GEOPOLÍTICA, REDES SOCIALES Y LA ELECCIÓN EN MÉXICO

[ARTURO SARUKHÁN]

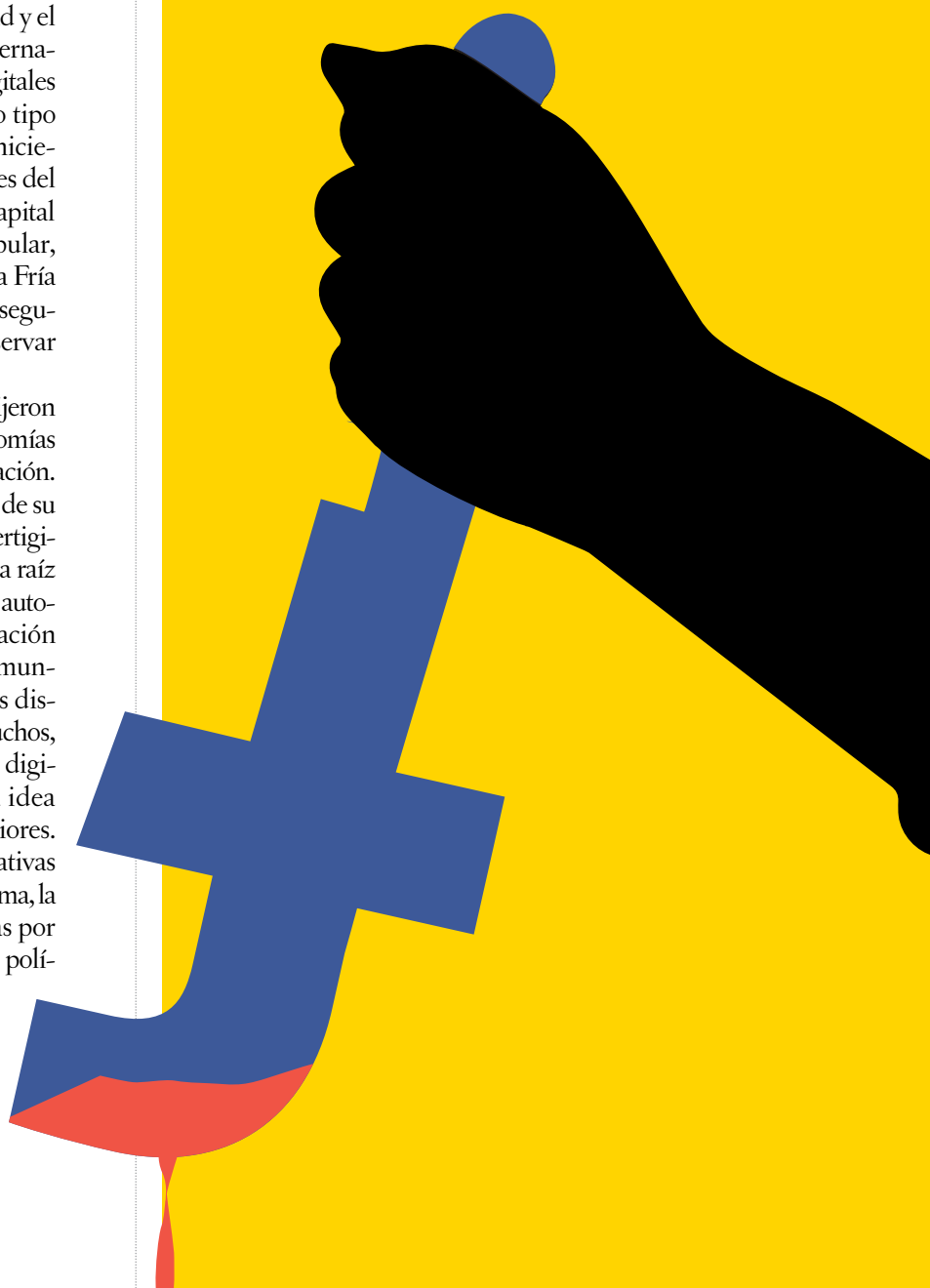
Un reto crucial este año para el sistema internacional –y para México y sus comicios en julio– es la disrupción digital en la política y la geopolítica, un fenómeno que hace a la narrativa más importante que los hechos, que las personas descalifiquen más de lo que debaten y que los algoritmos determinen nuestra visión del mundo. El internet no fue concebido como una infraestructura global de la cual dependieran todas las sociedades. Que una tecnología diseñada en los años setenta haya funcionado tan bien y hoy le dé soporte a cerca de dos mil millones de usuarios es un hito. Pero esa conectividad abre vulnerabilidades, pues en la simpleza de su objetivo –enlazar– radica también su amenaza: cualquiera con acceso a estas redes puede usarlas para infligir daño. Propicia, además, un efecto que es a la vez transformativo y disruptivo, y que presagia trastornos profundos para la manera en que instrumentamos políticas públicas y garantizamos la seguridad, el bienestar y nuestros derechos individuales y colectivos.

La gran paradoja es que, a lo largo de la historia, las sociedades han sido exitosas en función de sus interconexiones humanas; una de las tensiones seminales del sistema internacional del siglo XXI se da precisamente entre sociedades abiertas y sociedades cerradas. La fase de globalización que hoy vivimos está definida más por la divergencia que por la convergencia: estamos interconectados pero no unidos. Lo que más nos vincula, el internet, se ha convertido en el principal campo

> El internet y las redes sociales son el nuevo campo de batalla geopolítica. Estados como Rusia usan tecnologías digitales para polarizar la opinión, sembrar confusión entre los ciudadanos y minar su confianza en las elecciones y la democracia. México no está exento de estas amenazas.

de batalla –tanto de las ideas como de la seguridad y el poder militar y económico– de las relaciones internacionales de este siglo, y las nuevas tecnologías digitales están siendo usadas como armas para un nuevo tipo de enfrentamiento. Desde que las fronteras se hicieron más porosas a la información, a las actividades del crimen organizado trasnacional, a los flujos de capital y de datos o a las interacciones de la cultura popular, el tipo de globalización que nos heredó la Guerra Fría ha hecho más complejo el trabajo del Estado. La seguridad nacional es hoy mucho más difícil de preservar que hace tres décadas.

Con el "deshielo bipolar", varios analistas predijeron que la expansión de instituciones globales y economías regionales "eliminaría" la necesidad del Estado-nación. Eso, como es evidente, no ocurrió, pero la merma de su poder e influencia sí caminó de la mano con la vertiginosa integración del dinero, las ideas y la cultura a raíz de la posguerra fría, erosionando así su autoridad y autonomía. Las consecuencias de esa hiperglobalización se intensificaron después de la crisis financiera mundial de 2008, provocando movimientos políticos disruptivos tanto de izquierda como de derecha. Muchos, en especial aquellos ciudadanos interconectados digitalmente, están menos comprometidos con la idea de un Estado-nación que las generaciones anteriores. Buscan, en cambio, identidades comunes alternativas –animados ya sea por la cultura, la fe, la etnia, el idioma, la clase social o la orientación sexual–. Potenciadas por las redes sociales, las fisuras que han generado las políticas de identidad están ejerciendo una nueva presión sobre el Estado. La combinación de esta disrupción digital, vía redes sociales, y el empoderamiento del individuo –la creación del *homo digitalis*– está en el corazón de una de las tensiones seminales de este



siglo, entre Estado y ciudadano. Los Estados-nación –que, por lo regular, tienen sistemas burocráticos torpes y reflejos lentos, son adversos a tomar riesgos y ahora están faltos de credibilidad social– han tardado en adaptarse a los retos internos y externos que todo esto conlleva.

Este nuevo desorden global digital tiene tres características. Es asimétrico: la conectividad, las plataformas y las redes digitales nivelan el terreno de juego, de modo que los actores no estatales –o incluso naciones menos poderosas– pueden minar la seguridad de las potencias, la de sus aparatos burocráticos y su infraestructura vital. Es vulnerable: entre más conexiones existen, hay más puntos de acceso para ciberataques o ciberespionaje, y cualquier Estado, organización, corporación o persona es actor o blanco de estas actividades. No está regulado: hay una ausencia real de medidas diplomáticas o de mitigación de riesgo eficaces. Y los gobiernos no están estructurados para responder de manera ágil y flexible al cambio. En este momento es prácticamente imposible contener, por su rango y origen, las amenazas digitales y, mientras se construyen formas más eficaces de protección (mediante acuerdos internacionales), los gobiernos, el sector privado y la sociedad tendrán que encontrar mecanismos que nos blinden del abanico de las amenazas cibernéticas, pero que al mismo tiempo preserven la fluidez, la libertad y la independencia en las redes.

A su vez, la demanda de soluciones para problemas trasnacionales sigue en aumento, pero no hay paradigmas que puedan darnos claridad estratégica para confrontar todos los retos o que, al menos, propicien la unidad alrededor de un mismo propósito. El sistema internacional se había tardado en reaccionar: ya en 2010 se perfilaban problemas inconmensurables, cuando ese mismo año hubo un ataque a Google que penetró su seguridad, WikiLeaks publicó miles de archivos gubernamentales filtrados y Estados Unidos e Israel crearon un virus (Stuxnet) para detener el avance del programa nuclear bélico iraní.

DE TUCÍDIDES A TWITTER

Las relaciones internacionales se han transformado de manera radical en el último lustro, como resultado de tres tendencias en particular: i) el desarrollo de tecnologías de información y comunicación, ii) el papel de actores ajenos al Estado y la emergencia de una nueva agenda de seguridad internacional ante una fluidez cada vez mayor y, iii) el surgimiento de potencias que retan al *statu quo* de la posguerra fría y la explosión de nuevos actores que inciden en la seguridad y las relaciones internacionales. Las tres están relacionadas y se retroalimentan entre sí, lo cual explica que las redes sociales ya se usen como arma y que el internet sea uno de los principales teatros de batalla y cálculo geopolítico. Hoy existen 3.4 mil millones de usuarios de internet, se emiten cerca de quinientos millones de tuits diarios y cada segundo se sube el equivalente a siete horas de video a YouTube. Con 1.7 mil millones de usuarios, Facebook podría ser el país más grande del mundo. El 62% de las personas en Estados Unidos obtiene sus noticias de las redes sociales. Y eso que no estamos en la cresta de la ola; casi la mitad de la población adulta del mundo todavía no está en línea. Pero las redes sociales ya revolucionaron nuestras vidas, desde comprar un producto hasta encontrar una pareja, redefiniendo así los mecanismos de interacción social. Las redes, es cierto, son un espejo que refleja todo tipo de intereses y tendencias humanas; por ello, abarcan de manera ineluctable al poder. No sorprende que las plataformas digitales estén cambiando la manera de hacer política y el modo en que se relacionan las naciones y los actores no estatales. Si en el siglo XIX Carl von Clausewitz concebía la guerra como la continuación de la política por otros medios, no nos debe extrañar que, en el sistema internacional de hoy, las redes sociales se estén erigiendo en la continuación de la guerra por otros medios.

En el corazón de estos cambios en las relaciones internacionales contemporáneas hay un cariz adicional: la línea divisoria entre la guerra y la paz se ha desdibujado. Pocas facetas del sistema internacional de este siglo apuntan tanto a este cambio como lo hace el papel que juegan las redes sociales y el internet en la teoría del conflicto (y en cómo lo hemos entendido y abordado) y en la caja de herramientas de poder con la que el Estado y los actores no estatales cuentan para conseguir sus objetivos.

La noción de que las redes sociales podían ser usadas para detonar transformaciones políticas arrancó con las elecciones de 2009 en Moldavia y adquirió fuerza durante la Primavera Árabe de 2011. El común denominador de esa lectura era que los gobiernos autoritarios o cerrados estaban amenazados por el poder del individuo y de los colectivos sociales que empleaban herramientas de las sociedades abiertas, como el internet. Sin embargo, rápidamente se desató una opinión a contracorriente. Como apuntó poco después el sociólogo canadiense Malcolm Gladwell, pronto fue evidente que la revolución no podría ser tuiteada. A cinco años de convulsión en el norte de África y Medio Oriente, hoy Egipto es gobernado por el ejército, Arabia Saudita bombardea a los rebeldes hutíes en Yemen y la oposición siria fue aplastada. Esto no implica que no se utilice a las redes sociales para desestabilizar el *statu quo*. Terroristas, grupos sociales y el Estado mismo echan mano de estas plataformas y de su capilaridad para difundir propaganda y miedo; controlar, desinformar y fragmentar; potenciar troles, bots y campañas negativas en internet, o como un instrumento más en el arsenal

del "poder duro" de una nación, tradicionalmente asentado en lo militar y lo económico. El uso de estas herramientas, ya sea por parte del Daesh o en la elección presidencial de Estados Unidos, es un ejemplo claro de estos patrones.

Por un lado, las operaciones en tierra y la propaganda en línea del Daesh están entrelazadas a tal grado que cuesta trabajo distinguir una de la otra. Hace dos años, a medida que sus combatientes invadían el norte de Irak, el Daesh inundaba las redes sociales con un *blitzkrieg* de imágenes y datos de sus triunfos y sobre lo que deparaba a quienes se oponían a su avance (Twitter informa que ha borrado más de 125 mil cuentas vinculadas al Daesh desde mediados de 2015). Este fue el primer grupo terrorista en controlar territorio tanto físico como digital. Por el otro, la elección estadounidense conjuga dos de estas tendencias de ruptura. Primero, el aparente uso de verdaderas granjas de troles por parte de una nación para socavar la confianza en los sistemas electorales de otro país, obtener y filtrar información y hacer lo que ahora se denomina *astroturfing*, la simulación de opinión y la movilización de bases. Y, segundo, el empoderamiento de la extrema derecha –etiquetada de manera eufemística como "derecha alternativa"– a través de tribalismo y silos ideológicos en línea, e impulsada por narrativas simplistas de "nosotros contra ellos" y por las mentiras y noticias falsas sobre las cuales se construyó el triunfo de Donald Trump.

La tecnología está en el centro del poder disruptivo de todos estos actores. Somos testigos del inicio de una revolución mayor, una que está empezando a reconfigurar, por un lado, las conductas y el comportamiento de los grupos sociales y, por el otro, las estrategias político-militares de los actores no estatales y las potencias mundiales. Insisto: en el actual sistema internacional, lo que más nos conecta es también lo que nos hace más vulnerables. El poder de una nación en 2018 se expresa de maneras que habrían sido impensables hace tan solo unas décadas. La proyección y el uso del poder y su militarización en las relaciones internacionales y la geopolítica atestiguan un arco que va de Tucídides a Talleyrand hasta llegar a Twitter. Y no obstante, Sun Tzu, el estratega chino del siglo V a. C., reconocería lo que hoy ocurre con el uso del internet, las redes sociales, el hackeo y la posverdad: "El arte supremo de la guerra es dominar al enemigo sin haber luchado."

GUERRA FRÍA 2.0

Desde la administración de Ronald Reagan, en plena Guerra Fría, Rusia no tenía un sitio tan prominente en la vida política estadounidense. A la sorpresiva victoria electoral de Trump –la cual fue recibida en el parlamento ruso con vítores y champán– le siguieron acusaciones sobre el hackeo ruso a la campaña demócrata. Dos semanas antes de la toma de posesión de Trump, el director de Inteligencia Nacional de Estados Unidos, James Clapper, divulgó un informe que concluyó que Moscú había instrumentado una campaña para dañar a Hillary Clinton, fortalecer a Trump y "minar la confianza pública en el proceso democrático estadounidense". Estas acusaciones se han acrecentado a la luz de las subsecuentes revelaciones de vínculos y potencial colusión con Rusia del equipo de campaña y transición del ahora presidente de la Unión Americana, de las denuncias formales contra varios integrantes de este equipo y de la presión por parte del Congreso para que el fiscal especial Robert Mueller avance en la investigación.

No cabe duda que Rusia es el país que mejor ha entendido, en un mundo plenamente interconectado, el papel de las redes sociales como un instrumento clave en la caja de herramientas del poder duro de un Estado en el siglo XXI. Ninguna otra nación ha concebido y aplicado de manera tan eficaz esta nueva doctrina montada sobre un arsenal híbrido, militar, digital y propagandístico, tal y como quedó demostrado en 2008 en el conflicto con Georgia por el control de Osetia del Sur –la primera ocasión en que operaciones militares convencionales se llevaron a cabo de la mano de ciberataques– y luego en 2014 con la invasión a Ucrania y la ocupación de Crimea –una de sus facetas centrales fueron las granjas de bots, que sembraron confusión y desinformación entre los ucranianos–. Esta estrategia de *dezinformatsiya* –el uso y diseminación de información falsa para descalificar y desacreditar datos duros, a la prensa o a la verdad misma– estuvo acompañada de la articulación de una amplísima campaña de diplomacia pública hacia el exterior. La narrativa que se propala de manera masiva e iterativa a través de redes sociales se ha convertido en un arma más.

La elección presidencial estadounidense dio una oportunidad para aplicar –sin el componente militar– esta nueva doctrina. Era patente la animadversión de Vladimir Putin hacia el presidente Obama y la exsecretaria de Estado Hillary Clinton, junto con el recelo por la forma en que, desde su punto de vista, Estados Unidos había copado a Rusia desde el deshielo bipolar. Aunado a ello, todas las encuestas sobre política pública, valores sociales y filiación partidista muestran una y otra vez que los estadounidenses nunca habían estado tan polarizados ideológicamente en las últimas tres décadas como ahora. Esa balcanización mediática y de opinión pública alimentó una serie de conspiraciones, desde el presunto lugar de nacimiento de Obama (Kenia) hasta el supuesto instigador de la "falsa tesis" del cambio climático (China), ambas defendidas por el actual presidente de Estados Unidos. Al labrar su identidad y marca políticas, Trump promovió su visión de complots en un entorno que facilitaba la diseminación de las narrativas

"nosotros contra ellos", alimentando la certeza emocional a costa de la racionalidad de los datos duros.

Investigaciones periodísticas, de agencias de inteligencia europeas y estadounidenses y de las propias empresas de tecnología indican que un grupo ruso, activo desde hace una década y conocido como APT28 –al que se le vincula con el GRU, el servicio de inteligencia militar rusa, aunque Moscú ha negado de forma reiterada cualquier conexión con APT28, si bien el ministro de Defensa ha reconocido que existen "tropas de información"–, hackeó al Comité Nacional Demócrata y divulgó miles de correos electrónicos para desacreditar a Clinton y poner en duda la confianza de los ciudadanos en el sistema electoral y en la misma democracia estadounidense. En febrero de este año, el fiscal Mueller presentó acusaciones formales contra una granja de troles rusa (Internet Research Agency) que operó en territorio estadounidense durante la campaña y contra trece de sus empleados, de nacionalidad rusa, vinculados con actividades de hackeo y desinformación.

Estados Unidos no fue el único blanco. Un reportaje del *Financial Times*, de febrero de 2017, dio a conocer que los ciberataques contra la OTAN y las instancias de la Unión Europea aumentaron en 60% y 20%, respectivamente, con relación al año anterior; también, que se habían vulnerado computadoras de partidos políticos en Francia y Alemania, dos naciones que celebraron elecciones nacionales ese año. Es patente, además, que la combinación de hackeo a las campañas y los registros estatales electorales, el uso de granjas de troles y la diseminación masiva de desinformación –por medio de cuentas y *spots* pagados en redes sociales– pudo haber ayudado a decantar los 77 mil votos en tres estados (Michigan, Wisconsin y Pensilvania) que otorgaron a Trump la victoria en el Colegio Electoral. Tanto Twitter como Facebook han efectuado investigaciones internas en los últimos meses; recientemente alertaron que cientos de miles de sus usuarios se relacionaron con cuentas, información y contenidos alimentados por bots y cuentas provenientes de Rusia, a los que incluso retuitearon. El principio operativo era sencillo: sembrar –por medio de millones de interacciones y miles de cuentas– discordia y dudas en un país polarizado y capitalizar –a través de contenidos e información falsa– asuntos de la guerra cultural y de la política de identidad que hoy dividen a los estadounidenses –como el aborto, el derecho al matrimonio igualitario, la legalización de la cannabis, el papel de la religión en las escuelas o el racismo.

Hoy el poder se desplaza hacia los Estados, las corporaciones y los grupos religiosos y sociales que entienden y despliegan narrativas. Una de ellas, la narrativa "armada", busca socavar a su rival creando confusión, falsedades y cismas políticos y sociales; esta narrativa puede usarse tácticamente, como herramienta en un conflicto particular, o estratégicamente, para debilitar, neutralizar o derrotar a un adversario. En las elecciones pasadas, el objetivo táctico fue apoyar a Trump; el estratégico, debilitar a Estados Unidos. Pero una vez que Trump subió al poder, se desvanecieron las aspiraciones rusas de un descongelamiento en la relación con Washington –en especial, la revocación de sanciones aplicadas por Estados Unidos contra empresarios y funcionarios rusos–, pues el presidente no ha podido reconducir la relación con Moscú (como prometió) y, a medida que avanza la investigación sobre los vínculos de su campaña con actividades rusas, el Congreso ha redoblado su presión para mantener y ampliar las sanciones, pese a la resistencia del mandatario.

Hay que decirlo sin rodeos: las acciones cibernéticas y de desinformación rusas no son las responsables del Brexit, la victoria de Trump o el surgimiento de movimientos chovinistas y demagogos en Europa. Mayor peso han tenido el resentimiento contra la globalización y la dislocación socioeconómica, producto de la desindustrialización. Pero lo que sí es un hecho es que esta fragmentación política e ideológica, así como la embestida de Trump contra las alianzas y las instituciones de la posguerra, proveen a Rusia de un espacio para minar el actual sistema internacional basado en reglas, uno que Moscú considera geopolíticamente desfavorable. Alexei

Venediktov, editor en jefe del *Eco de Moscú*, no podría haberlo explicado mejor: "Hay que crear turbulencia al interior de Estados Unidos. Un país que se sume en la turbulencia, se ensimisma y se cierra al mundo."

¿Y EN MÉXICO? MIRÁNDONOS EL OMBLIGO

En el país estamos en pañales ante esta nueva realidad global. Frente a los retos que se avecinan, debemos dejar de nadar de muertito y de enterrar la cabeza en la arena. De entrada, es bien sabido en círculos de inteligencia internacionales que en México hay numerosos actores –del sector privado, los gobiernos estatales, los partidos políticos y los grupos criminales– que poseen herramientas, programas y equipo de intercepción y disrupción digital tanto o más sofisticados que los del Estado mexicano, y que también movilizan granjas de bots. Si a ello se suma la posibilidad –real– de que estos sean utilizados, por intereses variopintos, para incidir en nuestros comicios presidenciales de 2018, para vulnerar las instituciones electorales o sembrar desinformación, confusión y ruido, se vuelve incuestionable nuestro deber de hacer mucho más –y de hacerlo ya– para mitigar los riesgos. No minimizo en absoluto las prácticas y los frentes internos que se han usado en procesos electorales estatales recientes de nuestro país y que también se deben cuidar. Pero esto no significa que seamos invulnerables en el frente extranjero. Hay que blindar a México de amenazas que provengan del exterior y protegerlo de actores internos que, por diseño geopolítico o designio político, puedan dañar sus instituciones y su democracia. Se debe repensar la ciberseguridad, tanto en su vertiente interna como externa, para adecuarla a la compleja red global, donde la conectividad, la velocidad, la apertura, la oportunidad y las capacidades abren nuevos horizontes para nuestra economía y bienestar, pero que encierran retos fundamentales para el diseño e instrumentación de políticas públicas para nuestra seguridad y gobernanza.

Estamos a escasos meses de acudir a las urnas para elegir al próximo presidente de México. Mientras los partidos, la sociedad civil, los medios de comunicación y los analistas, encuestadores y empresarios se enfocan en los candidatos y en sus estrategias y propuestas de campaña, también habría que levantar la vista y poner atención a lo que sucede en el resto del mundo. Pese a que muchos crean con ingenuidad que los sucesos del exterior poco importan y poco nos afectan –o bien, que México, por alguna razón mágica, no forma parte de los cálculos geopolíticos globales–, los asuntos internacionales suelen ser muy tercos, y en ocasiones llegan a impactar los procesos políticos internos, tal y como podría suceder en nuestra elección presidencial. Dos factores convergentes hacen de esto un escenario posible: el primero tiene que ver con la ubicación de México y el actual contexto geoestratégico global; el segundo, con la debilidad institucional del país frente a un alto nivel de malestar político y social, que atestiguará una elección muy reñida y con un voto atomizado.

No es descabellado, pese a los pregones de muchos analistas y usuarios de redes sociales, que la gran estrategia rusa para replegar del mundo a los intereses estadounidenses –y, hasta cierta medida, los europeos– se enfoque en México. Bajo esa premisa, la siguiente oportunidad importante para crearle un frente de distracción a Estados Unidos se halla en su frontera sur. A diferencia de aquel país, donde hay cincuenta sistemas electorales, algunos de ellos digitales, en México hay un solo padrón electoral, electrónico, nacional y centralizado. En lugar de hackear diez registros electorales, como ocurrió allá, aquí solo habría que penetrar uno. Si se pudo hacer en una nación que tiene estándares y protocolos de ciberseguridad elevados, es fácil imaginar lo que podría ocurrir en un país con instituciones y protocolos rudimentarios en estos temas. Además, el contexto político mexicano se presta a ello: el nuestro es un país polarizado, con gran rechazo a los partidos y las instituciones gubernamentales, en el que diversas voces han puesto en entredicho la credibilidad del INE y la FEPADE y donde se cuestiona la imparcialidad, transparencia y equidad en todos los ámbitos de la vida nacional. También aquí los bots, como mecanismos de desinformación o intimidación, han echado raíces y se tiene documentada la presencia de empresas como Cambridge Analytica –actor en el triunfo del Brexit y de Trump– y de plataformas de propaganda oficial (Russia Today, RT, por ejemplo) que han sido usadas en otras naciones como vehículos de narrativas "armadas". Por si fuera poco, en las dos últimas elecciones presidenciales mexicanas se presentaron acusaciones de fraude.

De darse este escenario en 2018 –hay que decirlo con claridad y contundencia– no estará necesariamente dirigido contra México sino contra Washington. Y, a diferencia de lo que presenciamos en Gran Bretaña o Estados Unidos, su propósito esencial no es necesariamente apoyar un resultado electoral determinado o a un candidato en particular. Con mayor probabilidad buscará, antes que nada, provocar incertidumbre, confrontación y conflicto en el vecino "incómodo" de la administración Trump. No podemos ignorar que se ciernen un peligro para nuestro proceso electoral y una profunda y real amenaza a la seguridad nacional mexicana. Es tiempo de que entendamos que la combinación de nuestra geografía con nuestras divisiones internas y flaquezas institucionales puede ser aprovechada para esparcir desinformación, posverdad y crisis, minando de paso nuestra gobernabilidad democrática. –

ARTURO SARUKHÁN es embajador de carrera del Servicio Exterior Mexicano, consultor internacional y columnista de *El Universal*.