea el autoritarismo digital.

Por ejemplo, el movimiento prodemocracia en Hong Kong, además de adoptar muchas de las adaptaciones técnicas descritas, también ha reformado radicalmente la estructura del movimiento. Mientras que la comunicación inicial pasó de un pequeño grupo de líderes bien identificados al movimiento más amplio, la necesidad de protegerse contra la represión digital ha llevado a una estructura más difusa y descentralizada. En la actualidad, la mayor parte de la actividad del movimiento tiene lugar en foros en línea anónimos abiertos, como LIHKG, similar a Reddit. Estos debates incluyen lenguaje de grupo y bromas en cantonés para distinguir a los participantes del movimiento de los saboteadores del Gobierno que intentan infiltrarse. Este cambio ha dado lugar a una estructura de movimiento radicalmente horizontal en la que las tácticas y la estrategia deben contar con la aceptación general de todos los participantes. También ha facilitado un activismo continuado (aunque reducido), incluso a pesar de la fuerte represión física y digital del Gobierno.[10]

Si bien los activistas son cada vez más conscientes de la seguridad en línea, las personas entrevistadas expresaron, con frecuencia, cautela sobre sus esfuerzos por adaptarse al autoritarismo digital.

Los activistas de Hong Kong han combinado esta estructura descentralizada y anónima de foros de discusión en línea con un aumento del activismo local en persona, mediante el desarrollo de redes en sus vecindarios que no dependen de la mediación digital y que, por lo tanto, el Gobierno tiene más dificultades para detectar.

De manera similar, varios activistas describieron un meticuloso enfoque en no tener "nada que ocultar" como una de sus principales adaptaciones no técnicas. Toman todas las medidas técnicas que pueden para frustrar la vigilancia del Gobierno y los esfuerzos de censura, pero tratan cualquier comunicación en línea, incluso en los canales más seguros, como información que podría ser controlada y utilizada en su contra.

Otra adaptación no técnica clave consiste en aumentar la presión social entre los grupos de activistas sobre la importancia de la seguridad digital. Muchos grupos, en particular los que trabajan en contra de los autócratas digitales más sofisticados, analizaron el desarrollo de protocolos de seguridad detallados, lo que fue un tema común de conversación entre ellos y sus colegas activistas. "Es lo primero en lo que pienso cuando me despierto por la mañana", dijo un activista por la democracia e instructor de seguridad digital. Un activista ruso informó que mantenían sus protocolos de seguridad digital utilizando una combinación de leve humillación social y duras consecuencias profesionales. "Cuando vemos que alguien no cumple con el protocolo de seguridad, por lo general porque deja su computadora portátil abierta cuando no la está usando, debe comprar pizza para todos lo que están en la oficina. Si sucede nuevamente, esa persona es despedida".

Desafíos actuales de la seguridad digital

Si bien los activistas son cada vez más conscientes de la seguridad en línea, las personas entrevistadas expresaron, con frecuencia, cautela sobre sus esfuerzos por adaptarse al autoritarismo digital. De sus inquietudes surgen cuatro desafíos generales y persistentes a los que se enfrentan los movimientos en la era digital.

RELACIÓN ENTRE SEGURIDAD Y COMODIDAD

El primer desafío es un problema conocido comúnmente como *relación entre seguridad y comodidad*. Las medidas de seguridad más eficaces tienden a ser más engorrosas y menos fáciles de usar, por lo que es menos probable que los voluntarios de los movimientos las adopten ampliamente.

Tal vez el ejemplo más claro de esta relación sea el uso de VPN. Como se describió antes, muchos activistas en contextos especialmente represivos utilizan las VPN de manera regular. Sin embargo, otros las rechazaron porque eran de difícil acceso, lentas y supuestamente innecesarias para las actividades en línea "no confidenciales".[11] Asimismo, muchos dicen que, aunque Signal es más seguro que Telegram y WhatsApp, siguen prefiriendo la funcionalidad de WhatsApp y todavía deben migrar completamente de los servicios antiguos. Varias personas encuestadas también indicaron que los grupos de chat anónimos son más seguros que aquellos identificables, pero los participantes se sienten más incómodos y confían menos, lo que desalienta su uso. Estas inquietudes no pueden compararse con la rigurosidad de un protocolo de seguridad integral, que puede incluir eliminación rutinaria de datos, teléfonos desechables, contraseñas complejas, unidades cifradas, separación cuidadosa de perfiles en línea de activistas y no activistas, y planes de destrucción remota de datos en caso de arresto, entre otras medidas.

Parte de la reticencia a adoptar protocolos de seguridad eficaces proviene de la dependencia de patrones establecidos a nivel grupal: los activistas necesitan interactuar con audiencias masivas y, por lo tanto, no pueden cambiar fácilmente de las plataformas consolidadas a opciones más nuevas y seguras que todavía deben desarrollar grandes bases de usuarios. Pero gran parte del problema es simplemente la comodidad. Por ejemplo, un activista ruso lamentó que algunos de sus colegas siguieran usando Mail.ru y Yandex, proveedores rusos de correo electrónico y búsqueda en Internet con vínculos claros con el Kremlin, aunque haya opciones seguras disponibles como ProtonMail. Otros hablaron sobre sus esfuerzos por convencer a amigos y colegas activistas para que adoptaran nuevas plataformas o prácticas de seguridad, a veces sin resultado. Como bromeó un instructor de seguridad digital iraní: "Los activistas solo quieren presionar un botón y que todo se resuelva". El deseo de comodidad de los usuarios sigue dificultando la adopción de mejores prácticas de seguridad.

COORDINACIÓN EN EL ÁMBITO DEL MOVIMIENTO

Estrechamente conectado con la relación entre la seguridad y la comodidad está el problema de la *coordinación en el ámbito del movimiento*: si bien la seguridad digital comienza con las personas, la seguridad de las campañas es un esfuerzo colectivo, y los activistas pueden estar tan confiados como sus colegas menos confiados.

El desafío de la legibilidad es el centro de esta inquietud. A medida que pasamos cada vez más tiempo en línea, los procesos cívicos que antes eran demasiado sutiles para advertir o demasiado complejos para analizar ahora están documentados fielmente en listas de amigos, membresías en grupos, fotografías geolocalizadas, registros de chats e historiales de búsqueda. Los regímenes represivos, especialmente aquellos armados con tecnologías avanzadas de vigilancia y procesamiento automático de datos, pueden aprovechar estos datos para identificar e ingresar en redes enteras de activistas. El teléfono desbloqueado o la cuenta pirateada de un usuario descuidado puede comprometer a muchos activistas, como bromeó un activista de Hong Kong: "Si se me cae el teléfono, todos los miembros de mi equipo saldrán perjudicados". Las personas entrevistadas relataron episodios desgarradores en los que regímenes detenían a activistas, los obligaban a desbloquear sus dispositivos y, luego, usaban la información para fundamentar casos y rastrear a más activistas. Un activista describió el acceso ilegal al grupo de Facebook que coadministraba, que otorgó temporalmente el control del grupo a la policía, a pesar de que los otros administradores estaban protegidos. Estas anécdotas ayudan a explicar la frustración de algunas personas encuestadas por la falta de protección de los datos de los demás. Como dijo el mismo activista de Hong Kong, los colegas descuidados están "destruyendo a todo el equipo".

Lamentablemente, este problema de coordinación no tiene soluciones rápidas. La adopción generalizada de las mejores prácticas de seguridad mejoraría la seguridad de los movimientos colectivos, pero en muchos países las normas de higiene digital siguen siendo deficientes y cambian a paso lento. Dentro de los movimientos, los activistas pueden dividir sus contactos para limitar el daño ante cualquier infracción, falsificando redes locales desconectadas dentro de las ciudades o los vecindarios. De hecho, los movimientos masivos descentralizados se prestan naturalmente para esta estructura, aunque la división impone problemas inherentes de coordinación, y las personas entrevistadas no lo mencionaron a menudo. Hace poco, muchos activistas aceptaron autoeliminar mensajes en Signal, Instagram y otras plataformas para evitar dejar un registro en los dispositivos de los demás. Estas medidas son útiles, pero básicamente solo pueden mitigar de manera parcial los riesgos del activismo en línea interconectado.

Personas sosteniendo carteles que dicen "¡Libertad para Navalni!" y con las luces de sus teléfonos inteligentes encendidas durante un mitín en apoyo al líder opositor encarcelado Alexéi Navalni en Moscú el 21 de abril de 2021. (Fotografía de Alexander Zemlianichenko/AP)

COMPLEJIDAD E INCERTIDUMBRE

Un tercer desafío es la naturaleza intrínsecamente compleja y cambiante de la tecnología digital, que genera incertidumbre tanto entre los activistas como entre el público, lo que provoca que a los activistas les cueste comprender e implementar las mejores prácticas.

La tecnología digital se desarrolla con rapidez, con frecuencia tras puertas cerradas en las corporaciones, y el panorama legal sigue siendo turbio. Las aplicaciones y los programas que son seguros un día están comprometidos o bloqueados al día siguiente, los regímenes adquieren nuevas funciones de vigilancia y censura, las aplicaciones cambian sus configuraciones de privacidad o condiciones de servicio, y las empresas están más dispuestas a cooperar con las nuevas leyes locales de ciberseguridad. Varios activistas rusos dijeron que el aspecto legal es complejo en particular, porque el Kremlin está reformando las leyes que rigen el discurso en línea, lo que genera incertidumbre entre los activistas sobre cómo se aplicarán en la práctica. Los aspectos básicos de la seguridad digital pueden encontrarse en muchas guías en línea, como las que ofrecen Electronic Frontier Foundation (EFF), The Citizen Lab, Paradigm Initiative y la aplicación Umbrella de Security First.[12] Sin embargo, estas guías no están traducidas a idiomas y contextos locales, y es posible que los activistas de los países donde más se necesitan no puedan acceder a ellas o ni siquiera las conozcan. Además, la complejidad técnica de los procedimientos de privacidad digital y el gran volumen de material pueden convertirse en una curva de aprendizaje pronunciada para quienes no tienen experiencia en informática.

Al no tener fuentes acreditadas sobre estos temas, es posible que sea difícil mantenerse al día. La incertidumbre y el desacuerdo entre los activistas sobre las mejores prácticas de seguridad es algo común. Por ejemplo, algunas personas encuestadas expresaron inquietudes por la falta de seguridad de WhatsApp y las prácticas de compartir de datos, aun cuando otras sostuvieron que la plataforma está cifrada y es segura.[13] Un activista iraní por los derechos digitales explicó que la confusión sobre incluso una jerga informática básica dificultaba poder ayudar a los activistas iraníes que intentaban conectarse a un servidor seguro.

Un aspecto clave de esta incertidumbre es que los activistas generalmente descubren que sus medidas de seguridad son vulnerables solo después de haber fallado. En este sentido, suelen ser, por desgracia, reactivos, no proactivos. Por ejemplo, las personas encuestadas empezaron a desconfiar de los grupos de Facebook o a abandonar grupos infiltrados de Telegram o WhatsApp solo después de que los administradores de esos grupos (en algunos casos sus propias cuentas) habían sido pirateados. Del mismo modo, dado que los activistas por lo general no pueden detectar la vigilancia encubierta del régimen ni los intentos de piratería en tiempo real, nunca pueden sentirse del todo seguros de haber hecho lo suficiente para protegerse. La carga cognitiva de la incertidumbre agobia incluso a aquellos que siguen todas las precauciones recomendadas.

Una respuesta común a esta falta de conocimiento son los programas de educación y capacitación. Algunas personas encuestadas habían participado en capacitaciones sobre seguridad digital y dominaban los aspectos básicos. Sin embargo, estas capacitaciones tienen un alcance limitado; las personas encuestadas sin capacitación expresaron su inquietud por la ignorancia relativa sobre el tema, y casi todos querían más asesoramiento. Además, la capacitación sobre seguridad digital tendió a reforzar las desigualdades en el acceso a la comunidad internacional. Grupos reconocidos en países de alta prioridad, como Rusia, pueden acceder a capacitaciones básicamente cuando quieran, pero los de países como Sudán del Sur pocas veces tuvieron acceso a asesoramiento sobre seguridad digital. Estos problemas de acceso son exacerbados por el agravamiento de la represión, en el sentido de que los grupos locales de derechos digitales restringen su alcance a los activistas que conocen y pueden autorizar la protección de los instructores del país de la vigilancia del régimen.

AUMENTO DE LA CAPACIDAD DEL GOBIERNO

Por último, los desafíos descritos se magnifican ante la capacidad cada vez mayor de los regímenes en términos de represión digital. A pesar de la variación significativa en la competencia técnica entre los países, la mayoría de los regímenes compensan el tiempo perdido, lo que aumenta la presión sobre una generación de activistas nativos digitales que alguna vez estuvieron acostumbrados a tener el control del espacio virtual.[14] En la actualidad, los activistas de Irán (en contraste con los de hace una década, cuando el régimen no estaba familiarizado con la tecnología digital) le temen al astuto y deshonesto programa de vigilancia digital, que apunta a activistas locales y extranjeros. Una activista iraní que vive en el extranjero describió cómo los funcionarios iraníes habían intentado engañarla con mensajes del teléfono de su hermano detenido. A fines de 2020, Irán también participó en intentos de *phishing* avanzado en Suecia con una aplicación maliciosa (*malware*, en inglés) al parecer diseñada para ayudar a los hablantes persas a obtener una licencia de conducir local.[15]

Esta creciente represión digital no se limita a Irán. Un activista ruso contó que, hace diez años, rusos de todo tipo publicaban sin temor en Facebook sobre las protestas contra Putin. Ahora, él y otros activistas están preocupados por la aplicación extrema por parte del Kremlin de las leyes de censura y discurso digital, que facilita el omnipresente sistema de vigilancia SORM (sistema de medidas de investigación operativa) que ha permitido el acceso sin restricciones

al tráfico de Internet ruso no cifrado, junto con la mayor capacidad del régimen para bloquear o reducir el tráfico de sitios web internacionales e incluso VPN. En Nicaragua, la represión física se une a una nueva ley de delitos cibernéticos (enero de 2021), que penaliza cualquier noticia supuestamente falsa o distorsionada que se difunda en línea, lo que empuja a los activistas a la clandestinidad. En Sudán del Sur, para evitar la vigilancia del Servicio de Seguridad Nacional, los activistas no hablan sobre temas confidenciales por teléfono.[16] Los regímenes represivos también están aprendiendo a socavar las herramientas comunes de seguridad digital, como bloquear proveedores de VPN o interceptar códigos de autenticación de dos factores enviados a través de mensajes de texto. Aun así, la herramienta represiva más preocupante sigue siendo la tecnología menos avanzada, ya que los regímenes obligan a los activistas detenidos a desbloquear sus dispositivos y, luego, a identificar a otros activistas para arrestarlos.

En resumen, el espacio cívico en línea verdaderamente libre es cada vez más escaso, lo que provoca un efecto desalentador entre los activistas. El ejemplo reciente más llamativo es el de Hong Kong, donde en 2020, activistas desesperados cancelaron sus cuentas en redes sociales en respuesta a una nueva ley de seguridad. Muchos activistas rusos huyeron del país. Aunque los activistas extranjeros siguen operando en línea, no pueden unirse a las protestas físicas en el país, y algunos incluso limitan su contacto con los que permanecen en Rusia por cuestiones de seguridad. De todos modos, algunas de las personas entrevistadas expresaron su confianza en que podrían protegerse en línea, y la mayoría se resigna a la idea de que su Gobierno podría, en última instancia, meterse en su vida privada si decidiera hacerlo. Tampoco es necesario que los regímenes promulguen medidas represivas totales para desencadenar este efecto desalentador, como explicó un activista de Hong Kong: solo un arresto al mes basta para intimidar a los activistas y lograr la autocensura. Que muchos acepten con valentía los riesgos como un sacrificio necesario para el activismo no los hace menos preocupantes.

Gigantes tecnológicos: ¿Aliados o enemigos?

Más allá de los Gobiernos hostiles, los activistas también enfrentan desafíos de empresas tecnológicas internacionales. Estas empresas utilizan su poder para dar forma a las posibilidades del activismo en línea, una realidad inminente en la mente de casi todas las personas entrevistadas. Como dijo un activista e instructor de seguridad digital: “Lo primero que pienso cuando me despierto por la mañana es qué hizo Facebook hoy”. Históricamente, los gigantes tecnológicos han priorizado sus ganancias por encima de la seguridad y las aspiraciones de los activistas, y sus medidas a veces son perjudiciales para las campañas no violentas.

Otros han escrito en detalle sobre los derechos humanos y los gigantes tecnológicos en la era digital.[17] La siguiente sección destaca dos dificultades principales para los activistas: el control del contenido en las redes sociales y la rápida proliferación de tecnologías de vigilancia digital.

CONTROL DEL CONTENIDO EN LAS REDES SOCIALES

Quién puede decir qué en línea es fundamental para la acción no violenta del siglo XXI. En este sentido, las empresas de redes sociales dictan sus propias leyes, lo que delimita la libertad de expresión en diversos contextos sociales y políticos, pero con poca responsabilidad respecto de errores incluso atroces. Si bien el control del contenido representa un desafío excepcional en las mejores circunstancias, los empresarios tecnológicos de Silicon Valley han estado (y en gran medida siguen estando) trágicamente mal preparados para administrar las responsabilidades éticas y morales asociadas con el control del contenido.

Las empresas de redes sociales con frecuencia aceptan las demandas del régimen para eliminar el contenido de la oposición, lo que las convierte directamente en cómplices de la represión autocrática. Asombrosamente, esta práctica es común y a menudo se produce en respuesta a solicitudes privadas.

De forma paradójica, las empresas de redes sociales realizan tanto un control deficiente como excesivo del contenido. Con respecto al control deficiente, Facebook se expandió con rapidez a muchos países sobre los que la empresa carece incluso de conocimiento de las diferencias culturales, ni que hablar de personal dedicado que domine los idiomas locales. Como resultado, no logra controlar de manera sistemática el contenido realmente violento. Por ejemplo, no pudo restringir un aluvión de expresiones de odio contra los rohinyás en Birmania que alimentó una campaña de limpieza étnica en ese país, ni controlar la incitación al odio en Etiopía durante la guerra civil en curso. En ambos casos, se debió a que la empresa no tenía apoyo lingüístico local, a pesar de las reiteradas advertencias internas. Activistas de Etiopía enviaron hojas de cálculo de Excel llenas de publicaciones ofensivas a Facebook para su eliminación y, por lo general, no recibieron respuesta o, en algunos casos, en las respuestas se solicitaban las traducciones al inglés.[18]

Con respecto al control excesivo, los ejemplos de censura injustificable son tantos que desafían el registro integral.[19] El problema empeoró cuando las grandes empresas de redes sociales, abrumadas por la gran cantidad de publicaciones diarias, cambiaron a un control algorítmico del contenido que incorpora sesgos sistemáticos. Facebook ha bloqueado publicaciones propalestinas que los censuradores relacionan por error con terrorismo; por otro lado, los censuradores antiviolencia de YouTube eliminan videos, publicados por activistas, de los crímenes de guerra del régimen de Assad.[20] Hace poco, Facebook empoderó a un nuevo organismo, la Junta de Supervisión, que ha revertido algunas de sus decisiones de censura. Sin embargo, los millones de eliminaciones injustas que quedan sin resolver eclipsan el tiempo y los recursos limitados que tiene la Junta de Supervisión para presentar apelaciones.[21]

Además, las empresas de redes sociales con frecuencia aceptan las demandas del régimen de eliminar el contenido de la oposición, lo que las convierte directamente en cómplices de la represión autocrática. Asombrosamente, esta práctica es común y a menudo se produce en respuesta a solicitudes privadas. Por ejemplo, el director ejecutivo de Facebook, Mark Zuckerberg, autorizó personalmente censurar el contenido de la oposición antes del congreso del partido de Vietnam en enero, y hace poco, Google y Apple cedieron a las presiones para eliminar la aplicación de votación inteligente “Smart Voting” del líder opositor Alexei Navalny el día de las elecciones de 2021 en Rusia.[22] Es indiscutible que dicha censura es contraria a los valores democráticos liberales. Sin embargo, las empresas de redes sociales suelen ceder ante las leyes locales (para preservar así el acceso al mercado), incluso cuando las leyes locales no concuerdan con las leyes internacionales sobre derechos humanos.

El control del contenido a escala es un desafío sin una solución directa. La censura automática puede limitar las expresiones de odio, pero también censurar sin querer contenidos de activistas auténticos. Por esa razón, los esfuerzos continuos de la Unión Europea por responsabilizar a las empresas de redes sociales por el contenido pueden ser contraproducentes: las empresas pueden imponer una censura absolutamente estricta para evitar la exposición legal y restringir así el alcance global de los activistas.[23] Sin embargo, lo que está claro es que las grandes empresas de redes sociales ingresaron en nuevos mercados sin prestar demasiada atención a las posibles inquietudes de seguridad y, con demasiada frecuencia, anteponen su deseo de obtener ganancias a los derechos humanos de sus usuarios activistas. Que solo Reddit haya cumplido en su totalidad los Principios de Santa Clara para el control del contenido, un parámetro relativamente bajo, sugiere que existe una desconfianza fundamental de los activistas con respecto a los gigantes tecnológicos.[24]

TECNOLOGÍAS DE VIGILANCIA

Otra gran inquietud es la venta de tecnologías de doble uso a regímenes que facilitan la represión violenta de forma directa. El ejemplo reciente más destacado es NSO Group de Israel y su programa informático espía (*spyware*, en inglés) Pegasus, que al parecer se vende con fines antiterroristas, pero que en realidad está vinculado a la vigilancia ilegal de miles de objetivos lícitos por parte de regímenes represivos.

Dicho esto, la raíz del problema es más mundana que las innovadoras vulnerabilidades sin clics. Durante años, empresas privadas han vendido la tecnología de doble uso necesaria para el filtrado y la vigilancia de contenido básico a dictaduras despiadadas, en algunos casos con el respaldo directo de los Estados Unidos y otras democracias liberales occidentales.[25] Esto ha permitido a los regímenes que no tienen industria tecnológica nacional desarrollar una mejor capacidad represiva digital. Entre muchos otros ejemplos, el régimen militar de Birmania ha utilizado equipos de vigilancia occidentales para aplastar a la oposición actual y lograr el reciente golpe de Estado.[26] Sudán del Sur depende de la tecnología de vigilancia israelí para vigilar a sus ciudadanos.[27] Y Bielorrusia utilizó tecnología de inspección profunda de paquetes de la empresa canadiense Sandvine para incluir sitios web de la oposición en la lista negra durante sus elecciones presidenciales de 2020.[28]

En la mayoría de estas democracias, la comercialización de tecnología de doble uso está al parecer regulada por las leyes existentes. Sin embargo, como lo demuestra la rápida propagación de la tecnología de vigilancia occidental a las autocracias del mundo, estas regulaciones son débiles, se las puede ignorar con facilidad y están mal aplicadas.[29] De este modo, la industria privada ha facilitado la proliferación mundial de tecnologías represivas digitales, en detrimento de los activistas.

DEFENSA DE LOS DERECHOS DIGITALES

En respuesta a estos desafíos, los activistas han aceptado la necesidad de una defensa transnacional de los derechos digitales. Los movimientos sociales modernos no pueden abandonar el activismo en línea, por lo que los activistas están haciendo un gran esfuerzo para luchar contra la complicidad de los gigantes tecnológicos con el autoritarismo digital.

Para empezar, trabajan para apelar al control injustificado del contenido. A veces, aprovechan los vínculos personales con quienes tienen buenos contactos en la industria tecnológica o con periodistas que actúan como intermediarios entre los activistas y los equipos de redes sociales. Por ejemplo, en 2010, el empleado de Google Wael Ghonim pudo usar su influencia como empleado de una importante empresa tecnológica para deshacer rápidamente el bloqueo de Facebook de la página "We Are All Khaled Saeed" (Todos somos Khaled Saeed) que él administraba, un importante foro para hablar sobre política y violencia policial en Egipto. La página se llama así por un joven que había sido asesinado a golpes por la policía a principios de ese año.[30] De manera similar, un activista de Sudán del Sur informó que se comunica de manera habitual con Facebook para identificar usuarios maliciosos y ayudar a los activistas a resolver problemas. En otros casos, surgen amplias campañas transnacionales de defensa para combatir el abuso sistemático que, a menudo, se presentan en las propias plataformas ofensivas, como las campañas palestinas contra la censura en Facebook.[31]

Este sistema de rectificación no es ideal porque privilegia a los usuarios con buenos contactos que hablan inglés con fluidez y tienen vínculos con empresas tecnológicas estadounidenses. Un activista de Sudán del Sur informó que pudo lograr que Facebook eliminara o restableciera el acceso a su antigua cuenta que los agentes del régimen habían pirateado. Como se mencionó, la mayoría de las apelaciones de los usuarios a la censura algorítmica incorrecta no se procesan, y los fracasos de Facebook en Birmania y Etiopía evidencian aún más los límites del alcance activista a las empresas de redes sociales. Sin embargo, la retroalimentación colectiva constante es una herramienta esencial para la defensa de los derechos de los usuarios.

Wael Ghonim, en el centro, llega a la plaza Tahrir en El Cairo después de la declaración televisada del presidente egipcio Hosni Mubarak a la nación el 10 de febrero de 2011. Ghonim utilizó sus conexiones tecnológicas para deshacer un bloqueo de Facebook. (Fotografía de Tara Todras-Whitehill/AP)

En un nivel más amplio, la necesidad de defender los derechos digitales ha fomentado una nueva especialización entre los activistas en torno a estas cuestiones. Algunas de las personas entrevistadas para este informe se autoidentificaron como activistas de derechos digitales y se han dedicado a preservar Internet como un espacio para la libertad de expresión y el cambio social. Quienes no tenían habilidades técnicas especializadas con frecuencia informaron que conocían a alguien o algún grupo al podían recurrir para obtener ayuda. Sus esfuerzos se parecen a las actividades de organizaciones internacionales como EFF, The Citizen Lab, Paradigm Initiative y muchas otras que han establecido colaboraciones laborales duraderas con comunidades activistas, y ofrecen asesoramiento técnico y capacitación, documentan la propagación global de programas informáticos espías (*spyware*) y otras prácticas abusivas, y presionan tanto a los gigantes tecnológicos como a los Gobiernos de todo el mundo para que realicen las reformas necesarias.

Estos son acontecimientos aceptados, lo que sugiere que las comunidades activistas están desarrollando constantemente el conocimiento, la capacidad y los vínculos internacionales necesarios para combatir el autoritarismo digital. Sin embargo, el campo de juego sigue estando desnivelado, porque los activistas compiten contra Gobiernos represivos con mejores recursos y que también presionan a los gigantes tecnológicos. Estas empresas han demostrado una buena predisposición a cumplir con las solicitudes de desmantelamiento y las restricciones de acceso a fin de preservar la participación en el mercado, a pesar de la indignación de activistas. Otras venden de manera intencional equipos de vigilancia avanzada a las dictaduras con fines de

lucro y eluden con cinismo la responsabilidad cuando esa tecnología se utiliza inevitablemente para reprimir a los activistas pacíficos. Como se analiza en las siguientes recomendaciones, la presión pública ha tenido algunos éxitos notables al obligar a las empresas tecnológicas a cambiar su comportamiento. Sin embargo, muchos de sus negocios se llevan a cabo fuera del ojo público, y las victorias aisladas ante la falta de regulaciones más amplias representan un control inadecuado de los excesos de los gigantes tecnológicos.

Recomendaciones sobre políticas: Acelerar las innovaciones de los activistas

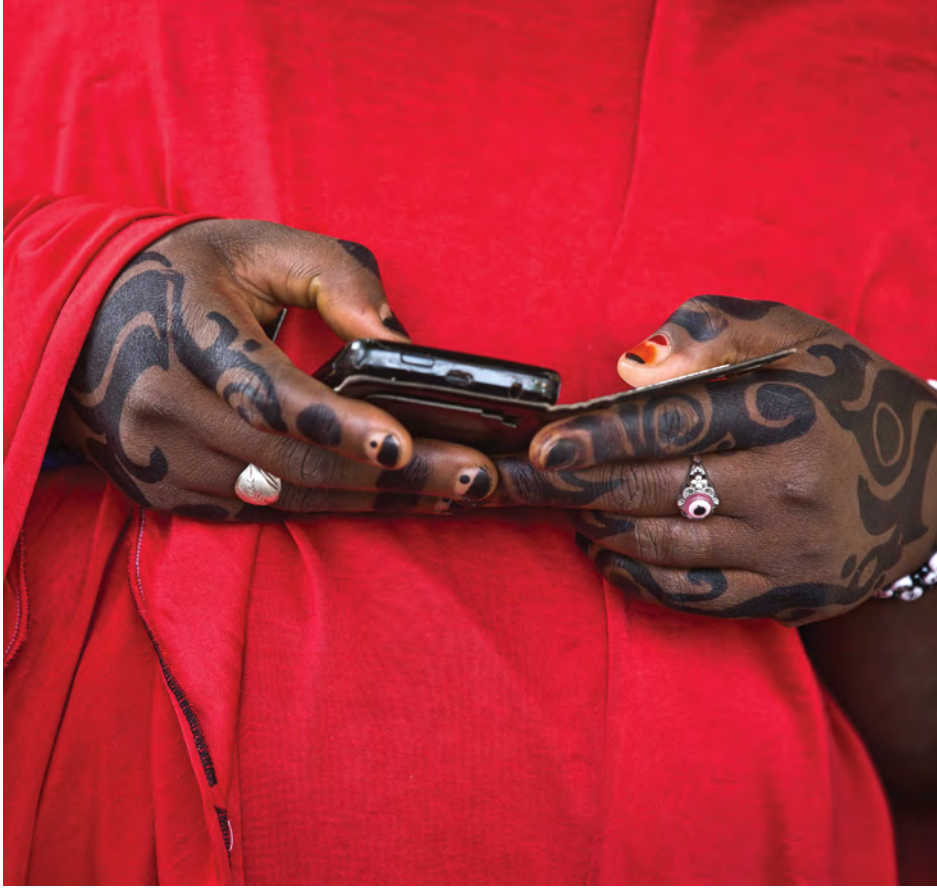
La dinámica aquí descrita es una instantánea en el tiempo dentro de un proceso más amplio, el del equilibrio en constante cambio de las capacidades digitales entre activistas y autócratas. Testimonio tras testimonio, los activistas describen cómo el ritmo acelerado del cambio tecnológico ha modificado a favor y en contra este equilibrio de poder. Tienen una gran motivación para innovar y a menudo son los primeros en reconocer las ventajas de las nuevas tecnologías. Es posible que los opositores autoritarios solo aprecien tarde este potencial; sin embargo, una vez que reconocen la amenaza, ordenan los recursos superiores para borrar la ventaja inicial de los activistas, lo que requiere un nuevo ciclo de innovación táctica y tecnológica para recuperar la paridad, si no ventaja. Este equilibrio tecnológico entre activistas y autócratas se encuentra en constante evolución. Por lo tanto, el crecimiento del autoritarismo digital no es un evento único, sino un proceso continuo de interacción y aprendizaje entre activistas, autócratas y empresas tecnológicas.

En este sentido, estar a la altura del desafío del autoritarismo digital requiere actuar en dos frentes paralelos. En primer lugar, las comunidades activistas y sus defensores internacionales deben esforzarse por acelerar el ritmo de la innovación de los movimientos en respuesta a las oportunidades y limitaciones digitales. En segundo lugar, los Estados Unidos y otras democracias liberales deben tener como prioridad obstruir, sancionar y, de otro modo, desacelerar el ritmo de la innovación autocrática en las tecnologías represivas digitales.

ACELERAR LAS ADAPTACIONES DE LOS ACTIVISTAS ANTE LA TECNOLOGÍA EMERGENTE

Una respuesta esencial al autoritarismo digital cada vez más sofisticado es mejorar la capacidad de los activistas para innovar con rapidez y adaptarse a los nuevos desafíos. En particular, las recomendaciones a corto plazo o las soluciones técnicas a problemas inmediatos son necesarias, pero inadecuadas. Ciertas recomendaciones estándar no son controvertidas, como el uso de cifrado de extremo a extremo, administradores de contraseñas y VPN fiables que no registran el tráfico y cambian con frecuencia entre servidores. Pero incluso estas vienen con advertencias contextuales. Un experto en seguridad digital destacó que su capacitación para activistas siempre comienza con un análisis contextual minucioso, una visión holística de cómo funciona ese grupo. Un enfoque miope sobre las recomendaciones técnicas puede parecerse peligrosamente a culpar a las víctimas, criticar a los activistas por no adoptar herramientas específicas, y aun así eludir las tantas presiones políticas, sociales y psicológicas que moldean sus elecciones.

Además, cualquier recomendación específica quedará inevitablemente obsoleta debido a los acontecimientos, en este ámbito con mayor rapidez que la mayoría. Incluso a corto plazo, los autócratas toman medidas para contrarrestar las adaptaciones técnicas descritas en este informe, por ejemplo, intentan regular el uso de VPN (como lo estipula una ley rusa sobre VPN de 2017) o separan la Internet nacional de la global (como hace Irán). A largo plazo, es casi seguro que los próximos



Una mujer de la tribu hausa mira su teléfono inteligente el 28 de marzo de 2015, en un centro de votación en Daura, Nigeria. En respuesta a la violencia en los estados del noroeste y centro de Nigeria, los gobernadores bloquearon las telecomunicaciones en muchas áreas de cinco estados para permitir las operaciones militares. (Fotografía de Ben Curtis/AP)

avances tecnológicos afectarán el equilibrio de poder entre autócratas y activistas. Es probable que las computadoras cuánticas ampliables, que podrían aparecer en la próxima década, conviertan el cifrado existente en obsoleto de la noche a la mañana, lo que pondría en peligro la seguridad digital de los activistas, pero también empoderaría a quienes intentan descubrir evidencia oculta de los abusos del Gobierno.[32] Es posible que pronto los avances en inteligencia artificial permitan a los Gobiernos autoritarios analizar grandes cantidades de datos de vigilancia y, así, identificar patrones que pongan al descubierto a los activistas. Las mejoras en la tecnología de cadena de bloques podrían convertir la criptomoneda (que hoy no está disponible para la mayoría de los activistas debido a las barreras técnicas) en una forma fácil de recaudar fondos sin la vigilancia gubernamental. Un servicio de Internet por satélite de baja latencia y fácil acceso podría descentralizar los puntos de acceso a Internet y, así, inutilizar la censura y la vigilancia autocráticas.

Un examen más detallado de estas nuevas tecnologías queda fuera del alcance del presente informe. Cualquiera de estas innovaciones tiene el potencial de cambiar de forma radical el terreno tecnológico en el que los activistas y autócratas compiten de múltiples e impredecibles maneras.[33] En cambio, este informe hace hincapié en que lo que necesitan los activistas no es una respuesta técnica específica a los desafíos actuales, sino más bien cambios en el ecosistema activista para acelerar el aprendizaje y la adaptación al ritmo vertiginoso del cambio tecnológico, tanto para la actualidad como para el futuro.

Una forma de lograrlo es una mayor difusión de la capacitación en seguridad digital básica y pensamiento estratégico sobre amenazas digitales. Con el tiempo, diversas formas de represión digital adquirirán relevancia en casi todos los países, pero, como se indicó, las desigualdades mundiales en términos de quién puede acceder a capacitaciones en seguridad digital son significativas. Los esfuerzos internacionales se han centrado en unos cuantos países de alto perfil, como Rusia e Irán, cuyas comunidades activistas están ahora saturadas de conocimiento sobre seguridad digital, incluso cuando activistas en autocracias más periféricas o de menor capacidad tienen poco o ningún acceso. Una inclinación a favor de Occidente y los angloparlantes en el activismo digital y el espacio de seguridad significa también un gran obstáculo para la difusión de la innovación digital a través de las comunidades activistas.

En este sentido, los esfuerzos internacionales deben centrarse en ampliar la capacitación más allá de los países “prioritarios” más estrechamente asociados al autoritarismo digital y llegar a países en los que este desafío sigue latente. Un esfuerzo conjunto para traducir el conocimiento sobre seguridad digital a más idiomas avanzaría hacia la aceleración del ritmo de aprendizaje de

El activismo digital y la represión son posibles, en gran medida, gracias a empresas tecnológicas radicadas en las democracias occidentales . . . Las decisiones tomadas en las salas de juntas de Silicon Valley tienen efectos secundarios desde Moscú hasta Managua.

los activistas. Además, estos esfuerzos deben trascender un simple modelo de capacitación basado en el "volcado de información". Un curso rápido sobre los aspectos básicos de la seguridad digital es solo una pequeña parte de una estrategia más amplia para acelerar la adaptación activista al autoritarismo digital. En su lugar, los participantes internacionales deben buscar una capacitación holística que no cubra solo los fundamentos de una buena higiene digital, sino que también considere cómo el activismo digital se conecta con el activismo del mundo real, cuestione de manera crítica las tendencias actuales sobre activismo digital y cómo podrían cambiar con el tiempo, y ofrezca apoyo para la carga psicológica asociada con el activismo digital, entre otros temas útiles.

Otra sabia inversión a largo plazo para los participantes internacionales es facilitar el crecimiento de redes sólidas de activistas transnacionales. Como dijo un activista bielorruso: "Lo que necesitamos es la gestión y el intercambio de conocimiento. . . . Cuando estábamos creando soluciones en Bielorrusia, ni siquiera sabíamos dónde preguntar. Tuvimos que crear todo desde cero. Si hubiéramos obtenido la experiencia de otros países, habríamos ahorrado mucho tiempo y esfuerzo". Como dijo otro activista e instructor de seguridad digital: "Conocer las historias de otros activistas nos ayuda a reconocer nuestros errores más rápido y crear estrategias. Saber que no estamos solos es un poderoso motivador".

Numerosas pruebas indican que reunir a activistas de una amplia gama de contextos para compartir historias y lecciones aprendidas es una de las formas más eficaces de obtener apoyo externo.[34] En las últimas décadas, las redes activistas transnacionales han sido fundamentales para muchos de los desarrollos estratégicos más importantes en la acción no violenta.[35] La comunidad internacional puede ayudar a crear estas redes, ofreciendo foros para el debate y aprendiendo sobre activismo y seguridad digital. Cuanto más completas sean estas redes y más fácil fluya la información dentro de ellas, más probable será que las innovaciones relevantes generadas en un contexto puedan adoptarse con rapidez en otro.

Por otro lado, los donantes internacionales y quienes apoyan la acción no violenta deben incorporar mejor la seguridad digital como un componente esencial de todos los proyectos realizados en contextos potencialmente represivos. Varios activistas dijeron que era difícil convencer a los financiadores internacionales para que consideraran con seriedad los costos operativos asociados con medidas básicas de seguridad digital, como licencias de VPN, computadoras y teléfonos seguros o almacenamiento cifrado en la nube. Al elegir socios y diseñar programas, los financiadores deben evaluar con cautela el panorama digital con el mismo cuidado que el panorama político o económico de un país. Naturalmente, los partidarios externos de las campañas de acción no violenta deben analizar en profundidad su propia seguridad digital para identificar posibles puntos débiles que expongan a sus socios activistas.

SOFOCAR LA INNOVACIÓN AUTOCRÁTICA

Al mismo tiempo, los actores internacionales también deben esforzarse por frenar el autoritarismo digital negando a los autócratas el acceso a las herramientas, las tecnologías y los conocimientos necesarios para innovar en nuevas técnicas represivas. Los Estados democráticos que esperan apoyar la expresión libre y pacífica de reclamos a través de la acción no violenta tienen un papel crucial que desempeñar. El activismo digital y la represión son posibles, en gran medida, gracias a empresas tecnológicas radicadas en las democracias occidentales (las más influyentes se encuentran en los Estados Unidos). Las decisiones tomadas en las salas de juntas de Silicon Valley tienen efectos secundarios desde Moscú hasta Managua.

A su vez, es esencial la coordinación intergubernamental en torno a controles estrictos, amplios y bien aplicados sobre la distribución de tecnologías de vigilancia de doble uso. En este sentido, los Estados ya han tomado algunas medidas en la dirección correcta. La Unión Europea está trabajando con una evidente determinación para endurecer la regulación de las empresas tecnológicas, sobre todo a través de la Ley de Servicios Digitales, que probablemente entrará en vigencia en 2022.[36] Estados Unidos también ha empezado a tomar con mayor seriedad los controles de exportación de tecnología de doble uso y, hace poco, agregó más empresas tecnológicas (incluida NSO Group de Israel) a la lista de entidades del Departamento de Comercio, que prohíbe a las empresas estadounidenses exportar tecnología a las partes incluidas, y adoptó nuevas regulaciones que prohíben la exportación de software de intrusión y otras tecnologías de ciberseguridad sin una licencia aprobada.[37]

Además de alinear los incentivos financieros de las empresas tecnológicas con los derechos humanos básicos, un control más estricto de las exportaciones también podría lanzar el cambio normativo tan necesario en la política de ciberseguridad de los Estados Unidos. Durante la mayor parte de las últimas dos décadas, Estados Unidos adoptó herramientas que invaden la privacidad en nombre del antiterrorismo y a costa de los activistas. En el futuro, Washington debe esforzarse por desarrollar nuevas normas globales de privacidad y cifrado, invirtiendo recursos para mejorar el acceso al cifrado y a la tecnología antivigilancia y, al mismo tiempo, condicionando la ayuda extranjera a las garantías del Estado para cumplir con los principios fundacionales de la privacidad digital. También debe colaborar con las empresas de redes sociales para animarlas a resistir las demandas de los regímenes autocráticos de eliminar contenido crítico o proporcionar información personal de los usuarios en casi todas las circunstancias. Si bien analizar por completo las medidas políticas disponibles está fuera del alcance de este informe, en general, Estados Unidos debe desarrollar nuevas normas de privacidad y libertad en línea en vez de mantener un *statu quo* totalmente incompatible con el ejercicio de los derechos humanos en la era digital.

Por último, la presión pública también es una fuente importante de influencia contra corporaciones obstinadas y regímenes represivos por igual. Por ejemplo, la reciente protesta pública sobre la tecnología de filtrado de Sandvine que permitía interrupciones de Internet en Bielorrusia tuvo una exitosa presión para que la empresa finalizara su contrato con el Gobierno bielorruso.[38] Del mismo modo, la combinación de indignación pública y presión gubernamental en respuesta a las revelaciones sobre las fechorías de NSO Group llevó a Israel a recortar su lista de exportación cibernética permitida para excluir una serie de autocracias violentas.[39] También se pueden usar diversas formas de presión externa directamente contra las autocracias ofensivas, lo que aumenta el "dilema digital del dictador", en el que la represión digital provoca una reacción pública significativa y un perjuicio para la reputación.[40]

A medida que el frente de la tecnología emergente cambie en los próximos años, el equilibrio digital de poder entre los autócratas represivos y los activistas no violentos que se oponen a estos cambiará de maneras impredecibles. Independientemente de las nuevas tecnologías que traiga el futuro, los actores internacionales pueden ayudar a inclinar la balanza a favor de los activistas no violentos, tanto reforzando la capacidad estratégica de los activistas para responder a los avances tecnológicos como obstaculizando la capacidad de los autócratas para utilizar tecnologías emergentes para reprimir el cambio pacífico. Luego de un esfuerzo tan decidido y coordinado, las tecnologías digitales podrán al fin cumplir la promesa como herramientas de liberación masiva.

Notas

1. Para ver una introducción de las publicaciones sobre tecnología digital y protestas masivas, consulte Larry Diamond, "Liberation Technology", *Journal of Democracy* 21, n.º 3 (2010): 69–83; Marc Lynch, "After Egypt: The Limits and Promise of Online Challenges to the Authoritarian Arab State", *Perspectives on Politics* 9, n.º 2 (junio de 2011): 301–10; Jennifer Earl y Katrina Kimport, *Digitally Enabled Social Change: Activism in the Internet Age* (Cambridge, MA: MIT Press, 2013); Andrew T. Little, "Communication Technology and Protest", *Journal of Politics* 78, n.º 1 (enero de 2016): 152–66; Nils B. Weidmann y Espen Geelmuyden Rød, *The Internet and Political Protest in Autocracies* (Nueva York: Oxford University Press, 2019); Killian Clarke y Korhan Kocak, "Launching Revolution: Social Media and the Egyptian Uprising's First Movers", *British Journal of Political Science* 50, n.º 3 (julio de 2020): 1025–45; Ruben Enikolopov, Alexey Makarin y Maria Petrova, "Social Media and Protest Participation: Evidence From Russia", *Econometrica* 88, n.º 4 (2020): 1479-514.
2. Wael Ghonim, *Revolution 2.0: The Power of the People Is Greater Than the People in Power* (Nueva York: Houghton Mifflin Harcourt, 2012).
3. Matthew Cebul y Jonathan Pinckney, "Digital Authoritarianism and Nonviolent Action: Challenging the Digital Counterrevolution", Informe especial n.º 499, United States Institute of Peace, julio de 2021, www.usip.org/publications/2021/07/digital-authoritarianism-and-nonviolent-action-challenging-digital; Andrea Kendall-Taylor, Erica Frantz y Joseph Wright, "The Digital Dictators", *Foreign Affairs*, 2 de febrero de 2020, www.foreignaffairs.com/articles/china/2020-02-06/digital-dictators; Steven Feldstein, *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance* (Nueva York: Oxford University Press, 2021).
4. Freedom House, "Freedom on the Net 2021: The Global Drive to Control Big Tech", 2021, www.freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech.
5. Entre ellos, se incluyen Bangladés, Bielorrusia, China (Hong Kong), Irán, Nicaragua, Nigeria, Rusia, Sudán del Sur y Vietnam.
6. Debido a las restricciones de viaje impuestas por la pandemia de COVID-19, las entrevistas se realizaron a través de sesiones de Zoom cifradas. Estas entrevistas se realizaron luego de la aprobación de la Junta de Revisión Institucional de Health Media Lab (revisión n.º 950USIP21). Para proteger la seguridad de las personas entrevistadas, todas las citas son anónimas. Las personas entrevistadas se identifican únicamente con descripciones no específicas de su país y función.
7. Feldstein, *Rise of Digital Repression*; Adrian Shahbaz, "The Rise of Digital Authoritarianism", Freedom House, 2018, www.freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism; Cebul y Pinckney, "Digital Authoritarianism and Nonviolent Action".
8. Stephanie Kirchgaessner *et al.*, "Revealed: Leak Uncovers Global Abuse of Cyber-Surveillance Weapon", *The Guardian*, 18 de julio de 2021, www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus.
9. La legibilidad de las comunicaciones digitales es uno de los dos desafíos principales que plantean las tecnologías emergentes para los movimientos no violentos. Consulte Cebul y Pinckney, "Digital Authoritarianism and Nonviolent Action", 5-7.
10. Consulte también Rachel Yeo, "What Is LIHKG and How Did It Become Go-to Forum for Hong Kong's Protesters?", *South China Morning Post*, 3 de agosto de 2019, www.scmp.com/news/hong-kong/society/article/3021224/hong-kong-protests-how-citys-reddit-forum-lihkg-has-become; Nicolle Liu y Sue-Lin Wong, "How to Mobilize Millions: Lessons from Hong Kong", OZY, 7 de julio de 2019, www.ozy.com/around-the-world/how-to-mobilize-millions-lessons-from-hong-kong/95354.
11. Curiosamente, el estímulo para la adopción de VPN a menudo parece ser un intento del Gobierno de prohibir por completo contenido popular en línea, como Instagram o YouTube; consulte William R. Hobbs y Margaret E. Roberts, "How Sudden Censorship Can Increase Access to Information", *American Political Science Review* 112, n.º 3 (agosto de 2018): 621-36.
12. EFF, "Surveillance Self-Defense", https://ssd.eff.org/en; The Citizen Lab, "Security Planner", www.citizenship lab.ca/category/research/tools-resources/security-planner; Security First, "What is Umbrella?", www.secfirst.org/umbrella; Paradigm Initiative, "Ayeta: A proactive toolkit for African digital rights actors", www.paradigmhq.org/programs/digital-rights/ayeta.
13. Facebook asegura que todos los mensajes de WhatsApp están cifrados de extremo a extremo, pero en los informes de los medios de comunicación se indican violaciones no reveladas anteriormente de este cifrado. Consulte, por ejemplo, Peter Elkind, Jack Gillum y Craig Silverman, "How Facebook Undermines Privacy Protections for its 2 Billion WhatsApp Users", *ProPublica*, 8 de septiembre de 2021, www.propublica.org/article/how-facebook-undermines-privacy-protections-for-its-2-billion-whatsapp-users.
14. Cebul y Pinckney explican el auge de las autocracias digitales en "Digital Authoritarianism and Nonviolent Action".
15. Check Point Research, "Rampant Kitten: An Iranian Espionage Campaign", 18 de septiembre de 2020, https://research.checkpoint.com/2020/rampant-kitten-an-iranian-espionage-campaign.

16. También consulte Amnistía Internacional, "These Walls Have Ears: The Chilling Effect of Surveillance in South Sudan", febrero de 2021, www.amnesty.org/en/documents/afr65/3577/2021/en/.
17. Para los aspectos básicos útiles, consulte Rebecca MacKinnon, *No sin nuestro consentimiento: La lucha por la libertad en Internet*, edición reimpresa (Nueva York: Basic Books, 2013); Ronald J. Deibert, "The Road to Digital Unfreedom: Three Painful Truths About Social Media", *Journal of Democracy* 30, n.º 1 (enero de 2019): 25–39; Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Nueva York: PublicAffairs, 2019); Jillian C. York, *Silicon Values: The Future of Free Speech Under Surveillance Capitalism* (Londres: Verso, 2021).
18. Consulte Euan McKirdy, "Facebook: We didn't do enough to prevent Myanmar violence", CNN, 6 de noviembre de 2018, https://edition.cnn.com/2018/11/06/tech/facebook-myanmar-report/index.html; Eliza Mackintosh, "Facebook knew it was being used to incite violence in Ethiopia. It did little to stop the spread, documents show", CNN, 25 de octubre de 2021, www.cnn.com/2021/10/25/business/ethiopia-violence-facebook-papers-cmd-intl/index.html; Rishi Inyengar, "Facebook has language blind spots around the world that allow hate speech to flourish", CNN, 26 de octubre de 2021, www.cnn.com/2021/10/26/tech/facebook-papers-language-hate-speech-international/index.html.
19. York, *Silicon Values*.
20. Elizabeth Dwoskin y Gerrit De Vynck, "Facebook's AI Treats Palestinian Activists Like It Treats American Black Activists. It Blocks Them", *Washington Post*, 28 de mayo de 2021, www.washingtonpost.com/technology/2021/05/28/facebook-palestinian-censorship; Human Rights Watch, "Israel/Palestine: Facebook Censors Discussion of Rights Issues", 8 de octubre de 2021, www.hrw.org/news/2021/10/08/israel/palestine-facebook-censors-discussion-rights-issues.
21. Es probable que Facebook tome cientos de miles de decisiones incorrectas cada día sobre eliminación de contenido. Consulte Kristen Grind, "Inside 'Facebook Jail': The Secret Rules that Put Users in the Doghouse", *Wall Street Journal*, 4 de mayo de 2021, www.wsj.com/articles/inside-facebook-jail-trump-the-secret-rules-that-put-users-in-the-doghouse-11620138445.
22. Anton Troianovski y Adam Satariano, "Google and Apple, Under Pressure from Russia, Remove Voting App", *New York Times*, 17 de septiembre de 2021, www.nytimes.com/2021/09/17/world/europe/russia-navalny-app-election.html; Elizabeth Dwoskin, Tory Newmyery Shibani Mahtani, "The case against Mark Zuckerberg: Insiders say Facebook's CEO choose growth over safety", *Washington Post*, 25 de octubre de 2021, www.washingtonpost.com/technology/2021/10/25/mark-zuckerberg-facebook-whistleblower.
23. Christopher Schmon, "European Parliament's Plans of a Digital Services Act Threaten Internet Freedom", Electronic Frontier Foundation, 10 de noviembre de 2021, www.eff.org/deeplinks/2021/11/european-parliaments-plans-digital-services-act-threaten-internet-freedoms.
24. The Santa Clara Principles on Transparency and Accountability in Content Moderation, https://santaclaraprinciples.org.
25. Consulte Steven Feldstein, "Governments Are Using Spyware on Citizens: Can They Be Stopped?", Carnegie Endowment for International Peace, 21 de julio de 2021, www.carnegieendowment.org/2021/07/21/governments-are-using-spyware-on-citizens.-can-they-be-stop-pub-85019; Siena Anstis, Sharly Chan, Adam Senft y Ronald J. Deibert, "Annotated Bibliography: Dual-Use Technologies: Network Traffic Management and Device Intrusion for Targeted Monitoring", The Citizen Lab, septiembre de 2019, www.citizenship lab.ca/wp-content/uploads/2019/09/Annotated-Bibliography-Network-Traffic-Management-and-Device-Intrusion-for-Targeted-Monitoring.pdf.
26. Hannah Beech, "Myanmar's Military Deploys Digital Arsenal of Repression in Crackdown", *New York Times*, 1 de marzo de 2021, www.nytimes.com/2021/03/01/world/asia/myanmar-coup-military-surveillance.html.
27. Amnistía Internacional, "These Walls Have Ears".
28. Ryan Gallagher, "U.S. Company Faces Backlash After Belarus Uses its Tech to Block Internet", Bloomberg, 11 de septiembre de 2020, www.bnnbloomberg.ca/u-s-company-faces-backlash-after-belarus-uses-its-tech-to-block-internet-1.1492656.
29. Para obtener más información sobre las empresas que comercializan tecnologías de intrusión cibernética a adversarios de la OTAN, consulte Winnona DeSombre, Lars Gjesvik y Johann Ole Willers, "Surveillance Technology at the Fair: Proliferation of Cyber Capabilities in International Arms Markets", Atlantic Council, noviembre de 2021, www.atlanticcouncil.org/wp-content/uploads/2021/11/Surveillance-Technology-at-the-Fair.pdf.
30. Zeynep Tufekci, *Twitter and Tear Gas: The Power and Fragility of Networked Protest* (New Haven, CT: Yale University Press, 2017); York, *Silicon Values*.
31. Por ejemplo, consulte Tell Facebook: Stop Silencing Palestine, www.stopsilencingpalestine.com.
32. Consulte William Barker, William Polk y Murugiah Souppaya. "Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms", NIST Cybersecurity White Paper, Instituto Nacional de Estándares y Tecnología, 28 de abril de 2021, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04282021.pdf.

33. Por ejemplo, consulte los posibles numerosos escenarios descritos en Miles Brundage *et al.*, "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation", *ArXiv Preprint*, febrero de 2018.
34. Erica Chenoweth y Maria J. Stephan, *The Role of External Support in Nonviolent Campaigns: Poisoned Chalice or Holy Grail?* (Washington, DC: ICNC Press, 2021); Ray Salvatore Jennings, "Serbia's Bulldozer Revolution: Evaluating Internal and External Factors in Successful Democratic Breakthrough in Serbia", documento de trabajo n.º 105 de *CDDRL* (Stanford, CA: Sanford University, Center on Democracy, Development and the Rule of Law, 2009), https://cddrl.fsi.stanford.edu/publications/serbias_bulldozer_revolution_evaluating_internal_and_external_factors_in_successful_democratic_breakthrough_in_serbia.
35. Margaret E. Keck y Kathryn Sikkink, *Activists Beyond Borders: Advocacy Networks in International Politics* (Ithaca, NY: Cornell University Press, 1998); Valerie J. Bunce y Sharon L. Wolchik, *Defeating Authoritarian Leaders in Postcommunist Countries* (Nueva York: Cambridge University Press, 2011).
36. Eliska Pirkova, "How the Digital Services Act Could Hack Big Tech's Human Rights Problem", Access Now, 15 de octubre de 2020, www.accessnow.org/eu-digital-services-act.
37. Drew Harwell, Ellen Nakashima y Craig Timberg, "Biden Administration Blacklists NSO Group over Pegasus Spyware", *Washington Post*, 3 de noviembre de 2021, www.washingtonpost.com/technology/2021/11/03/pegasus-nso-entity-list-spyware; Ellen Nakashima, "Commerce Department announces new rule aimed at stemming sale of hacking tools to Russia and China", *Washington Post*, 20 de octubre de 2021, www.washingtonpost.com/national-security/commerce-department-announces-new-rule-aimed-at-stemming-sale-of-hacking-tools-to-repressive-governments/2021/10/20/ecb56428-311b-11ec-93e2-dba2c2c11851_story.html.
38. Ryan Gallagher, "Francisco-Backed Sandvine Nixes Belarus Deal", *Bloomberg News*, 15 de septiembre de 2020, www.bloomberg.com/news/articles/2020-09-15/sandvine-says-it-will-no-longer-sell-its-products-in-belarus.
39. Meir Orbach, "Israeli Defense Ministry slashes cyber export list, drops Saudi Arabia, UAE", *Calcalist*, 25 de noviembre de 2021, www.calcalistech.com/ctech/articles/0,7340,L-3923361,00.html.
40. Feldstein, *Rise of Digital Repression*.

ACERCA DEL INSTITUTO

El Instituto de Paz de los Estados Unidos es un instituto nacional, no partidario e independiente, fundado por el Congreso y dedicado a la propuesta de que un mundo sin conflictos violentos es posible, práctico y esencial para la seguridad de los Estados Unidos y del mundo. En zonas de conflicto en el extranjero, el Instituto trabaja con socios locales para prevenir, mitigar y resolver conflictos violentos. Para reducir futuras crisis y la necesidad de intervenciones costosas, el USIP trabaja con los Gobiernos y las sociedades civiles para ayudar a sus países a resolver los problemas de forma pacífica. El Instituto ofrece experiencia, capacitación, análisis y apoyo a quienes trabajan para construir un mundo más pacífico e inclusivo.

JUNTA DIRECTIVA

George E. Moose (presidente), profesor adjunto de Práctica, The George Washington University, Washington, DC • Judy Ansley (vicepresidenta), exasistente del presidente y viceasesora sobre Seguridad Nacional durante el mandato del presidente George W. Bush, Washington, DC • Eric Edelman, profesional docente en ejercicio en Residencia en Roger Hertog, Johns Hopkins University School of Advanced International Studies, Washington, DC • Joseph Eldridge, profesional docente en ejercicio distinguido, School of International Service, American University, Washington, DC • Stephen J. Hadley, director, Rice, Hadley, Gates & Manuel LLC, Washington, DC • Kerry Kennedy, presidente, Robert F. Kennedy Human Rights, Washington, DC • Ikram U. Khan, presidente, Quality Care Consultants, LLC, Las Vegas, NV • Stephen D. Krasner, Graham H. Stuart Professor of International Relations, Stanford University, Palo Alto, CA • John A. Lancaster, exdirector ejecutivo, National Council on Independent Living, Potsdam, NY • Jeremy A. Rabkin, profesor de Derecho, Antonin Scalia Law School, George Mason University, Arlington, VA • J. Robinson West, expresidente, PFC Energy, Washington, DC • Nancy Zirkin, vicepresidente ejecutiva, Leadership Conference on Civil and Human Rights, Washington, DC

Miembros de derecho

Antony J. Blinken, secretario de Estado • Lloyd J. Austin III, secretario de Defensa • Michael T. Plehn, teniente general, Fuerza Aérea de los EE. UU.; presidente, National Defense University • Lise Grande, presidenta y directora ejecutiva, United States Institute of Peace (sin derecho a voto)

IMPRENTA DEL INSTITUTO DE PAZ DE LOS ESTADOS UNIDOS

Desde 1991, la imprenta del Instituto de Paz de los Estados Unidos ha publicado cientos de influyentes libros, informes y resúmenes sobre la prevención, el manejo y la resolución pacífica de conflictos internacionales. Esta área se compromete a promocionar la paz mediante la publicación de obras significativas y útiles destinadas a legisladores, profesionales, académicos, diplomáticos y estudiantes. Para mantener las mejores tradiciones de las publicaciones académicas, cada obra se somete a una rigurosa revisión de pares llevada a cabo por expertos en la materia externos para garantizar que la investigación, las perspectivas y las conclusiones sean equilibradas, relevantes y estén fundamentadas.

OTRAS PUBLICACIONES DE USIP

- *China's Security Force Posture in Thailand, Laos, and Cambodia* por John Bradford (Special Report, diciembre de 2021).
- *Removing Sanctions on North Korea: Challenges and Potential Pathways* por Troy Stangarone (Special Report, diciembre de 2021).
- *Engaging with Muslim Civil Society in Central Asia: Components, Approaches, and Opportunities* por Sebastien Peyrouse y Emil Nasritdinov (Peaceworks, diciembre de 2021).
- *Advancing Global Peace and Security through Religious Engagement: Lessons to Improve US Policy* por Peter Mandaville y Chris Seiple (Special Report, noviembre de 2021).
- *Young and Angry in Fezzan: Achieving Stability in Southern Libya through Greater Economic Opportunity* por Mary Fitzgerald y Nate Wilson (Peaceworks, noviembre de 2021).

UNITED STATES
INSTITUTE OF PEACE PRESS

2301 Constitution Avenue NW
Washington, DC 20037
(202) 457-1700
www.USIP.org