SPECIAL REPORT

N.º 499 | JULIO DE 2021 UNITED STATES INSTITUTE OF PEACE www.usip.org

Autoritarismo digital y acción no violenta: Desafiando la contrarrevolución digital

Por Matthew Cebul y Jonathan Pinckney

Personas encienden las linternas de sus teléfonos inteligentes en una manifestación en Hong Kong el 16 de junio de 2019 en conmemoración de la muerte de un compañero manifestante. (Fotografía de Lam Yik Fei/New York Times)

Contenidos

Resumen

- Las campañas de acción no violenta, en las que ciudadanos comunes usan tácticas como protestas, huelgas y boicots para ejercer presión sobre quienes detentan el poder, han sido una de las formas más eficaces de propiciar el cambio de manera pacífica en países autocráticos indiferentes.
- Estas campañas se crean cada vez más a través de tecnologías emergentes (Internet, redes sociales, inteligencia artificial y reconocimiento facial) que ofrecen beneficios significativos para la acción no violenta. Al mismo tiempo, estas tecnologías representan cada vez más una ventaja para los regímenes autoritarios, que las usan para sofocar el disenso y sostener sistemas políticos opresivos.
- Estas tecnologías presentan dos desafíos clave: aumentan la legibilidad de la vida pública por parte del Estado y reducen las oportunidades de que la acción no violenta desencadene deserciones entre los leales al régimen.
- Estos desafíos se ven ejemplificados en las formas en las que dos regímenes autoritarios, China y Rusia, han desarrollado herramientas de censura, propaganda y vigilancia usando tecnologías más nuevas.
- Dado que los regímenes autoritarios usan estas tecnologías en cada vez mayor medida, es fundamental que los formuladores de políticas y activistas respondan a los desafíos de mayor legibilidad y menor deserción.

United States Institute of Peace
Making Peace Possible

SPECIAL REPORT

N.º 499 | JULIO DE 2021

ACERCA DEL INFORME

Este informe analiza cómo el uso de las tecnologías más nuevas y emergentes afecta las campañas de acción no violenta. Identifica dos grandes desafíos relacionados y presenta evidencia de esta dinámica en la práctica en dos autocracias digitales: China y Rusia. 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 499. Publicado por primera vez en 2021.

ISBN: 978-1-60127-859-3

UNITED STATES
INSTITUTE OF PEACE PRESS

Personas encienden las linternas de sus teléfonos móviles durante una concentración en favor del líder de la oposición en prisión, Alexéi Navalni, en Moscú, Rusia, el 21 de abril de 2021. (Fotografía de Alexander Zemlianichenko/AP)

Introducción

En 2019, los ciudadanos de Hong Kong salieron a las calles contra una nueva ley que ampliaría la posibilidad de que el Gobierno de China en Pekín extraditara a residentes de Hong Kong y los trasladara al territorio continental de China. Durante los meses siguientes, las protestas se intensificaron para exigir mayor democracia e incluso la secesión de Hong Kong de China. Las protestas atrajeron una participación masiva, y las tácticas creativas de los jóvenes, siguiendo el consejo de la estrella en artes marciales, Bruce Lee, de "ser agua", inspiraron movimientos en todo el mundo.

Los Gobiernos de Hong Kong y Pekín respondieron con una variedad de tácticas, desde gases lacrimógenos y bastones hasta arrestos y disparos masivos. Aun así, quizás la batalla más crítica en la guerra entre los manifestantes en favor de la democracia y el Gobierno continental se libró en línea. Hong Kong ha disfrutado desde siempre de reglas más flexibles en torno a la libertad de expresión, a diferencia de China continental, y está, aparentemente, fuera de la censura del Gran Cortafuegos de Pekín. No obstante, Pekín implementó una serie de herramientas represivas cada vez más sofisticadas, que incluyen cámaras de reconocimiento facial, vigilancia en línea invasiva y una ley de seguridad draconiana para silenciar al movimiento.[1] Los activistas contraatacaron y coordinaron la resistencia a través de sistemas de mensajes cifrados, como Signal y Telegram, y publicaron videos en línea sobre cómo engañar a las cámaras de reconocimiento facial usando láseres y peinados creativos para cubrir los rostros.

A principios de 2021, se produjeron manifestaciones en Rusia después del arresto del líder de la oposición, Alexéi Navalni, en las que los manifestantes hicieron frente a temperaturas bajo cero para expresar su rechazo al presidente Vladímir Putin. Las protestas fueron impulsadas por un video en YouTube publicado por el partido de Navalni, en el que se presentaban pruebas de que Putin se

Residentes de Hong Kong sujetan en alto hojas de papel en blanco en una manifestación el 3 de julio de 2020 en protesta por la prohibición de los lemas por parte del Gobierno. (Fotografía de Lam Yik Fei/New York Times)

había apropiado de manera ilícita de una mansión en el mar Negro. El Gobierno de Rusia arrestó a miles y probablemente intimidó a otros tantos. Sin embargo, también contraatacó en línea con desinformación virtual y un régimen de censura y vigilancia cada vez más agresivo.[2]

Las campañas de acción no violenta como estas, que implican tácticas como protestas, huelgas y boicots para lograr objetivos políticos, son una de las formas más comunes en las que los ciudadanos intentan cambiar de manera pacífica sistemas políticos indiferentes.[3] A menudo, las campañas se libran para aumentar la igualdad, combatir la corrupción y garantizar la buena gobernanza. Son una forma poderosa de transformar la fragilidad política y social, y convertirla en estabilidad a largo plazo, ofreciendo una forma de implementar el cambio sin violencia a las personas descontentas y perjudicadas. Dado que el autoritarismo global está en alza, la capacidad de las personas comunes de ejercer una resistencia no violenta es fundamental para construir un mundo pacífico y democrático.

Aun así, tal como estos estudios de caso dejan en claro, las tecnologías recientemente desarrolladas y emergentes están transformando la naturaleza de las polémicas interacciones entre activistas y Gobiernos autoritarios. Si bien una amplia gama de factores influye en el éxito o el fracaso de los movimientos, el panorama tecnológico adquiere cada vez más relevancia. Los disidentes han usado las redes sociales para movilizar el apoyo y coordinar actividades de resistencia. Aun así, los dictadores también están implementando nuevas tecnologías cada vez con más frecuencia usando la automatización para inundar los foros en línea con desinformación e identificando a los disidentes con algoritmos sofisticados basados en la más reciente inteligencia artificial (IA). Estas interacciones no son aleatorias ni fortuitas, sino que constituyen estrategias coordinadas de Gobiernos autoritarios para preservar su régimen en el entorno cambiante del siglo XXI.

Los Gobiernos democráticos también han empleado muchas de estas tecnologías, y muchas de las tecnologías subyacentes provienen de compañías de tecnología estadounidenses. Aun así, los usos más atroces de tecnología emergente para vigilar y sofocar el disenso proceden directamente de regímenes autoritarios que intentan mantenerse en el poder sin el consentimiento de sus pueblos.[4]

Dos desafíos para la acción no violenta

Las tecnologías emergentes presentan dos desafíos particulares para la acción no violenta. El primero es la mayor legibilidad de la vida social y política a través de la vigilancia digital, que elimina la posibilidad de tener un espacio libre para coordinar acciones colectivas. El segundo es la menor cantidad de oportunidades para que los activistas induzcan deserciones en el régimen, una consecuencia de la represión preventiva más eficaz y la mayor centralización del aparato represivo. Ambos desafíos son centrales para la forma en que funciona la acción no violenta. Ambos se vinculan con la necesidad inmediata de respuestas de políticas que permitan campañas de acción no violenta para contrarrestar de manera eficaz los autoritarismos digitales.

MAYOR LEGIBILIDAD

El primer gran desafío es la forma en que las tecnologías de información y comunicación digitales están cambiando la comunicación interpersonal, la interacción y la movilización por entornos de información que son "legibles" de manera más directa para el Estado, es decir, aquellos a los que puede acceder y que puede interpretar con facilidad.

La movilización de campañas de acción no violenta comúnmente exige "espacios libres" fuera del control estatal, donde la acción y las actitudes puedan coordinarse, y donde se pueda desarrollar una "ideología revolucionaria".[5] Los espacios libres permiten un intercambio sincero de ideas que de otra forma provocarían represión. Este tipo de espacios puede adoptar muchas formas, desde instituciones religiosas como las iglesias del este de Alemania que alentaron protestas por la paz en la década de 1980 hasta asociaciones comerciales, como Bazaaris, que ayudó a organizar la revolución iraní en la década de 1970. Su característica clave es que lo que allí sucede no está sujeto a la supervisión ni control gubernamental.

Los Gobiernos autoritarios, en especial las dictaduras totalitarias, han intentado por mucho tiempo escrudiñar los espacios libres usando redes integrales de informantes y vigilancia, o absorbiendo estructuras independientes de la sociedad civil para incorporarlas a sus coaliciones gubernamentales. Sin embargo, la complejidad de la sociedad moderna hace que el control total de la información sea prácticamente imposible. Incluso en situaciones de represión extrema, "las armas de los débiles" (como burla a quienes están en el poder o que eluden las responsabilidades exigidas por el Gobierno) pueden servir como cimiento para socavar los mitos del autoritarismo y generar una acción colectiva.[6] Los espacios libres permiten un intercambio sincero de ideas que de otra forma provocarían represión. Los regímenes autoritarios incorporan una "falsificación total de las preferencias", en la que las personas, por temor a la represión, ocultan sus verdaderas posturas hacia el Gobierno. No obstante, incluso una cantidad pequeña de disidentes resonantes puede suscitar olas revolucionarias mientras otros observan que la oposición al régimen es más amplia de lo que habían imaginado.[7]

En sus comienzos, la Internet y las redes sociales en particular parecían espacios libres casi ideales. Los activistas y observadores internacionales aclamaban la falta de filtros en Internet, la capacidad de las personas de diversos contextos de comunicarse directamente y las herramientas prácticas que la organización digital proporcionaba a movimientos con pocos recursos.[8] Los beneficios de la tecnología para los movimientos son reales. En la era de la Internet, la movilización de una protesta de millones es viable de una forma inimaginable para las generaciones anteriores.[9] Estas ventajas han transformado al activismo digital en una parte central de las estrategias de muchos movimientos,

> Las tecnologías del siglo XXI han otorgado a los regímenes una enorme ventaja cambiando una proporción cada vez mayor de la vida cívica. . . y convirtiéndola en un mundo de comunicación digital que, por su diseño, es fácilmente legible.

una tendencia que la pandemia de la COVID-19 efectivamente realzó.[10]

Aun así, mientras las redes sociales son una herramienta eficaz para organizar el disenso, los espacios virtuales comunes son un territorio peligroso para los activistas no violentos. Las tecnologías digitales no solo facilitan la comunicación, sino que también hacen que las comunicaciones sean más accesibles y legibles, tanto para las compañías que las producen como para el Estado. Las autocracias digitales pueden censurar de forma directa información en línea que amenace con fomentar la acción colectiva, inundar el discurso en línea con contrarrelatos y desinformación, rastrear los vínculos de redes sociales de usuarios disruptivos para comprender mejor las redes opositoras y espiar las comunicaciones supuestamente privadas de los opositores. Incluso si sus técnicas son algo primitivas, la presencia del régimen en estas plataformas y el conocimiento de los ciudadanos de este tipo de vigilancia pueden alentar la autocensura y sofocar el libre discurso.[11]

Cuando los ciudadanos intentan organizarse a pesar de la vigilancia gubernamental, la tecnología les brinda a los regímenes autoritarios una forma para reprimir preventivamente a la oposición. La vigilancia mejorada por la IA (desde algoritmos para rastrear redes sociales hasta avanzados sistemas de reconocimiento facial) permite que los procesos de movilización antes ininteligibles para el Estado sean cada vez más legibles y previsibles, empoderando así a los autócratas para identificar con rapidez las señales de advertencia de protestas coordinadas e intimidar a los activistas disruptivos. Armados con información de antemano, los regímenes pueden emitir medidas preventivas para evitar la movilización, cerrar lugares problemáticos y bloquear el paso de los disidentes antes de que se produzca una movilización a gran escala. A medida que la represión preventiva se vuelve más eficiente, los regímenes tienen menos necesidad de usar la violencia física para dispersar las protestas. Esto tiene un gran impacto, ya que uno de los principales factores que impulsa la deserción del régimen es la reacción adversa popular ante episodios visibles de represión contra manifestantes no armados.[12] Ante la mayor legibilidad, la represión queda cada vez más fuera de la vista y de la mente.

En pocas palabras, las tecnologías del siglo XXI han representado una gran ventaja para los regímenes alejando una parte cada vez mayor de la vida cívica del mundo complejo, a menudo inescrutable, de la interacción humana personal para acercarlo a un mundo de comunicación digital que, por su diseño, es de fácil acceso. De hecho, en la medida en que la comunicación en línea sustituya la interacción en persona, es posible que incluso impida indirectamente el desarrollo de otros espacios libres en tanto los ciudadanos abandonen actividades del mundo real que, en algún momento, estuvieron fuera del control gubernamental.

REDUCCIÓN DE LA DESERCIÓN EN LOS REGÍMENES

El segundo gran desafío para las campañas de acción no violenta es que las tecnologías emergentes pueden ayudar a los autócratas a prevenir las deserciones de sus regímenes de dos formas. La primera es mejorar la represión preventiva que permite a los regímenes evitar episodios riesgosos de represión violenta a gran escala. La segunda es alejar gran parte de la carga cotidiana de represión de un grupo numeroso de policías y soldados, y dejarla en poder de una pequeña cantidad de especialistas cuya lealtad pueda controlarse y garantizarse mejor, con una baja inclinación a la deserción.

Cuando todo lo demás falla, las autocracias dependen de la represión violenta para mantener el control de su población. La lógica de la acción no violenta reconoce que la capacidad de los autócratas para reprimir requiere la colaboración de complejos y extensos “pilares de apoyo”.[13] Las élites en el poder dependen de un aparato de seguridad (y, en algunos casos, civiles a favor del régimen) para identificar las amenazas y, cuando sea necesario, usar la violencia para disuadirlas.

Esta dependencia implica varios desafíos para los líderes autoritarios. Primero, la represión tiene un gran costo directo. Se debe pagar a policías secretos, se deben comprar y mantener equipos de vigilancia, y se deben movilizar las fuerzas de seguridad. Segundo, la represión genera un peligro significativo para la élite política del Estado en cuanto las instituciones a las que recurre por su capacidad represiva algún día pueden usar esa capacidad para tomar el poder en beneficio propio.[14] Por último, en el contexto de una campaña de acción no violenta, las fuerzas de seguridad pueden eludir sus responsabilidades, negarse a reprimir manifestantes pacíficos, o bien desertar del Estado y apoyar las exigencias de cambio. La deserción es común en campañas de acción no violenta y aumenta significativamente las probabilidades de éxito de la campaña.[15] Las deserciones a menudo comienzan en los niveles más bajos de las fuerzas de seguridad y van ascendiendo. Cuando las principales autoridades de seguridad desertan, esto comúnmente se debe a que temen que sus tropas no cumplan las órdenes de reprimir en nombre del gobernante. Este pilar de apoyo se desvincula entonces del régimen, facilitando así su colapso.

Existen numerosos factores que influyen en las deserciones del sector de seguridad durante las campañas de acción no violenta.[16] Uno de los más fundamentales es cuando se ordena a las fuerzas de seguridad reprimir de formas que consideran excesivas o injustificadas. Por ejemplo, en las protestas de 2020 contra el presidente Alexander Lukashenko en Bielorrusia, muchos agentes de policía se quitaron públicamente el uniforme y se negaron a obedecer las órdenes en rechazo a la demanda del Gobierno de usar la fuerza mortal contra los manifestantes pacíficos. De igual forma, un punto de inflexión en 2010-2011 se produjo en el levantamiento en Túnez cuando el presidente Zine el Abedine Ben Alí llamó a los militares para acallar con violencia la revolución. Los líderes militares se negaron, lo que precipitó la huida de Ben Alí del país.

Un factor relacionado que facilita la deserción implica conexiones personales con las fuerzas de seguridad.[17] Por ejemplo, en la Revolución Naranja de Ucrania de 2004, figuras de la oposición usaron lazos familiares para crear una amplia red de contactos en todos los niveles y acuerdos informales dentro del ejército de Ucrania para que los soldados no usaran la violencia contra los manifestantes pacíficos.[18] En Nepal, la falta de conexiones de este tipo provocó el surgimiento de una rebelión armada.[19]

Las tecnologías emergentes, en especial la inteligencia artificial, obstaculizan estos mecanismos y, de esta forma, reducen las probabilidades de deserción del régimen. En un comienzo, estas tecnologías mejoran la eficiencia de la represión preventiva y permiten que los regímenes mantengan bajo control a su población sin recurrir a episodios de violencia escandalosa que podrían incitar deserciones en las fuerzas de seguridad. La IA ofrece a los Gobiernos autoritarios herramientas informáticas que mejoran considerablemente su capacidad de censurar y vigilar a su población. Tal como los estudios de caso expresan con claridad, esta capacidad permite a los regímenes identificar opositores y sofocar la resistencia antes de que los activistas puedan organizar recursos visuales y llamados dramáticos para generar conciencia y dar lugar a deserciones, ya sea de las fuerzas de seguridad o entre los defensores del régimen de forma más general.[20]

La automatización de la represión permite a los gobernantes colocarla en las manos de una pequeña cantidad de leales al régimen.[21] Dado que hoy los algoritmos automatizados hacen el trabajo diario, un cierto grado de vigilancia, propaganda y censura que antes requería grandes cantidades de personas relativamente menos capacitadas (soldados, policías, informantes y agentes de inteligencia), ahora puedan realizarse con una cantidad menor de personas con un gran nivel de capacitación, responsables de diseñar y supervisar los sistemas automatizados. A su vez, el control de estos administradores, programadores e ingenieros (comúnmente miembros de la élite política y social) es más estricto y sencillo, para garantizar su lealtad. Además, en los niveles más bajos de estos aparatos, la inteligencia artificial posiblemente elimine incluso la posibilidad de la interacción humana o la compasión, al igual que las cámaras de tránsito automatizadas eliminan la interacción humana del cumplimiento de las leyes de tránsito.

China revoluciona la autocracia digital

China está desafiando los límites del autoritarismo digital. Si bien la Internet ha empoderado a la sociedad civil de China de algunas formas, las tecnologías emergentes han empoderado aún más al Partido Comunista de China (PCC), que le permite manipular información, identificar disidentes y prevenir de manera eficaz la movilización masiva. Las mejoras en la censura, la propaganda y la vigilancia han aumentado la legibilidad de la sociedad civil de China por parte del PCC como nunca antes, y así reducen las posibilidades de una movilización contra el régimen o de deserciones significativas.

CENSURA

El régimen de censura de China es el más amplio del mundo. Es bien sabido que, el Gran Cortafuegos bloquea el acceso de los usuarios chinos a muchos sitios web, desde Google y Twitter hasta el *New York Times*. El PCC también aplica un riguroso control de los filtros de Internet, supervisando los medios de comunicación y adueñándose de proveedores de servicios de Internet (ISP en inglés) y de contenido como Sina Weibo (el equivalente a Facebook en China), responsable del contenido en línea. Para evitar acusaciones, estas compañías emplean ejércitos de censores en coordinación con el Departamento de Propaganda del PCC. Las leyes de censura prohíben todo contenido que "difunda rumores, altere el orden social o perjudique la estabilidad social".[22] No obstante, los censores se centran en el contenido que fomente la acción colectiva o que cuestione la legitimidad del PCC.[23]

La censura china está lejos de ser hermética. Los usuarios de Internet pueden eludir el Gran Cortafuegos con una red privada virtual (VPN) y evadir bloqueos automatizados de palabras clave con un simple juego de palabras. Los usuarios de Weibo han hecho millones de publicaciones con críticas a las fallas del Gobierno local.[24] Además, si bien la imposición de Xi Jinping parece estar endureciéndose, las sanciones penales por violaciones del contenido son poco frecuentes, reservadas en gran medida a los opositores de gran perfil mediático, como el premio nobel Liu Xiaobo.[25]

Aun así, la "censura porosa" es eficaz. La mayoría de los usuarios no están dispuestos a invertir el esfuerzo de acceder a contenido censurado: la regulación de las páginas web, la reordenación de los resultados de búsqueda y la limitación de las VPN generan suficiente fricción para desviar sutilmente a los usuarios de contenido prohibido sin desencadenar una acción violenta.[26] Se calcula que solo del 3 % al 15 % de los más de novecientos millones de usuarios de Internet en China hacen uso de una VPN para eludir al Gran Cortafuegos.[27] El resto está satisfecho con permanecer dentro de un ecosistema de Internet chino restringido, pero dinámico.[28] Por lo tanto, los usuarios de Internet de China están en gran medida ciegos ante los peores excesos del PCC. Muchos estudiantes de la universidad de China ni siquiera reconocen las icónicas imágenes de las protestas en la plaza de Tiananmén de 1989.[29]

PROPAGANDA

El PCC también genera su propio contenido, mediante plataformas en línea, para manipular el discurso nacional. Cientos de miles de agentes del PCC, conocidos como "el partido de los 50 centavos" por su apócrifo pago por publicación, desbordan con regularidad las redes sociales con comentarios que elogian el régimen y sus políticas, y generan unos 450 millones de publicaciones al año.[30] Esto ayuda al PCC a enterrar la mala prensa al mismo tiempo que empuja a los ciudadanos de manera discreta hacia contenido favorable relacionado con propaganda más evidente de agencias de noticias tradicionales que, según se entiende en general, son órganos estatales.[31] La propaganda del PCC destaca en especial la restitución judicial por abusos locales, lo que alienta a los ciudadanos a expresar sus reclamos a través de vías institucionales en lugar de en protestas masivas.[32]

Una aplicación en el teléfono móvil de una persona muestra la ubicación de manifestantes y policías en el distrito de Tsim Sha Tsui de Hong Kong el 10 de octubre de 2019. (Fotografía/Kin Cheung/AP)

El partido de los 50 centavos hace uso de relativamente poca tecnología. A los empleados del Gobierno se les pide que generen propaganda a favor del régimen como condición de empleo. Los voluntarios a favor del PCC también pueden colaborar. No obstante, las tecnologías más nuevas y emergentes prometen mejorar la propaganda en línea del partido. Los programas de bots pueden diseminar olas coordinadas si se les ordena, para así distraer a los usuarios de eventos actuales desagradables, como las protestas en Hong Kong o la pandemia de la COVID-19. De igual forma, los avances en la IA probablemente permitirán al PCC identificar tendencias y abusar de algoritmos de contenido en las redes sociales para exhibir con más prominencia contenido a favor del régimen.[33] A medida que estas tecnologías evolucionan, la vigilancia y recopilación masiva de datos en China pueden incluso dar lugar a la personalización individualizada de la propaganda, por ejemplo, mediante el uso de anuncios publicitarios específicos en línea.[34]

VIGILANCIA

Quizás más importante, el PCC ha aprovechado los avances en macrodatos (*Big Data* en inglés) y tecnología de reconocimiento facial para crear un estado de vigilancia integral. Para comenzar, está desarrollando de manera acelerada la capacidad de analizar enormes repositorios de datos de redes sociales en función de asociaciones, preferencias y comportamiento del usuario. Las tendencias en línea pueden usarse para identificar disturbios en el mundo real, lo que facilita la represión preventiva. Por ejemplo, las autoridades del Gobierno en Chengdu respondieron a esfuerzos en línea de organizar manifestaciones los sábados extendiendo de forma preventiva la semana laboral hasta el fin de semana.[35] Un sistema de advertencia de redes sociales también puede automatizarse de manera eficaz, dado que los algoritmos ya buscan de manera constante tendencias que presagien acciones colectivas e indiquen actividad amenazante.

Pekín también usa la vigilancia en línea para identificar a simpatizantes de la oposición. Según la Ley de Ciberseguridad de 2016, los proveedores de Internet tienen la obligación de recopilar información identificativa. Se requiere la identificación para acceder a redes sociales, hacer compras a través de WeChat Pay o usar otras aplicaciones predominantes.[36] Mientras el anonimato virtual llega a su fin, el PCC puede espiar las comunicaciones privadas, rastrear redes virtuales de opositores y vincular con facilidad las críticas en línea con identidades del mundo real. El Gran Cortafuegos también puede rastrear solicitudes de usuarios para obtener acceso a sitios web censurados, otro indicio del sentimiento contra el régimen.[37] A su vez, el régimen puede dirigirse de manera más eficiente a supuestos opositores e "invitarlos a tomar el té" con seguridad, pero se olvida y deja en libertad a los demás ciudadanos.

Durante la última década, Pekín ha ampliado de manera masiva su programa de vigilancia. Instaló cientos de millones de cámaras en un intento por lograr una cobertura total de los espacios públicos.

Además, la vigilancia del PCC sigue a usuarios de Internet en su vida diaria, incluso después de haberse desconectado. El régimen ha dado grandes pasos en relación con la tecnología de reconocimiento facial y desarrolló un sistema de videovigilancia inigualable para identificar y rastrear personas en tiempo real.[38] Durante la última década, Pekín ha ampliado de manera masiva su programa de vigilancia. Instaló cientos de millones de cámaras en un intento por lograr una cobertura total de los espacios públicos.[39] Ahora es común para los ciudadanos ser fotografiados o grabados en áreas públicas, en especial en las ciudades principales. Esta expansión ha aumentado la cantidad de arrestos políticos.[40]

Es difícil sobreestimar las implicancias abusivas del gigante aparato de vigilancia del PCC. Consideremos el trabajo en curso en el sistema de crédito social (SCS) de China, anunciado por primera vez en 2014. Con la supuesta intención de fomentar la confianza social, el SCS asignará a cada ciudadano de China un puntaje de crédito social y recompensará a aquellos que exhiban una conducta "virtuosa" otorgándoles acceso preferencial a bienes públicos y negando estos bienes a ciudadanos con puntajes bajos. La diferencia entre el SCS de China y otros sistemas de crédito es su potencial para incorporar una increíble variedad de datos financieros y personales. Los programas piloto del SCS han ponderado no solo si los ciudadanos pagan sus facturas, sino también qué compran, qué publican en las redes sociales, con quiénes socializan en línea e incluso el tiempo que dedican a jugar videojuegos.[41] Si bien los pilotos del SCS y los datos están fragmentados en este momento en ciudades, regiones y compañías, Pekín tiene la intención de desarrollar un sistema nacional unificado. Además, a medida que el reconocimiento facial se vuelve más generalizado, resulta fácil imaginar la inclusión también de la ubicación u otros datos de comportamiento.

En el horizonte, se vislumbra un mundo en el que China pueda mantener expedientes personalizados que rastreen el lugar al que van sus ciudadanos, qué hacen y qué dicen, tanto en espacios virtuales como físicos, usando la IA, para identificar patrones en estos datos de maneras inimaginables hace algunos años. Muchas personas en China aceptan estos programas piloto del SCS, que el PCC catalogó como un sistema de recompensas por buena conducta.[42] No obstante, el SCS en última instancia otorgará a Pekín una ventaja increíble para castigar a aquellos que considere involucrados en comportamientos subversivos. Tal como destaca el investigador científico Ziao Qiang: "Una vez que funcione plenamente, el SCS (sobre la premisa de una invasión masiva a la privacidad de los ciudadanos a través del control a gran escala) proporcionará al Estado una variedad de mecanismos nuevos mediante los que pueda ejercer el control sobre la población de China".[43]

Por último, Pekín también usa las redes sociales para mejorar el desempeño del Gobierno. Por lo general, las autocracias represivas tienen un problema del agente principal, en el que las autoridades locales irresponsables exageran su desempeño ante élites centrales. Las redes sociales permiten al PCC tercerizar información más precisa sobre reclamos locales y, de esta forma, crear un nuevo mecanismo de responsabilidad.[44] Por este motivo, el PCC tolera vehementes críticas en línea de corrupción a nivel local: las élites del partido pueden usar esa información para sancionar a autoridades locales, atribuirse el mérito por abordar inquietudes locales y, al mismo tiempo, evitar las demandas de un cambio sistémico.[45] Este mecanismo es imperfecto, porque las autoridades locales posiblemente no denuncien las quejas en línea a sus superiores cuando estén ellos implicados de forma directa en la infracción.[46] Aun así, estas quejas por lo general pueden verse en línea, y los reclamos en línea han dado lugar a una responsabilización vertical en numerosos casos. El Partido Comunista también solicita de manera activa la opinión de los ciudadanos a través de diversas plataformas electrónicas del Gobierno, lo que mejora la legitimidad del régimen y amplía la canalización de los ciudadanos hacia formas de desagravio institucional en lugar de movilizaciones masivas que pongan en riesgo al régimen.

IMPLICANCIAS PARA LA ACCIÓN NO VIOLENTA

Tal como otros han observado, la Internet ha transformado el modo en que los ciudadanos de China interactúan con el Estado. Los foros en línea son mucho más críticos que los medios tradicionales, y las campañas virtuales han forzado al PCC a adaptar las políticas en diversas ocasiones prominentes.[47] Durante décadas, las protestas en China han alcanzado las decenas de miles al año en torno a problemas de tributación, toma de tierras y abuso laboral, entre otros.[48] Estos movimientos han mejorado gracias al activismo de Internet, que ha empoderado a la sociedad civil de China para forjar comunidades en línea, expresar reclamos y dirigir la atención nacional a fallas en la gobernanza local.[49]

No obstante, las tecnologías emergentes han ampliado todavía más el poder del PCC. La sociedad civil de China es más legible que nunca. El régimen puede rastrear tendencias en el ciberespacio, espiar conversaciones virtuales en WeChat, manipular narraciones de redes sociales y controlar el comportamiento cotidiano de los ciudadanos. Su capacidad para hacerlo no deja de crecer. Las redes sociales de China se expandieron exponencialmente, pero esta participación cívica dinámica se circunscribe a un espacio virtual con un control estricto. En China, el discurso político en línea pocas veces es libre, mucho menos libre de riesgos.

Además, las oportunidades de provocar deserciones del régimen son limitadas. A medida que el PCC mejora su capacidad para disipar preventivamente la movilización, tiene menos necesidad de represión física de gran repercusión mediática, lo que implica menos posibilidades de movimientos masivos para generar deserciones. Asimismo, la represión es cada vez más automatizada y difícil de desbaratar. La vigilancia virtual en las plataformas de redes sociales es muy eficaz y permite al PCC replicar una operación de inteligencia similar a la Stasi con una fracción de los recursos humanos y una huella pública menos dominante.[50] Una vez establecido, el SCS puede automatizarse y carecer de interacción personal, de modo que los ciudadanos experimenten el castigo por "desviarse" de conductas sin siquiera ver a un agente estatal y sin recurso alguno. El periodista Liu Hu narra desde sus experiencias después de haber sido incluido en una lista negra de personas deshonestas: "No había un archivo, no había una orden policial, no había una notificación oficial previa. Simplemente me privaron de las cosas a las que había tenido derecho en algún momento. Lo que en verdad me atemorizó es que no hay nada que se pueda hacer al respecto. No es posible presentar una denuncia. Estás perdido en el medio de la nada".[51]

En pocas palabras, Pekín se ha adaptado de manera eficaz a la era de la Internet. Mientras que el activismo en línea ha impulsado rebeliones masivas en otras autocracias, China no ha tenido ninguna movilización que ponga en riesgo al régimen desde 1989. Las protestas en el país son reformistas y se dan con exclusividad en torno a inquietudes no ideológicas. La participación cívica y el periodismo de investigación están en alza, pero los usuarios en línea evitan cuestionar al PCC de manera directa.[52] El régimen mantiene un estricto control de los medios y ha encarcelado a numerosos prominentes activistas por los derechos humanos.[53] El efecto paralizador resultante empuja a los ciudadanos chinos con una mente democrática cada vez más a la autocensura.[54] El temor a la censura está expuesto en plenitud en Hong Kong, donde simpatizantes de la oposición expusieron con desesperación su vida virtual de contenido revolucionario en el período posterior a la nueva ley de seguridad.[55] En estas circunstancias, la probabilidad de que una campaña no violenta a gran escala desencadene significativas deserciones del régimen parece escasa.

Aun así, incluso cuando el disenso organizado se ve sofocado, gran parte de la ciudadanía china parece tener menos temor al régimen. Muchos ignoran con dicha el alcance de la represión, disfrutan la vida virtual dentro de las restricciones sutiles del Gran Cortafuegos y valoran la comodidad de una sociedad interconectada bajo el ojo vigilante del PCC.[56] En otras palabras, los autócratas digitales de China lo tienen todo.

Rusia libra una batalla por la información

Al principio, Rusia adoptó un enfoque de total libertad con respecto a la Internet y se vio forzado a reaccionar a la defensiva ante el activismo en línea. El Kremlin carece de la capacidad técnica para emular por completo el kit de herramientas represivas de Pekín. Como contrapartida, Rusia ha desarrollado una enérgica máquina de desinformación en línea y una combinación cada vez más opresiva de restricciones legales, vigilancia y coerción. Si bien resulta eficaz, este sistema no explota por completo el potencial represivo de las tecnologías emergentes. A partir de esto, los desafíos de legibilidad y deserción para la acción no violenta son menos severos que en China. Por lo tanto, mientras China es ejemplo de las fronteras de posibilidad para una autocracia digital de alta capacidad, Rusia ilustra cómo incluso las autocracias de capacidad moderada pueden usar las tecnologías emergentes para frustrar las campañas de acción no violenta.

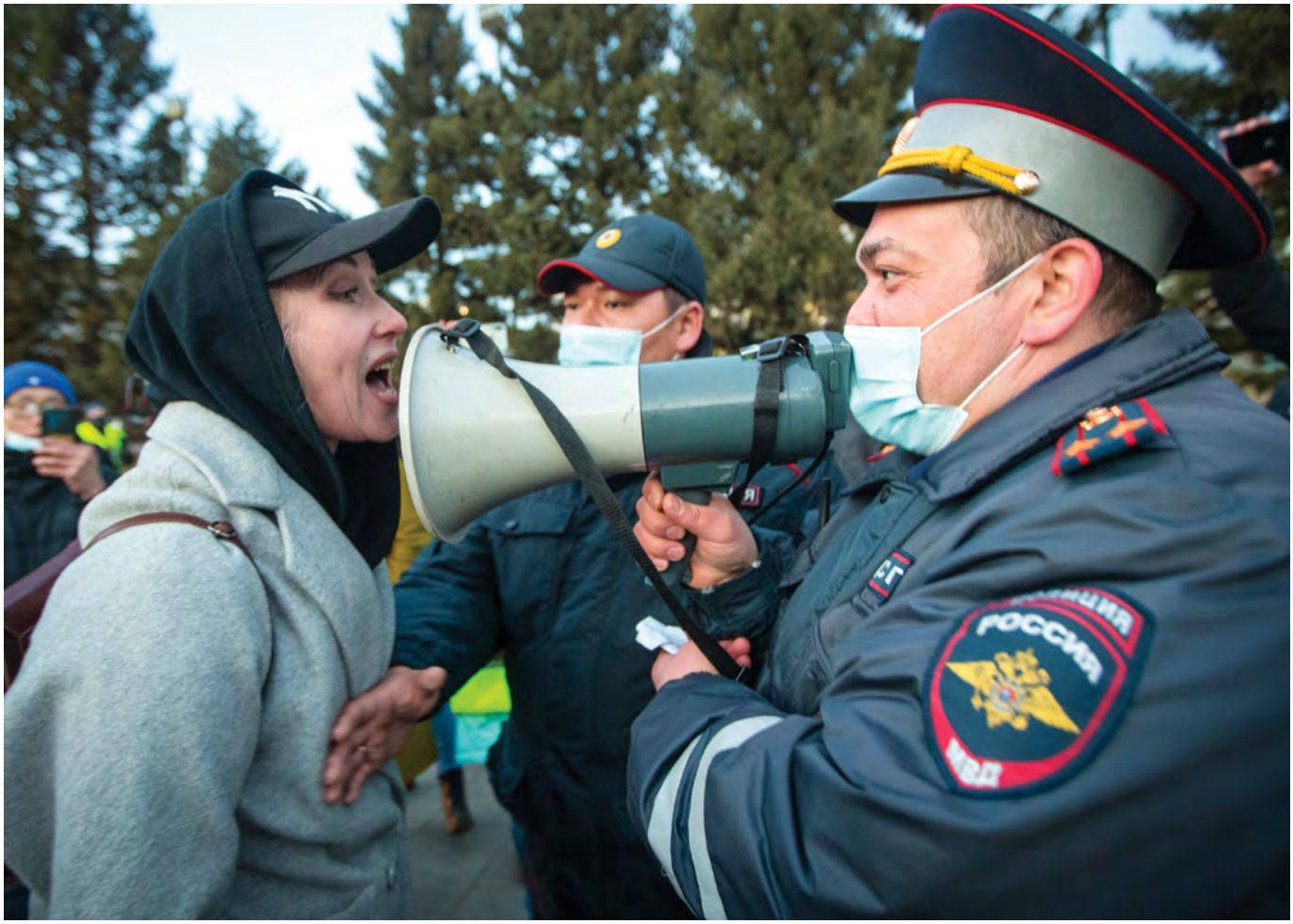
CENSURA

Durante gran parte de su existencia, el ecosistema de Internet de Rusia (RUNET) fue notablemente libre.[57] El presidente Putin restringió las libertades de los medios de comunicación después de su elección en el año 2000, pero dejó sin regular la incipiente Internet, rechazando la censura de estilo chino. En consecuencia, RUNET prosperó: Yandex y VKontakte (VK InContact) desplazaron a Google y Facebook entre los usuarios rusos, quienes cultivaron una biosfera dinámica.[58] Aun así, cuando la penetración de Internet se incrementó, el Kremlin reconsideró su enfoque. El control sobre los medios de comunicación tradicionales no pudo detener la movilización en línea, una realidad interrumpida por las protestas de 2011-2012. Después de regresar a la presidencia en 2012, Putin priorizó tomar el control de RUNET.[59]

Para comenzar, Rusia está creando un régimen de censura cuasi legal respaldado por la coerción del Estado. En 2012, la Duma estableció una lista negra de los denominados sitios web extremistas, a cargo de la agencia de censura Roskomnadzor. Poco después, la Duma otorgó al fiscal general la autoridad para bloquear sitios sin una orden judicial y amplió la lista negra para incluir sitios que publicitan eventos masivos no sancionados. Otras leyes obligan a los productores de contenido popular a registrarse en el Gobierno y los responsabilizan por el contenido del sitio (la Guía Legal del Blogger), además de sancionar a los ISP que no pueden bloquear VPN. A su vez, el Kremlin ha usado este barniz de legalidad para hostigar, intimidar e incluso capturar a los proveedores de contenido. Por ejemplo, el fundador de VK, Pavel Durov, se vio forzado a huir de Rusia en 2014 después de haberse negado a bloquear cuentas de supuestos extremistas asociados con el movimiento de Euromaidán. Durov fue reemplazado por leales al Kremlin y así se garantizó que VK siga flexible ante el Kremlin,[60]

Aun así, la censura de Rusia es tardía y rudimentaria. Mientras que el PCC incorporó la censura a la infraestructura de Internet de China desde sus inicios, veinte años de desarrollo privado sin restricciones entrelazaron íntimamente a RUNET con la Internet global. Por ahora, que Rusia aísle RUNET a través de un cortafuegos nacional sería un desafío prohibitivo. Tal como dijo Artem Kozlyuk, fundador de la ONG de libertades digitales Roskomsvoboda: “Separar a Rusia de la World Wide Web sería como cerrar su espacio aéreo”.[61] Los rusos están acostumbrados al acceso global a la Internet, y bloquear servicios de uso generalizado, como Facebook y Google, probablemente provocaría una reacción adversa.

Asimismo, la censura de Rusia no es sofisticada: prohíbe la dirección IP de un sitio web en lugar de filtrar en función de palabras clave. Esto implica que Roskomnadzor debe identificar de forma manual los sitios para bloquear. Los usuarios a favor del Kremlin pueden ayudar a tercerizar esta información,



Una mujer discute con un agente de policía durante una manifestación en favor del líder de la oposición, Alexéi Navalni, en Ulan-Ude, la capital regional de Buryatia, una región cerca de la frontera con Rusia y Mongolia, el 21 de abril de 2021. (Fotografía de Anna Ogorodnik/AP)

pero es difícil que la censura sea hermética.[62] Además, dado que los sitios web a menudo comparten direcciones IP, los bloqueos de IP pueden provocar daños colaterales, tal como se puede ver a partir del intento fallido de Rusia de bloquear Telegram, que interrumpió muchos servicios en línea.[63] Las compañías internacionales con frecuencia ignoran las exigencias de censura de Rusia y evaden los bloqueos de IP, y los usuarios de Rusia eluden la censura con VPN. En pocas palabras, si bien la censura del PCC es amplia, pero sutil, los esfuerzos del Kremlin son limitados, pero torpes. O bien como un blogger ruso lo expresó: Roskomnadzor está repleto de "monos con granadas".[64]

Habiendo dicho esto, Rusia está mejorando sus capacidades de censura. La ley de Internet soberana de 2019 fuerza a los ISP a instalar equipos que puedan permitir al Kremlin acceder temporalmente a la Internet global del servidor en regiones particulares, sin afectar los dominios nacionales de Rusia.[65] Rusia también está aumentando su agresividad contra las compañías extranjeras y, en estos momentos, regulando Twitter por violaciones de censura.[66] No obstante, la ruta de Rusia hacia la censura total es larga.

DESINFORMACIÓN

Para compensar estas deficiencias, Rusia ha optado por campañas de desinformación. Como sucede en China, el Kremlin paga a grupos de jóvenes a favor del régimen y soborna a bloggers con influencia para que hablen con motivación del régimen, elogien a Putin y difamen a sus oponentes.[67]

> Putin ha usado granjas de bots y trols para "inundar la zona" con desinformación y así contaminar el discurso en línea con conspiraciones y rumores irrelevantes. . . . En algunos días, más de la mitad de las publicaciones en Twitter de Rusia sobre política es generada por bots.

El efecto es desbaratar narraciones de la oposición sobre abusos del régimen, fomentar el cinismo en torno a la participación política y señalar la fortaleza incuestionable del régimen; en resumen, sembrar "distorsión, confusión y desaliento" en el ciberespacio.[68]

Esta estrategia se ha fortalecido gracias a la tecnología automatizada. Putin ha usado granjas de bots y trols para "inundar la zona" con desinformación y así contaminar el discurso en línea con conspiraciones y rumores irrelevantes. Esto genera curiosidad en los usuarios sobre la oposición, quien se ve forzada a hurgar entre la basura antes de encontrar información real sobre el desempeño del Gobierno.[69] En algunos días, más de la mitad de las publicaciones en Twitter de Rusia sobre política es generada por bots.[70] Esta es una estrategia económica, pero eficaz, y le permite al Kremlin enturbiar las aguas sobre la corrupción mientras cataloga a la oposición como una quinta columna patrocinada por Occidente. Los bots también reducen el impacto persuasivo del activismo en línea. Algunos son fáciles de detectar, pero las sofisticadas cuentas de trols no siempre son evidentes, y esto les permite infiltrarse y apropiarse del discurso opositor en línea.[71] La interacción de la oposición con defensores pagos del régimen es, como mínimo, infructífera.

Además, Rusia también ha utilizado la desinformación en línea y las operaciones de trols como un arma potente de política extranjera. Ha impulsado olas específicas de desinformación en varios frentes de políticas extranjeras usando la propaganda virtual para justificar la guerra contra Ucrania y la incorporación de Crimea, y para interferir en gran medida en las elecciones estadounidenses de 2016.[72] Estas campañas de propaganda son menos evidentes que la propaganda en las noticias tradicionales y notablemente sofisticadas.[73]

VIGILANCIA

Por último, Rusia ha explotado las redes sociales para mejorar su vigilancia. Si bien la vigilancia de las telecomunicaciones de Rusia (el sistema SORM) ha estado vigente desde la década de 1990, las tecnologías emergentes mejoran estas herramientas.[74] Las enmiendas de Yarovaya de 2016 exigen que todos los "organizadores de distribución de la información" archiven datos de usuarios durante tres años en los servidores rusos y que otorguen al Servicio Federal de Seguridad (FSB) acceso a estas comunicaciones y a cualquier código de cifrado. En 2017, la Duma legisló que las compañías de redes sociales deben identificar usuarios mediante un número de teléfono celular y prohibió el acceso anónimo a estos servicios a través de VPN. La ley de Internet soberana de 2019 exige a los ISP instalar la tecnología de inspección profunda de paquetes, que permite al FSB vigilar el contenido del tráfico en línea además de los metadatos, y sin el conocimiento o consentimiento del ISP.[75] El efecto combinado de estas leyes es otorgar al Kremlin acceso radical a la comunicación digital en Rusia.

Tal como sucede en China, la vigilancia en línea permite al Kremlin controlar y suprimir el disenso. Las acusaciones de extremismo en línea están aumentando y, en parte, se ven facilitadas por la colaboración de VK con las solicitudes del FSB de datos de usuarios.[76] Aun así, el sistema de vigilancia de Rusia sigue siendo limitado. El Kremlin no tiene la capacidad técnica para procesar la enorme cantidad de datos generados por las nuevas leyes de almacenamiento. Esto lo limita a la vigilancia orientada en lugar de a un control integral, aunque Rusia está trabajando con China para mejorar sus habilidades de procesamiento de datos de IA.[77] Gran parte de la ciudadanía rusa usa aplicaciones de mensajería con cifrado de extremo a extremo, como Telegram, que no son fáciles de vigilar (estas normalmente no están disponibles en China).[78] Los usuarios rusos también pueden eludir los requisitos de identificación de las redes sociales a través de programas de préstamo de tarjetas SIM.[79] También pueden hacerlo a partir del incumplimiento de proveedores de contenido

internacionales, a los que Rusia intenta frenar. Además, aunque Rusia ha invertido en vigilancia con reconocimiento facial en los principales centros de transporte, no puede acercarse a replicar la videovigilancia nacional de China.[80]

IMPLICANCIAS PARA LA ACCIÓN NO VIOLENTA

Las tecnologías más novedosas y emergentes han proporcionado a Rusia beneficios represivos similares a aquellos de China, pero en una menor magnitud. A diferencia de Pekín, el Kremlin no puede explotar en su totalidad el potencial represivo de la Internet; su censura es más porosa y su vigilancia es menos omnisciente. El PCC aprovecha las tecnologías emergentes para analizar cantidades de datos antes incomprensibles, lo que permite que la sociedad china sea cada vez más legible para el aparato represivo. El Kremlin no puede estar a la altura de este sistema, de modo que el activismo en línea sigue siendo un inconveniente. Para contrarrestar, Rusia ha optado por la desinformación reaccionaria, la intimidación y ocasionales asesinatos para interrumpir la coordinación de la oposición, ofuscar la mala prensa y apartar a los opositores.[81] Esto se asemeja a un modo de represión autoritaria más tradicional, con poca tecnología, aunque mejorado por la vigilancia digital. Irónicamente, mientras el régimen de China es, sin dudas, más opresivo, el régimen de Rusia parece ser más sanguinario y violento.

Esta distinción tiene importantes implicancias para la acción no violenta en Rusia. Para ser más precisos, la capacidad de Putin de reprimir la movilización masiva sigue siendo limitada, como lo evidencian las protestas recientes contra el régimen. Las noticias sobre el arresto de Alexéi Navalni y el juicio mediático se compartieron entre millones de espectadores en línea en YouTube, TikTok e Instagram, y el llamado a la acción de Navalni impulsó protestas masivas en todo el país. Roskomnadzor ejerció presión sobre las compañías para que quitaran contenido relacionado, pero el daño ya estaba hecho: los hashtags #FreeNavalny y #23January de TikTok generaron más de doscientos millones de visitas en días sobre el arresto de Navalni, y sus defensores continúan su campaña anticorrupción en línea.[82] Este tipo de contenido tendría extremadamente poca vida en la Internet de China. Por el contrario, Putin solo puede distorsionar la realidad, no borrarla.

A su vez, la incapacidad del Kremlin de evitar la movilización es importante para la posibilidad de deserciones del régimen. El Kremlin sigue dependiendo de la represión física para mantener a los manifestantes bajo control: la policía rusa arrestó a miles de manifestantes en las protestas recientes. Episodios abusivos como este aumentan el riesgo de una reacción adversa, en la que la represión excesiva solo alimenta aún más la indignación. Además, la mano dura expone al aparato de seguridad a una de las más eficaces herramientas de la oposición para alentar las deserciones del régimen: el sufrimiento injustificado en sus propias manos. Los trols anónimos en línea pueden ser inmunes a la persuasión, pero la fraternización de la oposición en persona con las fuerzas de seguridad puede ganar adeptos. De hecho, esto es lo que indica cierta evidencia anecdótica en protestas recientes, incluido un capitán de policía de Moscú que eligió retirarse en lugar de reprimir a manifestante expresando lo siguiente: “Me avergüenza usar este uniforme porque veo que está cubierto de sangre”.[83]

Con seguridad, dichos avances son limitados. Putin sigue siendo popular, la oposición rusa formal es débil y está fragmentada, y el Kremlin aumenta su capacidad para controlar el activismo en línea. Rusia posiblemente no sea un caso probable de una transición democrática exitosa. Aun así, la marca de la autocracia digital de Rusia presenta vulnerabilidades que podrían explotarse a través de un movimiento no violento determinado y disciplinado.

Recomendaciones para formuladores de políticas y activistas

Pocos regímenes han alcanzado el nivel de sofisticación que China e incluso Rusia exhiben en su uso de tecnologías más novedosas y emergentes, y la mayoría carece del dominio técnico y burocrático necesario para explotar en su totalidad los tipos de herramientas descritas aquí.[84] No obstante, muchos otros, como Arabia Saudita e Irán, han usado durante mucho tiempo sus propios aparatos avanzados de censura y filtración.[85] Los regímenes que no tienen estas capacidades están avanzando con rapidez para adquirirlos.[86]

Tanto China como Rusia están acelerando estos movimientos como parte de sus estrategias generales. China proporciona a docenas de países de todo el mundo tecnología de vigilancia mejorada por IA, desde Pakistán y Malasia hasta Argentina y Venezuela. Rusia también exporta su tecnología de vigilancia SORM a los países cercanos.[87] Tampoco los países de Occidente están exentos de la responsabilidad de la propagación del autoritarismo digital. Las empresas de tecnología en Estados Unidos, Israel, Italia y otros países desempeñan un papel importante en crear la infraestructura del Estado autoritario digital.[88] Si las tendencias actuales continúan, la propagación de tecnologías represivas simplemente se acelerará. Al mismo tiempo, los desafíos para la acción no violenta de mayor legibilidad y menor deserción se agravarán.

El debate político sobre la competencia de las grandes potencias por las tecnologías más novedosas y emergentes, en especial la inteligencia artificial, es sólido. El reciente informe final de la Comisión de Seguridad Nacional sobre Inteligencia Artificial documentó una aceleración en la competencia entre China y los Estados Unidos en torno a la IA e hizo hincapié en la importancia de "crear estándares que protejan la privacidad en tecnologías de IA y promover normas democráticas como guía para el uso de la IA".[89] Los hallazgos de este informe refuerzan las trilladas recomendaciones de un mejor control sobre la exportación de tecnologías que facilitan la represión digital, la defensa de una Internet menos sujeta a la vigilancia gubernamental y el desarrollo de estándares globales para promover la IA ética.

Centrarse en los desafíos centrales de legibilidad y deserción sugiere también varias recomendaciones singulares. En relación con la legibilidad, tres tienen especial relevancia:

Los actores externos deben aumentar su apoyo de los espacios libres basados en estructuras institucionales tradicionales. El optimismo en torno de la democratización del impacto de la tecnología emergente dio lugar a una ola de financiación externa de redes imprecisas, a menudo de jóvenes, que dependían en gran medida de las redes sociales. Incluso después de ese optimismo inicial, sigue habiendo una preferencia por apoyar al activismo digital, al igual que una fascinación por el potencial de movilización impulsado por las redes sociales en contextos autoritarios. Existen algunos fundamentos para seguir siendo optimistas ya que, en muchos países, la movilización en línea sigue superando tácticamente incluso las iniciativas especializadas de represión. Aun así, las tendencias tecnológicas no son alentadoras. El desarrollo y la propagación de la IA, junto con el cada vez mayor poder informático, aumentarán la facilidad con la que las herramientas aquí descritas puedan implementarse para suprimir la acción no violenta, incluso en Estados sin la capacidad y experiencia de China. Los donantes estarán acertados en redirigir su atención a las redes de trabajo, recreación y religión diarias que crean capacidad cívica subyacente para futuras movilizaciones, sin depender de un espacio en línea cada vez más legible.

Una bandera china flamea cerca de las cámaras de vigilancia montadas en una farola de la plaza de Tiananmén en Pekín, China, el 15 de marzo de 2019. (Fotografía de Andy Wong/AP)

Los activistas deben crear preventivamente redundancia sin conexión para el activismo en línea. Teniendo en cuenta que la Internet y las redes sociales están tan arraigadas en la vida diaria, los activistas no pueden tan solo abandonar el espacio digital. Aun así, es probable que exagerar el activismo en línea sea una debilidad mayor porque permite que los movimientos sean más legibles para la represión. Muchos movimientos han aprendido esta lección de la peor manera, creando de manera tardía redes fuera de línea menos vulnerables en respuesta a la represión. Por ejemplo, en Etiopía, activistas jóvenes en las protestas de 2015--2016, organizados al principio casi en su totalidad de forma digital, se vieron forzados a adaptarse al control de Internet por parte del Gobierno creando redes en persona en prisión después de arrestos masivos.[90] Los activistas pueden evitar esta desventaja creando redundancia fuera de línea para comunicarse, organizarse y tender redes antes de que se desencadene una crisis. De hecho, este tipo de desarrollo de la sociedad civil es, casi con seguridad, beneficioso para los movimientos, independientemente de las inquietudes sobre el autoritarismo digital.

Tanto los donantes como los activistas deben facilitar la capacitación en seguridad digital avanzada. Como muchos activistas saben muy bien, la seguridad digital es fundamental para garantizar la viabilidad y el éxito del movimiento. Existen numerosos recursos para enseñar los conceptos básicos de la seguridad digital, por ejemplo, cómo usar VPN, cifrado de extremo a extremo y computadoras aisladas.[91] No obstante, la naturaleza tan cambiante de este espacio exige que los

activistas actualicen con frecuencia sus conocimientos sobre la represión mejorada digitalmente y eviten depender de un único programa o serie de recursos. El análisis estratégico periódico del panorama digital y las posibles vulnerabilidades son una parte crítica de cualquier movimiento de acción no violenta del siglo XXI. Los actores externos pueden respaldar estas capacitaciones y pensamiento estratégico apoyando iniciativas que desarrollen recursos de capacitación, ayudando a proporcionar a los movimientos equipos técnicos (a menudo de manera prohibitiva) para incrementar su seguridad y publicitar investigaciones sobre avances en el autoritarismo digital.

En cuanto al menor potencial de deserción, incluimos tres recomendaciones adicionales de importancia.

Los actores externos deben promover la capacitación y el desarrollo profesional en el uso ético de tecnologías más novedosas y emergentes. Muchas de las élites profesionales y técnicas que operan los sistemas subyacentes al autoritarismo digital tienen pocas conexiones con los activistas que defienden el cambio no violento en sus países. Aun así, estas mismas élites a menudo reciben capacitación en democracias y también socializan allí, en especial en los Estados Unidos.[92] Esto permite incluir capacitación ética y crear las clases de redes interpersonales y de sociabilización profesional que puedan generar más dudas en estas élites sobre si participar en la represión digital.

Los activistas deben usar tácticas creativas no violentas para exponer la injusticia de la represión preventiva. Provocar la deserción es todo un desafío cuando la represión preventiva hace menos visible la injusticia de los sistemas opresivos, como sucede en China. Las tácticas que revelan el aparato de represión preventiva vigente y, al mismo tiempo, se burlan con humor de su sinsentido pueden ser útiles.[93] Por ejemplo, en 2013, el Gobierno de China censuró imágenes de patos de goma después de que un blogger publicara una versión retocada con Photoshop de la famosa imagen del hombre del tanque en las protestas en la plaza de Tiananmén de 1989, reemplazando los tanques por patos de goma gigantes. Hace poco, el PCC borró al oso Winnie-the-Pooh de Internet en respuesta a comparaciones sarcásticas entre Pooh y el presidente Xi Jinping. Este tipo de burla ligera puede parecer irrelevante ante el poder del PCC. Sin embargo, tal como lo demuestran muchas campañas pasadas, las acciones humorísticas sutiles que revelan la injusticia y la ridiculez de la represión pueden ser grandes precursores de movilizaciones futuras.[94]

Los activistas deben también crear redes con los científicos e ingenieros que diseñan y mantienen la infraestructura del autoritarismo digital. Los activistas han hecho hincapié durante mucho tiempo en la importancia de crear redes entre activistas y miembros de las fuerzas de seguridad para reducir la represión y facilitar las deserciones.[95] No obstante, dado que la represión de la acción no violenta está arbitrada cada vez más por la tecnología de la información y las comunicaciones digitales, los desertores más importantes serán cada vez con más frecuencia aquellos responsables de ejecutar la infraestructura digital del Estado. Los activistas pueden redireccionar sus esfuerzos en consecuencia, ya que el mismo método minucioso de creación de redes y relaciones que los movimientos han usado para frustrar la represión física puede usarse para frustrar la represión digital.

En este sentido, los activistas en diversos contextos están desarrollando estrategias creativas para responder a los desafíos del autoritarismo digital, usando tecnologías emergentes para promover el cambio social y político. La acción no violenta ha sido una de las fuerzas más potentes del cambio político pacífico y progresivo en las décadas recientes. A medida que cambie la base tecnológica que usan los movimientos de acción no violenta para luchar, las tácticas y estrategias para garantizar el éxito también deberán cambiar si los activistas de base quieren oponerse al autoritarismo en auge y abogar por un mundo mejor de manera pacífica.

Notas

1. Paul Mozur, "In Hong Kong, a Proxy Battle over Internet Freedom Begins", *New York Times*, 7 de junio de 2020, www.nytimes.com/2020/07/07/business/hong-kong-security-law-tech.html.
2. Alexy Gorbachev, "New Generation of Russian Protesters Harnesses Social Media", Voice of America, 4 de febrero de 2021, www.voanews.com/press-freedom/new-generation-russian-protesters-harnesses-social-media.
3. Erica Chenoweth, "The Future of Nonviolent Resistance", *Journal of Democracy* 31, n.º 3 (2020): 69-84.
4. Steven Feldstein, *The Rise of Digital Repression: How Technology Is Reshaping Power, Politics, and Resistance* (Nueva York: Oxford University Press, 2021).
5. Sobre los espacios libres, Sharon Erickson Nepstad, *Nonviolent Struggle: Theories, Strategies, and Dynamics* (Nueva York: Oxford University Press, 2015), 91; sobre ideología revolucionaria, John Foran y Jean-Pierre Reed, "Political Cultures of Opposition: Exploring Idioms, Ideologies, and Revolutionary Agency in the Case of Nicaragua", *Theory and Society* 28, n.º 3 (2002): 1-38.
6. James C. Scott, *Weapons of the Weak: Everyday Forms of Peasant Resistance* (New Haven, CT: Yale University Press, 1985).
7. Timur Kuran, "Now Out of Never: The Element of Surprise in the East European Revolution of 1989", *World Politics* 44, n.º 1 (1991): 7-48.
8. Clay Shirky, *Here Comes Everybody: The Power of Organizing Without Organizations* (Nueva York: Penguin, 2008); Manuel Castells, *Networks of Outrage and Hope: Social Movements in the Internet Age* (Hoboken, NJ: John Wiley & Sons, 2015); Wael Ghonim, *Revolution 2.0: The Power of the People Is Greater Than the People in Power* (Nueva York: Houghton Mifflin Harcourt, 2012).
9. Zeynep Tufekci, *Twitter and Tear Gas: The Power and Fragility of Networked Protest* (New Haven, CT: Yale University Press, 2017).
10. Jonathan Pinckney y Miranda Rivers, "Sickness or Silence: Social Movement Adaptation to COVID-19", *Journal of International Affairs* 73, n.º 2 (2020).
11. Elvin Ong, "Online Repression and Self-Censorship: Evidence from Southeast Asia", *Government and Opposition* 56 (2021): 141-62.
12. Gene Sharp, *The Politics of Nonviolent Action* (Boston, MA: Porter Sargent, 1973).
13. Gene Sharp, *Waging Nonviolent Struggle: 20th Century Practice and 21st Century Potential* (Boston, MA: Porter Sargent, 2005); Robert L. Helvey, *sobre el conflicto no violento estratégico: Thinking About the Fundamentals* (Boston, MA: Albert Einstein Institute, 2004).
14. Milan W. Svolik, *The Politics of Authoritarian Rule* (Nueva York: Cambridge University Press, 2012).
15. Erica Chenoweth y Maria J. Stephan, *Why Civil Resistance Works: The Strategic Logic of Nonviolent Conflict* (New York: Columbia University Press, 2011).
16. Sharon Erickson Nepstad, "Mutiny and Nonviolence in the Arab Spring: Exploring Military Defections and Loyalty in Egypt, Bahrain, and Syria", *Journal of Peace Research* 50, n.º 3 (2013): 337–49; Jaclyn Johnson y Clayton L. Thyne, "Squeaky Wheels and Troop Loyalty: How Domestic Protests Influence Coups d'État, 1951–2005", *Journal of Conflict Resolution* 62, n.º 3 (2018): 597–625; Holger Albrecht y Dorothy Ohl, "Exit, Resistance, Loyalty: Military Behavior During Unrest in Authoritarian Regimes", *Perspectives on Politics* 14, n.º 1 (2016): 38-52.
17. Chenoweth y Stephan, *Why Civil Resistance Works*; Kevin Koehler, Dorothy Ohl y Holger Albrecht, "From Disaffection to Desertion: How Networks Facilitate Military Insubordination in Civil Conflict", *Comparative Politics* 48, n.º 4 (2016): 439-57.
18. Anika Locke Binnendijk e Ivan Marovic, "Power and Persuasion: Nonviolent Strategies to Influence State Security Forces in Serbia (2000) and Ukraine (2004)", *Communist and Post-Communist Studies* 39, n.º 3 (2006): 419.
19. Ches Thurber, "Social Ties and the Strategy of Civil Resistance", *International Studies Quarterly* 63, n.º 4 (2019): 974-86.
20. Feldstein, *Rise of Digital Repression*.
21. Andrea Kendall-Taylor, Erica Frantz y Joseph Wright, "The Digital Dictators: How Technology Strengthens Autocracy", *Foreign Affairs*, marzo/abril de 2020, www.foreignaffairs.com/articles/china/2020-02-06/digital-dictators.
22. Xiaoyan Chen y Pen Hwa Ang, "The Internet Police in China: Regulation, Scope and Myths", en *Online Society in China: Creating, Celebrating, and Instrumentalising the Online Carnival*, ed. David Kurt Herold y Peter Marolt (Nueva York: Routledge, 2011), 45.
23. Gary King, Jennifer Pan y Margaret E. Roberts, "How Censorship in China Allows Government Criticism but Silences Collective Expression", *American Political Science Review* 107, n.º 2 (2013): 326-43.
24. Jonathan Sullivan, "China's Weibo: Is Faster Different?", *New Media & Society* 16, n.º 1 (2014): 24–37; Bei Qin, David Strömberg y Yanhui Wu, "Why Does China Allow Freer Social Media? Protests versus Surveillance and Propaganda", *Journal of Economic Perspectives* 31, n.º 1 (2017): 117-40.

25. Elizabeth C. Economy, "The Great Firewall of China: Xi Jinping's Internet Shutdown", *The Guardian*, 29 de junio de 2018, www.theguardian.com/news/2018/jun/29/the-great-firewall-of-china-xi-jinpings-internet-shutdown; Freedom House, "China: Freedom on the Net 2020 Country Report", Freedom House, www.freedomhouse.org/country/china/freedom-net/2020; Qin, Strömberg y Wu, "Why Does China Allow Freer Social Media?".
26. Margaret E. Roberts, *Censored: Distraction and Diversion Inside China's Great Firewall* (Princeton, NJ: Princeton University Press, 2018).
27. William R. Hobbs y Margaret E. Roberts, "How Sudden Censorship Can Increase Access to Information", *American Political Science Review* 112, n.º 3 (2018): 621–36; Yuyu Chen y David Y. Yang, "The Impact of Media Censorship: 1984 or Brave New World?", *American Economic Review* 109, n.º 6 (2019): 2294-2332.
28. Margaret Roberts también observa que, al permitir cierto uso de VPN, el PCC crea una bifurcación entre las élites que operan más allá de la censura y las masas que viven dentro de ella. De esta forma, el PCC "fomenta una brecha entre la élite y las masas", evitando vínculos de centro-periferia que puedan generar acciones colectivas que pongan en riesgo el régimen (*Censored*, 8).
29. Rebecca MacKinnon, "China's 'Networked Authoritarianism'", *Journal of Democracy* 22, n.º 2 (2011): 32–46.
30. Gary King, Jennifer Pan y Margaret E. Roberts, "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument", *American Political Science Review* 111, n.º 3 (2017): 484-501.
31. Rongbin Han, "Manufacturing Consent in Cyberspace: China's 'Fifty-Cent Army'", *Journal of Current Chinese Affairs* 44, n.º 2 (2015): 105-34.
32. Daniela Stockmann y Mary E. Gallagher, "Remote Control: How the Media Sustain Authoritarian Rule in China", *Comparative Political Studies* 44, n.º 4 (2011): 436-67.
33. Steven Feldstein, "The Road to Digital Unfreedom: How Artificial Intelligence Is Reshaping Repression", *Journal of Democracy* 30, n.º 1 (2019): 40-52.
34. Roberts, *Censored*.
35. Qin, Strömberg y Wu, "Why Does China Allow Freer Social Media?".
36. Paul Triolo y Samm Sacks, "Shrinking Anonymity in Chinese Cyberspace", Centro de Estudios Estratégicos e Internacionales, 26 de septiembre de 2017, www.csis.org/analysis/shrinking-anonymity-chinese-cyberspace.
37. Roberts, *Censored*, 109–10.
38. Joyce Liu y Xiqing Wang, "In Your Face: China's All-Seeing State", BBC News, 2017, www.bbc.com/news/av/world-asia-china-42248056.
39. Josh Chin y Clément Bürge, "Twelve Days in Xinjiang: How China's Surveillance State Overwhelms Daily Life", *Wall Street Journal*, 9 de diciembre de 2017, www.wsj.com/articles/twelve-days-in-xinjiang-how-chinas-surveillance-state-overwhelms-daily-life-1513700355; Xiao Qiang, "The Road to Digital Unfreedom: President Xi's Surveillance State", *Journal of Democracy* 30, n.º 1 (2019): 53-67.
40. Xu Xu, "To Repress or To Co-Opt? Authoritarian Control in the Age of Digital Surveillance", *American Journal of Political Science* 65, n.º 2 (2020): 309-25.
41. Triolo y Sacks, "Shrinking Anonymity in Chinese Cyberspace"; Qiang, "Road to Digital Unfreedom: President Xi's Surveillance State"; Kendall-Taylor, Frantz y Wright, "Digital Dictators".
42. Genia Kostka, "China's Social Credit Systems and Public Opinion: Explaining High Levels of Approval", *New Media & Society* 21, n.º 7 (2019): 1565-93.
43. Qiang, "Road to Digital Unfreedom: President Xi's Surveillance State", 60.
44. Seva Gunitsky, "Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability", *Perspectives on Politics* 13, n.º 1 (2015): 42-54.
45. Xiao Qiang, "The Battle for the Chinese Internet", *Journal of Democracy* 22, n.º 2 (2011): 47–61; Peter Lorentzen, "China's Strategic Censorship", *American Journal of Political Science* 58, n.º 2 (2014): 402–14; Nele Noesselt, "Microblogs and the Adaptation of the Chinese Party-State's Governance Strategy", *Governance* 27, n.º 3 (2014): 449–68; Sullivan, "China's Weibo".
46. Jennifer Pan y Kaiping Chen, "Concealing Corruption: How Chinese Officials Distort Upward Reporting of Online Grievances", *American Political Science Review* 112, n.º 3 (agosto de 2018): 602-20.
47. Ashley Esarey y Xiao Qiang, "Digital Communication and Political Change in China", *International Journal of Communication* 5 (2011): 298-319.
48. Teresa Wright, "Protest as Participation: China's Local Protest Movements", *World Politics Review*, 6 de abril de 2013, www worldpoliticsreview.com/articles/12877/protest-as-participation-chinas-local-protest-movements; Teresa Wright, *Handbook of Protest and Resistance in China* (Northampton, MA: Edward Elgar, 2019).
49. Guobin Yang, *The Power of the Internet in China: Citizen Activism Online* (Nueva York: Columbia University Press, 2009).
50. Como pregona Ronald Deibert: "¿Por qué un Gobierno se molestaría en construir su propia máquina de vigilancia cuando el sector privado ya le proporciona una?". "The Road to Digital Unfreedom: Three Painful Truths About Social Media", Journal of

Democracy 30, n.º 1 (enero de 2019): 35.

51. Nicole Kobie, "The Complicated Truth About China's Social Credit System", *Wired UK*, julio de 2019, www.wired.co.uk/article/china-social-credit-system-explained.
52. Qiang, "Battle for the Chinese Internet"; Lorentzen, "China's Strategic Censorship".
53. Human Rights Watch, "World Report 2021: Rights Trends in China", enero de 2021, www.hrw.org/world-report/2021/country-chapters/china-and-tibet.
54. MacKinnon, "China's 'Networked Authoritarianism'"; Darrel Robinson y Marcus Tannenberg, "Self-Censorship of Regime Support in Authoritarian States: Evidence from List Experiments in China", *Research & Politics* 6, n.º 3 (1 de julio de 2019); Freedom House, "China: Freedom on the Net 2020 Country Report".
55. Sarah Wu Zhou Joyce, "Editing History: Hong Kong Publishers Self-Censor Under New Security Law", Reuters, 14 de julio de 2020, www.reuters.com/article/us-hongkong-security-publishers-idUSKCN24F09P.
56. MacKinnon, "China's 'Networked Authoritarianism'", 33.
57. Ronald J. Deibert *et al.*, editores, *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace* (Cambridge, MA: MIT Press, 2010); Karina Alexanyan et al., "Exploring Russian Cyberspace: Digitally-Mediated Collective Action and the Networked Public Sphere", Publicación de investigación n.º 2012-2, Berkman Klein Center for Internet & Society, Harvard University, marzo de 2012, https://cyber.harvard.edu/publications/2012/exploring_russian_cyberspace; Sergey Sanovich, Denis Stukal y Joshua A. Tucker, "Turning the Virtual Tables: Government Strategies for Addressing Online Opposition with an Application to Russia", *Comparative Politics* 50, n.º 3 (2018): 435-54.
58. Sanovich, Stukal y Tucker, "Turning the Virtual Tables", apéndice.
59. Andrei Soldatov e Irina Borogan, *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries*, edición reimpresa (Nueva York: PublicAffairs, 2015).
60. Human Rights Watch, "Online and On All Fronts: Russia's Assault on Freedom of Expression", 18 de julio de 2017, www.hrw.org/report/2017/07/18/online-and-all-fronts/russias-assault-freedom-expression; Sanovich, Stukal y Tucker, "Turning the Virtual Tables"; Human Rights Watch, "Russia: Growing Internet Isolation, Control, Censorship", 18 de junio de 2020, www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship.
61. Jan Lindenau, "Russia's Sovereign Internet Law Comes into Force", *Moscow Times*, 1 de noviembre de 2019, www.themoscowtimes.com/2019/11/01/russias-sovereign-internet-law-comes-into-force-a68002. Consulte también Anton Troianovski, "China Censors the Internet. So Why Doesn't Russia?", *New York Times*, 21 de febrero de 2021, www.nytimes.com/2021/02/21/world/europe/russia-internet-censorship.html.
62. Soldatov y Borogan, *Red Web*, 195–205.
63. Alina Polyakova y Chris Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models" (Washington, DC: Brookings Institution, agosto de 2019); Human Rights Watch, "Russia: Growing Internet Isolation, Control, Censorship".
64. *Moscow Times*, "Twitter, Facebook Blacklisted in Russia's Telegram Ban", 27 de abril de 2018, www.themoscowtimes.com/2018/04/27/twitter-facebook-blacklisted-in-russias-telegram-ban-a61281.
65. Polyakova y Meserole, "Exporting Digital Authoritarianism"; Kendall-Taylor, Frantz y Wright, "Digital Dictators"; Human Rights Watch, "Russia: Growing Internet Isolation, Control, Censorship".
66. Grigory Levchenko, "Slow Down, Twitter Roskomnadzor Throttles Twitter over Failure to Remove 'Illegal Content'", Meduza, 10 de marzo de 2021, www.meduza.io/en/feature/2021/03/10/slow-down-twitter.
67. Miriam Elder, "Hacked Emails Allege Russian Youth Group Nashi Paying Bloggers", *The Guardian*, 7 de febrero de 2012, www.theguardian.com/world/2012/feb/07/hacked-emails-nashi-putin-bloggers; Adrian Chen, "The Agency", *New York Times*, 2 de junio de 2015, www.nytimes.com/2015/06/07/magazine/the-agency.html; Gunitsky, "Corrupting the Cyber-Commons".
68. Sanovich, Stukal y Tucker, "Turning the Virtual Tables". Consulte también Peter Pomerantsev, "The Kremlin's Information War", *Journal of Democracy* 26, n.º 4 (2015): 40–50; Kendall-Taylor, Frantz y Wright, "Digital Dictators".
69. Denis Stukal *et al.*, "For Whom the Bot Tolls: A Neural Networks Approach to Measuring Political Orientation of Twitter Bots in Russia", *SAGE Open* 9, n.º 2 (2019); Denis Stukal *et al.*, "Bots for Autocrats: How Pro-Government Bots Fight Opposition in Russia" (documento de trabajo, University of Sydney, 2019), www.denisstukal.com/uploads/8/4/7/0/84708866/stukal_et_al__2020__bots_for_autocrats.pdf.
70. Denis Stukal *et al.*, "Detecting Bots on Russian Political Twitter", *Big Data* 5, n.º 4 (2017): 310-24.
71. Anton Sobolev, "How Pro-Government 'Trolls' Influence Online Conversation in Russia" (informe presentado en NYU Jordan Center for the Advanced Study of Russia, Nueva York, 12 de febrero de 2021).
72. Sobre Crimea, Soldatov y Borogan, *Red Web*, 278–85. Sobre los Estados Unidos, Chen, "The Agency"; el Comité Selecto del

Senado sobre Inteligencia de los EE. UU., "Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Vol. 2", Informe 116–290 (Washington, DC: Oficina de Publicaciones del Gobierno, 2020), www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

73. Todd C. Helmus *et al.*, *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe* (Santa Mónica, CA: RAND Corporation, 2018), www.rand.org/pubs/research_reports/RR2237.html.
74. Deibert *et al.*, *Access Controlled*; Andrei Soldatov e Irina Borogan, "Putin Trolls Facebook: Privacy and Moscow's New Data Laws", *Foreign Affairs,* 3 de noviembre de 2015, www.foreignaffairs.com/articles/russian-federation/2015-11-03/putin-trolls-facebook.
75. Soldatov y Borogan, *Red Web*, 216–20; Polyakova y Meserole, "Exporting Digital Authoritarianism"; Human Rights Watch, "Russia: Growing Internet Isolation, Control, Censorship".
76. Human Rights Watch, "Online and On All Fronts".
77. Andrei Soldatov e Irina Borogan, "Putin Brings China's Great Firewall to Russia in Cybersecurity Pact", *The Guardian*, 29 de noviembre de 2016, www.theguardian.com/world/2016/nov/29/putin-china-internet-great-firewall-russia-cybersecurity-pact.
78. Human Rights Watch, "Online and On All Fronts".
79. Si bien la información de identificación directa se requiere en teoría para adquirir los números de teléfono celular usados para la verificación de redes sociales, en la práctica, este requisito puede eludirse.
80. Polyakova y Meserole, "Exporting Digital Authoritarianism".
81. Valentin Weber, "Why China's Internet Censorship Model Will Prevail Over Russia's", Consejo de Relaciones Exteriores, 12 de diciembre de 2017, www.cfr.org/blog/why-chinas-internet-censorship-model-will-prevail-over-russias.
82. Anton Troianovski *et al.*, "Russia Protesters Defy Vast Police Operation as Signs of Kremlin Anxiety Mount", *New York Times*, 31 de enero de 2021, www.nytimes.com/2021/01/31/world/europe/russia-protests-navalny-live-updates.html; Kat Lonsdorf, "Social Media Fueled Russian Protests Despite Government Attempts to Censor", NPR, 24 de enero de 2021, www.npr.org/2021/01/24/960113653/social-media-fueled-russian-protests-despite-government-attempts-to-censor.`
83. Joshua Yaffa, "The Russians Protesting Putin in Their Personal Lives", *New Yorker*, 4 de marzo de 2021, www.newyorker.com/news/a-reporter-at-large/the-russians-protesting-putin-in-their-personal-lives.
84. Feldstein, *Rise of Digital Repression*.
85. Freedom House, "Iran: Freedom on the Net 2019 Country Report", www.freedomhouse.org/country/iran/freedom-net/2019; Freedom House, "Saudi Arabia: Freedom on the Net 2019 Country Report", www.freedomhouse.org/country/saudi-arabia/freedom-net/2019.
86. Adrian Shahbaz, "The Rise of Digital Authoritarianism", Freedom House, 2018, www.freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism; Feldstein, *Rise of Digital Repression*.
87. Steven Feldstein, "The Global Expansion of AI Surveillance", Carnegie Endowment for International Peace, septiembre de 2019, https://carnegie endowment.org/files/WP-Feldstein-AISurveillance_final1.pdf; Polyakova y Meserole, "Exporting Digital Authoritarianism".
88. Feldstein, "Global Expansion of AI Surveillance". Para leer un ejemplo específico, consulte Bill Marczak *et al.*, "Champing at the Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware", Informe de investigación n.º 102, The Citizen Lab, University of Toronto, 6 de diciembre de 2017, www.citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware.
89. *Informe final de la Comisión de Seguridad Nacional sobre Inteligencia Artificial* (Washington, DC: Comisión de Seguridad Nacional sobre Inteligencia Artificial, 2021), https://reports.nscai.gov/final-report/table-of-contents.
90. Feldstein, *Rise of Digital Repression*, 201.
91. Consulte los recursos como "Surveillance Self-Defense", Electronic Frontier Foundation (www.ssd.eff.org) o "Security-in-a-Box", Front Line Defenders (www.securityinabox.org/en).
92. China y Rusia aumentan su capacidad nacional al respecto, pero los programas estadounidenses de las élites siguen superándolos significativamente. Prashant Loyalka *et al.*, "Computer Science Skills across China, India, Russia, and the United States", *PNAS* 116, n.º 14 (2019): 6732-36.
93. Majken Jul Sorensen, "Humor as a Serious Strategy of Nonviolent Resistance to Oppression", *Peace & Change* 33, n.º 2 (2008): 167-90.
94. Srdja Popovic, *Blueprint for Revolution: How to Use Rice Pudding, Lego Men, and Other Nonviolent Techniques to Galvanize Communities, Overthrow Dictators, or Simply Change the World* (Nueva York: Spiegel y Grau, 2015).
95. Binnendijk y Marovic, "Power and Persuasion".

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

Miembros de derecho

IMPRENTA DEL INSTITUTO DE PAZ DE LOS ESTADOS UNIDOS

Desde su creación en 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. Todos nuestros libros e informes surgen de la investigación y el trabajo de campo patrocinados por los numerosos programas del Instituto, y estamos comprometidos a extender el alcance del trabajo del Instituto a través de la publicación de documentos significativos y sostenibles para profesionales, intelectuales, diplomáticos y estudiantes. Cada obra se somete a una rigurosa revisión por pares llevada a cabo por expertos en la materia externos para garantizar que la investigación y las conclusiones sean equilibradas, relevantes y estén fundamentadas.

OTRAS PUBLICACIONES DE USIP

- *Processes of Reintegrating Central Asian Returnees from Syria and Iraq* por William B. Farrell, Rustam Burnashev, Rustam Azizi y Bakhtiyar Babadjanov (Special Report, julio de 2021).
- *Democracy in Afghanistan: Amid and Beyond Conflict* de Anna Larson (Special Report, julio de 2021).
- *Nonviolent Action and Transitions to Democracy: The Impact of Inclusive Dialogue and Negotiation* por Véronique Dudouet y Jonathan Pinckney (Peaceworks, julio de 2021).
- *National Dialogues in Peacebuilding and Transitions: Creativity and Adaptive Thinking* editado por Elizabeth Murray y Susan Stigant (Peaceworks, junio de 2021).
- *Nigeria's State Peacebuilding Institutions: Early Success and Continuing Challenges* por Darren Kew (Special Report, junio de 2021).

UNITED STATES
INSTITUTE OF PEACE PRESS

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