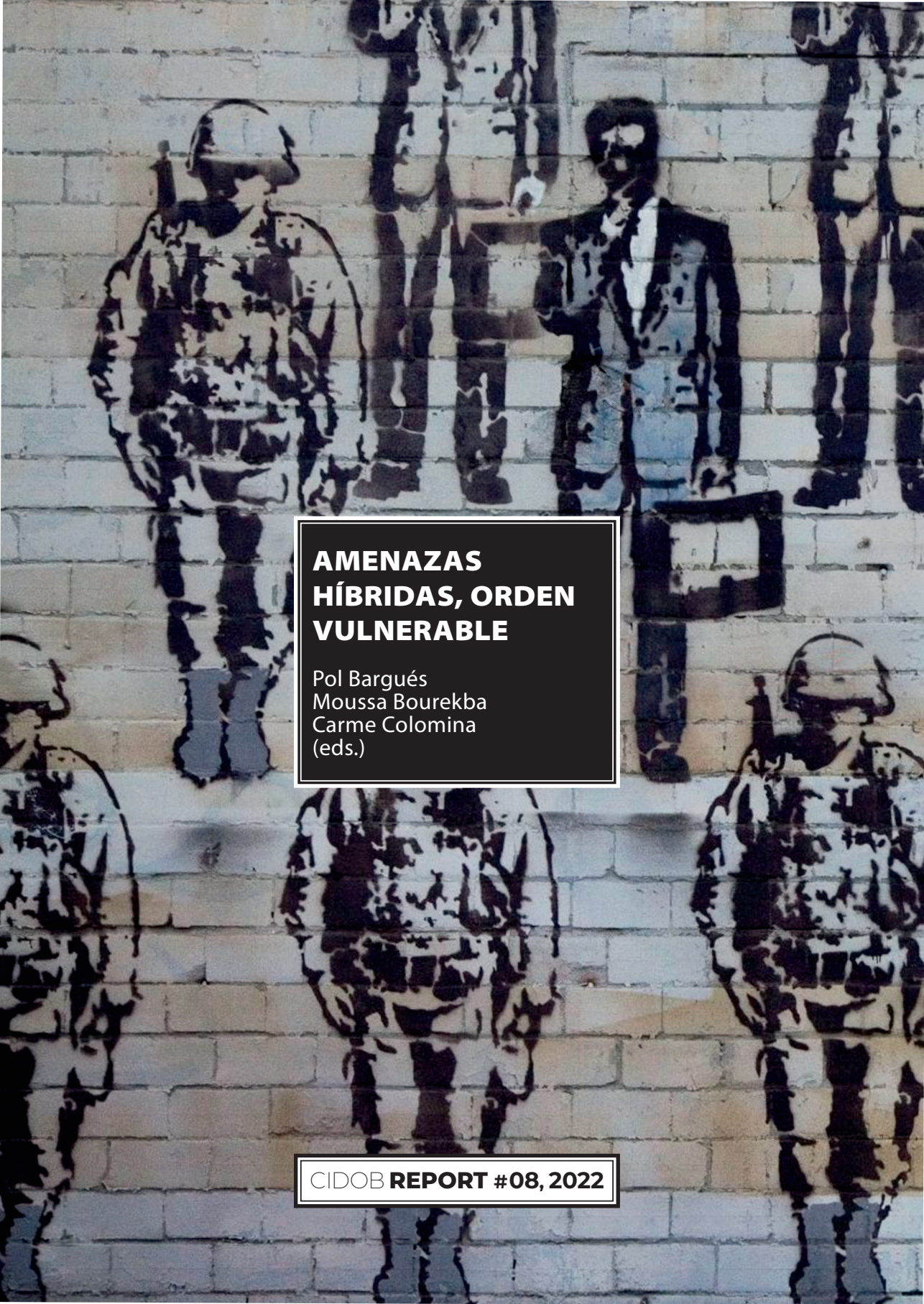

AMENAZAS HÍBRIDAS, ORDEN VULNERABLE

Pol Bargués
Moussa Bourekba
Carme Colomina
(eds.)

CIDOB **REPORT #08, 2022**

AMENAZAS HÍBRIDAS, ORDEN VULNERABLE

Pol Bargués, Moussa Bourekba
Carme Colomina (eds.)

CIDOB REPORT # 08
Barcelona, Septiembre 2022
ISSN: 2564-9078

CIDOB
BARCELONA
CENTRE FOR
INTERNATIONAL
AFFAIRS

Editores: Pol Bargués, Moussa Bourekba y Carme Colomina

Consejo editorial: Carmen Claudín, Carme Colomina, Anna Estrada, Blanca Garcés Mascareñas, Elisabet Mañé, Esther Masclans, Pol Morillas, Cristina Serrano, Sílvia Serrano y Eduard Soler

CIDOB
Elisabets, 12
08001 Barcelona
Tel.: 933 026 495
www.cidob.org
cidob@cidob.org

Impresión: Promotion Digital Talk S.L.
ISSN: 2564-9078 • E-ISSN 2564-9124
Depósito legal: B 11820-2017

Edición: Elisabet Mañé
Diseño y maquetación: Joan Antoni Balcells
Web y soporte técnico: Sílvia Serrano
Ventas y envíos: Marta Lizana
Producción: Anna Busquets Ferré

Barcelona, septiembre 2022

Imagen de la cubierta
Thomas Hawk, "Soldiers and Suits".
https://www.flickr.com/photos/thomashawk/91024106/in/photolist-93wi9-7AcQeF-8qYk3a-aqZ5do-bALwwk-7srmF1-dy6PvW-yp9qip-262qeEw-km964-cVvVbs-29L3HBg-eMTwa3-ecFP7V-a7xKDz-8E9FFC-ndrV2-zx3qX2-6Hhgs1-2bY5HR1-4ySCY-KXgCU-9jbHK8-7W97uG-K97jYR-aBxWU5-x6rkHu-9m5sqN-q6ULbi-4K9y1G-6pZ32n-4LojPy-2B2nK-2Kv8n6-mGiJxz-L53iMG-4zhNCh-8N72Cn-biWfN4-bs8LVj-zCk3j-6DbBai-cgbqyJ-aj1XxK-9NV89b-2WNbMH-8DVkGv-zVfvG-4Lyxbv-4K9xCN

SUMARIO

CIDOB REPORT
08- 2022

PRÓLOGO

Pol Morillas
Director, CIDOB

CIDOB REPORT
08- 2022

Las amenazas híbridas –la utilización de tácticas convencionales y no convencionales en escenarios de conflicto o en la confrontación geopolítica entre los grandes actores globales– son un elemento crecientemente desestabilizador en el orden internacional. En Occidente, el último Concepto Estratégico de la Organización del Tratado del Atlántico Norte (OTAN), presentado en la Cumbre de Madrid (29 y 30 de junio de 2022), reiteró que «competidores estratégicos utilizan tácticas híbridas para interferir en procesos e instituciones democráticas y para afectar la seguridad de los ciudadanos», destacando «las actividades maliciosas en el ciberespacio y el espacio, la promoción de campañas de desinformación, la instrumentalización de las migraciones, la manipulación de los suministros de energía y la coerción económica». También la Unión Europea, al menos desde 2016 y coincidiendo con la publicación de su Estrategia Global, ha creado instrumentos, estrategias y comunicaciones conjuntas para coordinar las políticas internas y externas, y así aumentar la resiliencia europea ante las amenazas híbridas.

Lejos de ser un fenómeno occidental, el auge de las tácticas híbridas se observa en varios continentes. En África, se detectan operaciones híbridas de apoyo a grupos extremistas, se interfiere

en elecciones o se ataca infraestructuras críticas. Por ejemplo, en 2021, Sudáfrica sufrió varios sabotajes en las líneas de transmisión de energía eléctrica que afectaron a las grandes industrias y agudizaron la crisis energética del país. En el Indo-Pacífico, según un informe del ASPI-ICPC, las amenazas híbridas están aumentando «en amplitud, aplicación e intensidad». Y, en plena invasión de Ucrania, aunque el Kremlin acusó a Occidente de lanzar una «guerra híbrida total» contra Rusia, las tácticas de desestabilización forman parte de manera reiterada del manual de operaciones de Moscú. En unas relaciones internacionales dominadas por la geoestrategia y la *Realpolitik*, las tácticas híbridas proliferan, dificultando la cooperación y la confianza en las instituciones de gobernanza global.

Sin embargo, ¿qué hay de nuevo en estas amenazas? En innumerables guerras a lo largo de la historia se han utilizado tácticas no convencionales –como el uso de *proxies*, de grupos insurgentes, o de propaganda– para desestabilizar o castigar al enemigo. Incluso en momentos de paz, durante el siglo XX, los estados rivalizaron con estrategias sucias de espionaje, propaganda, batallas económicas, intromisión en procesos democráticos, o instigación de insurgencias (Johnson, 2018). En la actualidad, puede que la intensificación de los conflictos híbridos –o su percepción aumentada– responda a una nueva conciencia de vulnerabilidad de los que se creían invulnerables.

PUEDE QUE LA INTENSIFICACIÓN DE LOS CONFLICTOS HÍBRIDOS –O SU PERCEPCIÓN AUMENTADA– RESPONDA A UNA NUEVA CONCIENCIA DE VULNERABILIDAD DE LOS QUE SE CREÍAN INVULNERABLES.

Este *CIDOB Report* parte de la constatación de que en los últimos años ha habido un incremento de tácticas híbridas y de amenazas percibidas como tal, así como una preocupación generalizada alrededor de lo *híbrido*. Hay dos factores principales que ayudan a entender esta intensificación: por una parte, la creciente interdependencia entre estados y, por otra, la exponencial diversificación de las tácticas híbridas.

Respecto al primer factor, la mayor conectividad en las relaciones internacionales, sobre todo con el fin de la Guerra Fría, facilitó la expansión de la globalización y los intercambios económicos, comerciales, energéticos, políticos y culturales. Se asumió que la conexión e interdependencia entre países frenaban el apetito por los conflictos y, al mismo tiempo, contribuían al desarrollo, la democratización y la paz global. Sin embargo, como sostiene Mark Leonard, esta *hiperconectividad* también ha ofrecido oportunidades para aquellos estados dispuestos a explotar las vulnerabilidades de otros. «El truco», dice Leonard (2016: 15), «es hacer que tus

competidores sean más dependientes de ti que tú de ellos –y utilizar esta dependencia para influir en su comportamiento–». Así, la interdependencia también tiene sus contraindicaciones, y puede ser utilizada como herramienta para explotar vulnerabilidades y exacerbar la confrontación entre grandes potencias, o incluso entre comunidades opuestas y polarizadas dentro de una misma sociedad. De aquí que actores como la Unión Europea hayan reforzado sus estrategias para dotarse de una mayor autonomía estratégica.

El segundo factor es la diversificación de las tácticas híbridas: desde la migración a la desinformación, pasando por la interferencia en procesos electorales, el uso de los recursos naturales o los virus informáticos. Todo es susceptible de ser convertido en un *arma* lanzada desde cualquier lugar y con consecuencias imprevisibles. Los desarrollos tecnológicos, sean de tipo civil o militar, así como el uso de las tecnologías de la información y la comunicación por actores estatales y no estatales, también han facilitado la explotación de las vulnerabilidades de otros. El proceso de digitalización, por su parte, ha multiplicado exponencialmente la capacidad de diseminación y penetración de la desinformación.

LOS DESARROLLOS TECNOLÓGICOS, SEAN DE TIPO CIVIL O MILITAR, ASÍ COMO EL USO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN POR ACTORES ESTATALES Y NO ESTATALES, TAMBIÉN HAN FACILITADO LA EXPLOTACIÓN DE LAS VULNERABILIDADES DE OTROS. EL PROCESO DE DIGITALIZACIÓN, POR SU PARTE, HA MULTIPLICADO EXPONENCIALMENTE LA CAPACIDAD DE DISEMINACIÓN Y PENETRACIÓN DE LA DESINFORMACIÓN.

Ante este nuevo escenario, en el que las amenazas híbridas se intensifican a partir de la explotación de la interdependencia y la creciente diversificación de tácticas, ¿qué estrategias y métodos se usan en el marco de estos conflictos?, ¿qué impacto tienen las amenazas híbridas en las sociedades de hoy?, ¿qué respuestas políticas se proponen? Este *CIDOB Report* aborda el reto que plantean dichas amenazas en las sociedades actuales y pretende contribuir al debate en un momento en el que el contexto internacional se caracteriza por el regreso de la guerra a Europa, la creciente contestación y polarización en el orden liberal internacional, la crisis del multilateralismo y de las normas de gobernanza global, así como la transformación geopolítica pospandemia.

Para ello, los autores y autoras del presente volumen se centran en algunas de las principales amenazas híbridas, así como en el desarrollo de los con-

flictos de este tipo en varias regiones del mundo. En el primer capítulo, Pol Bargués y Moussa Bourekba contextualizan la emergencia del concepto de *conflicto híbrido* y examinan las ventajas analíticas y prácticas que presenta dicho concepto. En el siguiente, Carme Colomina aborda la desinformación como instrumento de confrontación geopolítica, analizando cómo la transformación tecnológica ha amplificado el impacto de las guerras informativas. El capítulo tercero, de la mano de Blanca Garcés Mascareñas, reflexiona acerca de la instrumentalización de las migraciones por parte de actores estatales en el marco de diversos conflictos híbridos que afectan a varios países europeos. A continuación, en el cuarto capítulo, John Kelly pone de relieve el aumento en el uso de tácticas de desinformación con el fin de desestabilizar los regímenes democráticos, y apunta los principales retos a la hora de hacer frente a la amenaza multifacética que plantea la desinformación para las democracias. En esta misma línea, Manel Medina Llinàs, autor del quinto capítulo, demuestra cómo el ciberespacio se ha añadido a los tradicionales campos de batalla de los conflictos –tierra, mar y aire– y cómo el uso de ciberarmas se ha convertido en un reto estratégico en el marco de los conflictos híbridos.

A partir de aquí, el volumen se centra en espacios geográficos de confrontación. Así, la sexta contribución examina el concepto de resiliencia, poniendo el foco en un conflicto caracterizado por aunar tácticas híbridas y de guerra convencional: la actual invasión rusa de Ucrania. Al respecto, Andrey Makarychev y Yulia Kurnyshova sostienen que la reacción de la sociedad ucraniana a este conflicto es *también* híbrida, ya que no responde al esquema tradicional de gestión vertical de la respuesta civil por parte del estado atacado, sino que tiene un alto grado de autonomía y autoorganización. A continuación, ante un escenario global cada vez más marcado por la proliferación de conflictos híbridos, Guillem Colom Piella examina en la séptima contribución la evolución de los marcos estratégicos de la OTAN para detectar, contrarrestar y responder dichas amenazas., Por su parte, Inés Arco Escriche, autora del octavo capítulo, ahonda en esta misma dirección en su análisis de la estrategia de expansión emprendida por China, si bien lo híbrido no es ninguna novedad en la política exterior de este país. La milenaria estrategia híbrida china recurre a una genuina mezcla de medidas diplomáticas, económicas y militares para promover y defender sus intereses fundamentales de soberanía e integridad territorial, incluso en tiempos de paz. Por último, el noveno capítulo se detiene en otra región del mundo en la que se (des)dibuja un enfrentamiento combinando de métodos convencionales y no convencionales: el Magreb. En su contribución, Eduard Soler i Lecha analiza la creciente tensión entre Marruecos y Argelia, subrayando que, en vez de sustituir las amenazas convencionales, las tácticas híbridas podrían preceder o incluso favorecer un enfrentamiento armado.

Referencias

Leonard, Mark. *Connectivity Wars: Why Migration, Finance and Trade are the Geo-Economic Battlegrounds of the Future.* European Council on Foreign Relations, 2016 (en línea) [Fecha de consulta 13.06.2022] https://ecfr.eu/wp-content/uploads/Connectivity_Wars.pdf

Johnson, Robert. «Hybrid War and Countermeasures: A Critique of the Literature». *Small Wars & Insurgencies,* vol. 29, nº. 1 (2018), p. 141-163.

LA GUERRA POR TODOS LOS MEDIOS: LA INTENSIFICACIÓN DE LOS CONFLICTOS HÍBRIDOS

Pol Bargués
Investigador principal, CIDOB

Moussa Bourekba
Investigador, CIDOB

CIDOB REPORT
08- 2022

Origen de un concepto y sus críticas

El concepto de *conflicto híbrido* se popularizó a principios del siglo XXI en discusiones militares de la Organización del Tratado del Atlántico Norte (OTAN) para referirse a unas nuevas formas de librar batallas, que combinaban métodos regulares con irregulares. En la violencia que resultó de las intervenciones internacionales en Afganistán e Irak, en la guerra interconfesional entre sunitas y chiitas, en las estrategias de grupos terroristas transnacionales como Al Qaeda, así como en la guerra entre Israel y Hezbolá, actores estatales y no estatales utilizaron tácticas híbridas como la guerrilla urbana, el uso de armamento sofisticado (como los drones), la desinformación, los secuestros e, incluso, el terrorismo. Los ataques eran múltiples, heterogéneos, casi siempre rodeados de incertidumbre y sin apenas obediencia al derecho internacional. Así, la lucha en los conflictos híbridos iniciados a finales del siglo XX se alejaba de las «guerras antiguas» anteriores, como lo fueron las dos guerras mundiales, caracterizadas por enfrentamientos convencionales entre ejércitos regulares. En este sentido, los conflictos híbridos añadieron complejidad a las «nuevas guerras» de los años noventa, como Bosnia, Sierra Leona o Liberia, que enfrentaron a redes de actores estatales y no estatales en base a identidades diferenciadas, y que fueron gestionadas por misiones de paz internacionales (Kaldor, 2001).

Es probable que las diferencias entre estos conflictos no fueran tantas y que lo que realmente cambió fue la mirada de Occidente. En los años noventa, Estados Unidos y sus aliados occidentales, en paz y bonanza, alentados por lo que se asumía como una victoria al final de la Guerra Fría, no comprendían los enfrentamientos bélicos que libraban otros por territorio, interés económico o estratégico, identidad o religión (Bargués-Pedreny, 2018). Sin embargo, en la primera década del siglo XXI, en plena «guerra global contra el terror», el auge de tácticas híbridas puso fin al «autoengaño» de la década anterior, en la que se creía que paz y guerra podían ser limitadas y reguladas por instituciones internacionales (Johnson, 2018: 143).

Al poco tiempo, las amenazas híbridas no solo se observaban en zonas de conflicto, sino que también contaminaban las zonas de paz. En 2014, unos «hombres vestidos de verde», sin identificación militar, entraron en Crimea para controlar las infraestructuras, facilitar un referéndum, y lograr la anexión de este territorio de Ucrania a Rusia. La constatación, en los últimos años, de frecuentes ciberataques, campañas de desinformación, injerencias en procesos democráticos, o intentos de desestabilización por la movilización de migrantes en las fronteras externas de la Unión Europea (UE), ha erosionado profundamente la relación entre la UE y Rusia. Los ataques híbridos diluyen los límites entre guerra y paz. Se utilizan para explotar las oportunidades que brinda un mundo interconectado y globalizado, y así debilitar al adversario sin desgastarse en el terreno convencional (Colom Piella, 2018).

LOS ATAQUES HÍBRIDOS DILUYEN LOS LÍMITES ENTRE GUERRA Y PAZ. SE UTILIZAN PARA EXPLOTAR LAS OPORTUNIDADES QUE BRINDA UN MUNDO INTERCONECTADO Y GLOBALIZADO, Y ASÍ DEBILITAR AL ADVERSARIO SIN DESGASTARSE EN EL TERRENO CONVENCIONAL.

Voces críticas han subrayado que lo *híbrido* no es un fenómeno nuevo, ya que casi todos los conflictos a lo largo de la historia se han lidiado con tácticas diversas. Elementos no convencionales pueden apreciarse al menos desde las guerras púnicas, cuando los romanos se enfrentaron al ejército cartaginés, muy superior en el campo de batalla, a través de tácticas de desmoralización y desgaste, atacando las líneas de abastecimiento y esquivando combates directos (Carr & Walsh, 2022). Otros estudios críticos han señalado que el concepto de *conflicto híbrido* es un «concepto atrápalo-todo» y eurocéntrico que permite a Occidente explicar las estrategias de terceros con ejemplos tan dispares como la guerra en Ucrania, el conflicto entre Marruecos y Argelia, o la movilización intencionada de migrantes con fines políticos (Johnson, 2018). Además, si hay otros conceptos que ya se han utilizado para describir conflictos actuales

como *guerra asimétrica*, *conflicto complejo-irregular*, *guerras de conectividad*, *conflictos de cuarta o quinta generación* o *zona gris*, ¿qué valor aporta hablar de *conflictos híbridos*?

Es la intensificación de estas tácticas lo que ha revalorizado dicho concepto. Tanto en Europa como en otras regiones del mundo, en las estrategias de seguridad de gobiernos y organizaciones internacionales crece la percepción de que las amenazas híbridas nunca cesan, ni en momentos de paz ni en tiempos de guerra, y acechan por tierra, mar, aire, en línea o desde el espacio. Este capítulo conceptual, que pretende sentar las bases para el análisis que ofrece este *CIDOB Report*, se centra en tres características de los conflictos híbridos, que determinan las relaciones internacionales actuales: primero, la *incertidumbre* que envuelve a los conflictos híbridos, donde es difícil separar la guerra de la paz, así como probar quién está detrás de un ataque; segundo, las *tácticas*, que se diversifican para explotar las vulnerabilidades de los otros estados; y, finalmente, los *objetivos* de estas tácticas, que parecen buscar la erosión de los valores y la legitimidad de los sistemas políticos del adversario. Persiguen la desestabilización y no la victoria.

LA INCERTIDUMBRE ENVUELVE EL CONFLICTO HÍBRIDO. ES DIFÍCIL IDENTIFICAR AL RESPONSABLE DE UN CIBERATAQUE, O DE PROBAR QUIÉN ORGANIZÓ TUMULTOS O COMETIÓ AGRESIONES CONCRETAS; ES CASI IMPOSIBLE SABER QUIÉN EMPEZÓ UN RUMOR MACABRO, IGUAL QUE CUESTA DESMENTIR NOTICIAS FALSAS.

Incertidumbre, multiplicidad y confusión

Lejos quedan las declaraciones de guerra formales para dar comienzo a las hostilidades entre estados. A menudo se ha entendido lo híbrido como las tácticas que están por debajo del umbral de la guerra y que desgastan al oponente mientras se evitan enfrentamientos mayores y el riesgo de destrucción mutua –por ejemplo, entre potencias nucleares como Rusia y los países integrantes de la OTAN (Friedman, 2018)–. Lo que es seguro es que las tácticas híbridas enturbian los tiempos de paz y las relaciones entre estados, al mismo tiempo que provocan que las guerras sean más inciertas y confusas.

De hecho, la incertidumbre envuelve el conflicto híbrido. Es difícil identificar al responsable de un ciberataque, o de probar quién organizó tumultos o cometió agresiones concretas; es casi imposible saber quién empezó un rumor macabro, igual que cuesta desmentir noticias falsas. Además, mientras en una guerra convencional suelen ser el estado y el ejército los responsables de la lucha, en el marco de los conflictos híbridos también in-

tervienen *proxies*, *hackers*, grupos criminales, narcotraficantes, paramilitares, terroristas o contratistas privados como Blackwater, G4S Secure Solutions, o el grupo Wagner.

La segunda característica destacable que nos permite adentrarnos en las relaciones internacionales contemporáneas es el uso de nuevas tácticas de desestabilización. Inimaginables hace unos años, estas tácticas son cada vez más diversas. Los tanques y las ametralladoras se combinan con armamento sofisticado como drones, misiles hipersónicos o sistemas microelectromecánicos de insectos híbridos de vigilancia. Dichas tecnologías no solo están en manos de los estados, sino también de grupos terroristas, delincuentes o narcotraficantes. En las redes sociales, grupos terroristas reclutan a combatientes, forjan odio, difunden propaganda y preparan ataques terroristas. Los estados permiten que centenares de migrantes crucen las fronteras en pocas horas para generar la sensación de desbordamiento y vulnerabilidad en el país vecino; la desinformación contribuye a polarizar sociedades y deslegitimar instituciones; y empresas multinacionales ejercen de actores privados en los conflictos y en las relaciones internacionales (véanse los capítulos de Garcés y Colomina en este volumen).

LOS ESTADOS RECURREN CADA VEZ MÁS A TÁCTICAS HÍBRIDAS YA QUE PROPORCIONAN UNA VENTAJA INMEJORABLE DESDE EL PUNTO DE VISTA ESTRATÉGICO: PERMITEN AVANZAR HACIA LA CONSECUCIÓN DE DETERMINADOS OBJETIVOS, SEAN POLÍTICOS, ECONÓMICOS O DE OTRA NATURALEZA, SIN CERRAR LA PUERTA A LAS NEGOCIACIONES O A LAS RELACIONES DIPLOMÁTICAS O ECONÓMICAS DE TODO TIPO.

Estas tácticas diversas sirven para atacar y explotar las vulnerabilidades económicas, políticas y diplomáticas de otros estados. La clave está en ver cómo la globalización y la interconexión, que facilitan la cooperación y el intercambio, también abren oportunidades para lanzar ataques y generar tensión. En palabras de Mark Leonard, «la interdependencia, antes considerada la fórmula para evitar conflictos, se ha vuelto una moneda de cambio poderosa, ya que los países tratan de explotar las asimetrías de sus relaciones». Toda conexión es susceptible de ser instrumentalizada, y ha crecido el escepticismo o la desconfianza entre las grandes potencias: vivimos en un mundo moldeado por políticas del poder en el que «todo puede convertirse en un arma y nos enfrentamos a una batalla de narrativas» escribe el alto representante de la UE y vicepresidente de la Comisión, Josep Borrell, en el prólogo de la Brújula Estratégica de la Unión Europea.

La tercera característica significativa son los objetivos de estos conflictos híbridos. Igual que el comienzo es difícil de datar, tampoco en estos conflictos se persigue una «victoria» que ponga fin a la contienda (O'Driscoll, 2019). Entonces, si no se utilizan para ganar la guerra o la paz, ¿cuáles son los objetivos de las tácticas híbridas? Tácticas como la desinformación, la manipulación o la injerencia electoral buscan erosionar la legitimidad de las instituciones, la confianza en las administraciones o la manipulación de resultados electorales. Lo híbrido genera inestabilidad y desgaste en la democracia, crea polarización política y dinamita la coexistencia y los consensos.

Los estados recurren cada vez más a tácticas híbridas, ya que proporcionan una ventaja inmejorable desde el punto de vista estratégico: permiten avanzar hacia la consecución de determinados objetivos, sean políticos, económicos o de otra naturaleza, sin cerrar la puerta a las negociaciones o a las relaciones diplomáticas o económicas de todo tipo. En ausencia de una declaración de guerra o de una situación de conflicto abierto entre dos estados, siempre existe la posibilidad de hablar de paz y de negociar. Bajo esta perspectiva, los conflictos híbridos suelen tener un coste considerablemente más bajo que la carga que puede suponer una guerra convencional. Así, generalmente, son más fáciles de iniciar, eluden responsabilidades directas, son logísticamente menos complejos, económicamente menos costosos, y políticamente menos arriesgados, ya que no buscan la victoria militar.

Conclusión: tiempos híbridos

Aunque no sean un nuevo fenómeno, los conflictos híbridos han proliferado en un momento en que Occidente siente contestada su hegemonía y hay una erosión de las normas internacionales. Lo híbrido sirve para entender la creciente incertidumbre que envuelve tanto los tiempos de paz como los de guerra, y para poner el énfasis en la cantidad de métodos y medios que permiten a un actor lograr determinados objetivos. En otras palabras, este concepto puede ayudar a centrarse en cómo los actores se relacionan y en cómo pretenden luchar. Las implicaciones para el orden internacional son profundas. Esta modalidad de conflicto es recurrentemente utilizada por actores estatales y no estatales con fines de desestabilización militar, política, económica y social. Las normas se incumplen, las relaciones se deterioran. Las ventajas estratégicas de las tácticas híbridas, y el bajo coste que supone recurrir a ellas, explican la proliferación e intensificación en su uso. Desde esta perspectiva, conviene repensar nuestros marcos analíticos y estratégicos con vistas a reducir el potencial desestabilizador que puede acarrear esta nueva generación de conflictos.

Referencias

Bargués-Pedreny, Pol. *Deferring Peace in International Statebuilding: Difference, Resilience and Critique*. London: Routledge, 2018.

Carr, Andrew y Walsh, Benjamin. «The Fabian strategy: How to trade space for time». *Comparative Strategy,* vol. 41, nº. 1 (2022), p. 78-96.

Friedman, Ofer. *Russia 'Hybrid Warfare': Resurgence and Politicisation*. Oxford: Oxford University Press, 2018.

Kaldor, Mary. *Las nuevas guerras. Violencia organizada en la era global*. Barcelona: Tusquets, 2001.

Johnson, Robert. «Hybrid War and Countermeasures: A Critique of the Literature». *Small Wars & Insurgencies*, vol. 29, nº. 1 (2018), p. 141-163.

O'Driscoll, Cian. *Victory: The Triumph and Tragedy of Just War.* Oxford: Oxford University Press, 2019.

LA PALABRA COMO ARMA: DE LA DESINFORMACIÓN A LA BATALLA GLOBAL POR LA NARRATIVA

La desinformación es un instrumento clave en el catálogo de las amenazas híbridas: genera inestabilidad y desgaste en la democracia, crea polarización política y dinamita la coexistencia y los consensos. La capacidad de alterar la información o los datos, factores decisivos para la obtención del poder, se ha convertido en una amenaza para los procesos democráticos, pero también en una herramienta al servicio de una confrontación tecnológica y digital que determina una nueva bipolaridad en la agenda internacional. Sin embargo, la verdadera capacidad ofensiva de la palabra como arma no reside tanto en el contenido del mensaje como en el poder de viralización y penetración que le han ofrecido las redes sociales.

Carme Colomina
Investigadora principal, CIDOB

CIDOB REPORT
08- 2022

En 1998, el general Vladimir Slipchenko, entonces vicepresidente de la Academia rusa de Ciencias Militares, afirmaba que «la información es un arma al igual que los misiles, las bombas, los torpedos, etc. Ahora queda claro que la confrontación informativa se convierte en un factor que tendrá un impacto significativo en el futuro de la guerra en su origen, curso y resultado».

La lógica militar y la transformación tecnológica acabaron confluyendo en un espacio digital donde Internet se ha convertido en uno de los frentes esenciales para la desestabilización. «El elemento más importante de la invasión rusa de Ucrania en 2014 fue la guerra informativa concebida para desautorizar la realidad», escribía Timothy Snyder en *El camino hacia la no libertad* (2018). Desde aquella ofensiva cibernética inicial, «la más amplia de la historia», según el mismo Snyder, que «no llegó a los titulares de Occidente», hasta el frente digital de la invasión rusa de Ucrania iniciada el 24 de febrero de 2022, la hibridación del conflicto y la contestación del orden global han vivido su propia aceleración.

Para Occidente, Ucrania es hoy la primera guerra viralizada; retransmitida en tiempo real a través de las redes sociales; narrada a partir de fragmentos de imágenes que, en pocos segundos, intentan reflejar amenazas, miedos, heroicidades y devastación. Y no siempre el relato *online* coincide con los hechos *offline*. Aunque, en realidad, no es la primera guerra mediada por las redes sociales. Siria fue el primer laboratorio global donde el apagón informativo impuesto a la cobertura internacional se sorteó con un flujo torrencial de contenido en línea ofrecido por activistas o periodistas locales desde el interior del país, lo que ya entonces planteó retos éticos importantes sobre los circuitos de la información y la veracidad de las fuentes.

Sin embargo, Ucrania puede convertirse en el primer frente bélico donde miden sus fuerzas las dos grandes tendencias globales de digitalización y sus plataformas: el tecnoautoritarismo de Rusia y China, y el modelo estadounidense del Silicon Valley; entre el poder de Telegram y Tik Tok en la configuración del relato global de la guerra, y la implicación de los gigantes tecnológicos de Estados Unidos ejerciendo de actores privados en el conflicto, alineados con las estrategias occidentales, ya sea para la presión política para la captura y el control tanto de datos como de información (desde el mapeo a la censura), ya sea para la facilitación de análisis e información técnica para reforzar la seguridad del Gobierno ucraniano.

La (des)información es un arma en tiempos de guerra y una amenaza híbrida para la paz. Una herramienta no militar que puede emplearse para irrumpir en espacios civiles y desestabilizarlos, con implicaciones para la seguridad local, regional o nacional. Pero su verdadera capacidad ofensiva no reside tanto en el mensaje como en el poder de viralización y penetración que las redes sociales le han proporcionado. Por eso es imprescindible entender, primero, cómo la interconexión digital ha transformado las relaciones sociales, de la misma forma que los equilibrios de poder a escala global, ya sea entre potencias como entre los nuevos actores de las relaciones internacionales (estatales, no estatales y privados). No se puede separar la desinformación de los incentivos, *drivers* técnicos y factores sociopsicológicos que están presentes en estos tiempos hiperconectados (Van Raemdonk y Meyer, 2022).

Orden algorítmico

Internet es la infraestructura donde se construye nuestra cotidianidad. La tecnología ha transformado nuestra experiencia de inmediatez, nos ha sumido en una infinidad de posibilidades (des)informativas, de profusión de fuentes y de relatos –veraces, o no– que se nos ofrecen desde la red sin necesidad de intermediarios. La posverdad no es solo mentira; es una

distorsión de la verdad, cargada, sobre todo, de intencionalidad. Este es el espacio en el que la información compite con relatos contradictorios, bulos y medias verdades, teorías conspirativas, mensajes de odio, e intentos de manipulación de la opinión pública. La irrupción de la desinformación en línea ha supuesto la aparición de un «nuevo daño social» (Del Campo, 2021), que se expresa a través de falsedades de distinto tipo, algunas legales y otras ilegales, y que impacta en el discurso público y la seguridad humana.

La vieja propaganda, amplificada exponencialmente por la tecnología y la hiperconectividad, ha multiplicado su potencia y su sofisticación. Las posibilidades son ingentes: redes sociales (abiertas o encriptadas); bots (aplicaciones de *software* que ejecutan tareas automatizadas) y técnicas de microfocalización, como los *dark ads* –publicidad dirigida psicométricamente para influir en la opinión pública y envenenar el clima del discurso–; sistemas de inteligencia artificial que imitan a los humanos o reproducen la cognición humana a base de datos y entrenamiento; técnicas de manipulación de audio y video que alteran nuestra percepción y nos inducen a desconfiar incluso de nuestra capacidad de discernir sobre qué es y qué no es verdad... La *infocracia*, o «régimen de la información» en el mundo digital, que ha teorizado Byung-Chul Han (2022), es una forma de dominio en el que «la información y su procesamiento mediante algoritmos e inteligencia artificial determinan de modo decisivo los procesos sociales, económicos y políticos». La capacidad de alterar la información o los datos, factores decisivos para la obtención del poder, trastoca los procesos democráticos.

LA (DES)INFORMACIÓN ES UN ARMA EN TIEMPOS DE GUERRA Y UNA AMENAZA HÍBRIDA PARA LA PAZ. UNA HERRAMIENTA NO MILITAR QUE PUEDE EMPLEARSE PARA IRRUMPIR EN ESPACIOS CIVILES Y DESESTABILIZARLOS, CON IMPLICACIONES PARA LA SEGURIDAD LOCAL, REGIONAL O NACIONAL. PERO SU VERDADERA CAPACIDAD OFENSIVA NO RESIDE TANTO EN EL MENSAJE COMO EN EL PODER DE VIRALIZACIÓN Y PENETRACIÓN QUE LAS REDES SOCIALES LE HAN PROPORCIONADO.

Los algoritmos son explotados por empresas, como hizo Cambridge Analytica, que crean perfiles basados en el género de las personas, la orientación sexual, las creencias, o los rasgos de personalidad, entre otros, para la manipulación política. Las sociedades son vulnerables porque nosotros, como individuos, también lo somos. Estamos expuestos a la voluntad y al orden opaco de unos algoritmos que Cathy O'Neil (2016) elevó a la categoría de «armas de destrucción matemática».

La desinformación, entendida como «información falsa, creada deliberadamente para dañar a una persona, grupo social, organización o país» –según la definición de la Comisión Europea–, tiene como objetivo desestabilizar sociedades, atacando directamente a espacios civiles con el objetivo de fomentar la polarización y el malestar, cuando no el conflicto (Freedman *et al*., 2021; véase Medina, en este volumen). Sin embargo, la difusión de la desinformación no ocurre en el vacío. Su capacidad de penetrar en los debates públicos, de confundir o erosionar, por ejemplo, la confianza en instituciones o procesos electorales, bebe muchas veces de divisiones socioculturales existentes; apunta hacia vulnerabilidades previas y hacia ciertos grupos supuestamente inclinados a confiar en dichas fuentes o narrativas, que pueden contribuir voluntaria o involuntariamente a su difusión. Los abusos de poder, los sistemas políticos disfuncionales, las desigualdades y la exclusión son caldos de cultivo para la desinformación (Van Raemdonk y Meyer, 2022).

LOS INTENTOS DE MANIPULACIÓN NO TIENEN LÍMITES GEOGRÁFICOS NI UN ÚNICO ORIGEN. EN LOS ÚLTIMOS AÑOS, FACEBOOK Y TWITTER HAN ATRIBUIDO OPERACIONES DE INFLUENCIA EXTRANJERA A SIETE PAÍSES (CHINA, INDIA, IRÁN, PAKISTÁN, RUSIA, ARABIA SAUDÍ Y VENEZUELA), QUE HAN UTILIZADO ESTAS PLATAFORMAS PARA INFLUIR EN AUDIENCIAS GLOBALES. LAS REDES SOCIALES SON UN NUEVO INSTRUMENTO DE PODER GEOPOLÍTICO.

Es la identificación de estas vulnerabilidades, para generar mensajes que las exacerben, lo que se considera una amenaza híbrida a los sistemas democráticos, los cuales, precisamente por su naturaleza abierta, están más expuestos a sus efectos. Desde la perspectiva agonística de Chantal Mouffe (1999), el conflicto y el desafío al *statu quo* político y social son una parte esencial del pluralismo en las democracias deliberativas. Sin embargo, cuando la desinformación atenta contra el derecho a la formación de opiniones propias sin interferencias[1], o amplifica la vulnerabilidad de los ciudadanos ante el discurso de odio, o refuerza la capacidad de los actores estatales y no estatales para socavar la libertad de expresión, entonces se convierte en una amenaza para los derechos humanos y para los fundamentos democráticos. Por eso, la desinformación en todas sus formas –desde la mentira hasta la incitación al odio, pasando por los memes y la manipulación

1. Artículo 19 del Pacto Internacional de Derechos Civiles y Políticos (ICCPR, por sus siglas en inglés).

audiovisual– no son solo «armas de distracción masiva», sino que, muchas veces, responden a estrategias deliberadas de disrupción para alterar las percepciones de la opinión pública. En estos casos, la intención de perjudicar o lucrarse que caracteriza a estos contenidos falsos suele ir acompañada de estrategias y técnicas para maximizar su influencia. El objetivo es la erosión de los valores y la legitimidad del sistema político del adversario (véase Bargués y Bourekba, en este volumen).

El grupo de trabajo sobre libertad de expresión y abordaje de la desinformación de la UNESCO, en su análisis de los diferentes actores responsables de la desinformación, distingue entre los autores del contenido desinformativo y los encargados de su distribución: entre los instigadores (directos o indirectos), que están en el origen de la desinformación, y los agentes (*influencers*, individuos, organizaciones, gobiernos, empresas, instituciones) encargados de difundir las falsedades (Bontcheva y Posetti, 2020). Los agentes que participan en la diseminación de falsedades, conspiraciones o amenazas, que actúan como amplificadores de la desinformación –tanto si lo hacen de manera voluntaria como involuntaria– pueden ser, a su vez, víctimas de manipulación o de los intentos de instrumentalización de vulnerabilidades sociales. El resultado es un aumento del escepticismo y una erosión de la confianza en las instituciones. Los consensos que vertebran las sociedades democráticas son hoy más débiles.

No se trata solo de un fenómeno de Occidente ni, únicamente, de una amenaza exterior. A medida que la polarización ganaba terreno en la política global, sobre todo en el último lustro, el poder de las redes sociales en la radicalización del discurso público ha quedado al descubierto: desde la insurrección del 6 de enero ante el Capitolio de Washington, hasta el genocidio de los rohinyás en Birmania; desde la explotación del conflicto racial en Estados Unidos a través de cuentas falsas y troleos en línea, hasta la campaña de desinformación «brutal e implacable» auspiciada por los gobiernos de Rusia y Siria –según la investigación de Bellingcat en 2018– contra la ONG Cascos Blancos, encargada de investigar las evidencias de flagrantes violaciones de derechos humanos cometidas por los ejércitos de estos dos países en la guerra de Siria.

La geopolítica de la posverdad ha transformado amenazas y estrategias. Como advertía el Informe de riesgos globales del Foro Económico Mundial, en 2019, «las nuevas capacidades tecnológicas han intensificado las tensiones existentes sobre los valores –por ejemplo, debilitando la privacidad individual o aumentando la polarización–, mientras que son las diferencias en cuanto a valores, precisamente, las que están determinando el camino y la dirección de los avances tecnológicos en diferentes países».

Orden geopolítico

Los intentos de manipulación no tienen límites geográficos ni un único origen. En los últimos años, Facebook y Twitter han atribuido operaciones de influencia extranjera a siete países (China, India, Irán, Pakistán, Rusia, Arabia Saudí y Venezuela), que han utilizado estas plataformas para influir en audiencias globales. Las redes sociales son un nuevo instrumento de poder geopolítico, que ha entronizado a unos recién llegados actores de este orden desinformativo global, que rompe con las hegemonías tradicionales del relato internacional.

La pandemia de la COVID-19 no solo aceleró los procesos de digitalización sino también la «batalla global de narrativas», en palabras del Alto Representante para Asuntos Exteriores y Política de Seguridad de la Unión Europea, Josep Borrell, que alimentó aún más la sensación de vulnerabilidad de Occidente. No era una percepción nueva. El mundo digital había empezado a sacudir las estructuras del orden post-1945 desde hacía ya más de una década. En 2011, la entonces secretaria de Estado, Hillary Clinton, advirtió ante el Congreso de los Estados Unidos que su país se encontraba inmerso en «una guerra de información» y la estaban perdiendo. Clinton se refería a la presencia global de RT (Russia Today), al proyecto de televisión que China había lanzado en 2009 (CCTV), y al poder demostrado por Al Jazeera en la cobertura de las primaveras árabes. El Sur global tenía su propio relato de las transformaciones que estaban desafiando a las tradicionales estructuras de poder. Los instrumentos tradicionales del *soft power* estadounidense, como fue la CNN, perdían presencia global. La paradoja es que la candidatura de Clinton a la Casa Blanca acabó víctima tanto de esta guerra informativa como de la nueva centralidad de las herramientas y el discurso *online* que, en 2016, decidieron la suerte de las elecciones estadounidenses.

Sin embargo, desde la irrupción de la *infodemia* pandémica, la magnitud y la velocidad de esta transición han incrementado la sensación no solo de vulnerabilidad sino de pérdida de influencia por parte de Estados Unidos y la Unión Europea, que se han sentido obligados a replantearse su papel en las nuevas dinámicas de poder político y tecnológico.

Internet ha sido el gran multiplicador de este proceso de pérdida de hegemonía en el discurso global, que ha confrontado a Estados Unidos con sus propias tácticas, ahora desplegadas por Rusia o China, nuevos aliados políticos, económicos o securitarios de una parte importante del Sur global. La paradoja, además, es que muchas veces estas amenazas híbridas que desafían a los otrora espacios de influencia de Washington se despliegan a través de las grandes plataformas de Silicon Valley que han globalizado el poder.

La geopolítica, a través de las distintas aproximaciones a la tecnología, está moldeando la sociedad de la información. Este espacio de confrontación informativa, que vaticinaba el general Slipchenko, está en conflicto no solo por una lucha de poder, sino también por el choque de modelos para determinarlo. La palabra lleva implícita un marco mental y unos valores concretos, por eso se ha convertido en el arma híbrida de esta confrontación. La desinformación ofrece fértiles espacios de influencia a nuevos actores –estatales o privados– cada vez más determinantes en la confrontación de poderes de este nuevo orden global digital.

Referencias

Bontcheva, Kalina y Posetti, Julie (eds.). «Balancing Act: Countering Digital Disinformation While Respecting Freedom of Expression». *UNESCO Broadband Commission Report* (septiembre de 2020).

Del Campo, Agustina. «Disinformation is not Simply a Content Moderation Issue». En: Feldstein, S. (ed.). *Issues on the Frontlines of Technology and Politics*. Carnegie Endowment for International Peace, 2021, p. 23-24 (en línea) [Fecha de consulta: 21.02.2022] https://carnegieendowment.org/2021/10/19/disinformation-is-not-simply-content-moderation-issue-pub-85514

Freedman, Jane; Hoogensen Gjørv, Gunhild; Razakamaharavo, Velomahanina. «Identity, stability, Hybrid Threats and Disinformation». *ICONO 14, Revista de Comunicación y Tecnologías Emergentes*, vol. 19, nº. 1 (junio de 2021), p. 38-69.

Han, Byung-Chul. *Infocracia. La digitalización y la crisis de la democracia*. Barcelona: Penguin Random House, 2022.

Mouffe, Chantal. «Deliberative Democracy or Agonistic Pluralism». *Social Research*, vol. 66, nº.3 (1999), p. 745-758.

O'Neil Cathy. *Armas de destrucción matemática: cómo el* big data *aumenta la desigualdad y amenaza la democracia*. Madrid: Capitán Swing, 2016.

Snyder, Timothy. *El camino hacia la no libertad*. Barcelona: Galaxia Gutenberg, 2018.

Van Raemdonck, Nathalie; Meyer, Trisha. «Why Disinformation is Here to Stay. A Socio-technical Analysis of Disinformation as a Hybrid Threat». En: Lonardo, Luigi (ed.). *Addressing Hybrid Threats: European Law and Policies*. Bruselas: VUB, 2022.

LA «INSTRUMENTALIZACIÓN» DE LAS MIGRACIONES

La instrumentalización de las migraciones en las fronteras exteriores de la Unión Europea (UE) empieza a ser habitual. En febrero de 2020, el Gobierno turco mandaba más de 13.000 personas a la frontera con Grecia. En mayo de 2021, Marruecos dejaba entrar irregularmente a Ceuta más de 10.000 personas en dos días. En otoño de 2021 fue el turno del régimen bielorruso, al facilitar la llegada de miles de personas a la frontera con Polonia, Letonia y Lituania. En este contexto, Bruselas no ha dudado en calificar las llegadas de miles de personas (familias y menores incluidos) como una grave «amenaza híbrida» a su «seguridad». También lo ha hecho la OTAN en su nuevo Concepto Estratégico, donde la «instrumentalización de las migraciones» por parte de «actores autoritarios» es considerado como un ataque a la soberanía y la integridad territorial de los estados.

Blanca Garcés Mascareñas
Investigadora sénior, CIDOB

CIDOB REPORT
08- 2022

La instrumentalización de las migraciones no es nueva. La politóloga norteamericana Kelly M. Greenhill (2010) acuñó el término «*weaponisation of migration*» para referirse al uso de las migraciones como arma de guerra política y militar. Con una perspectiva histórica de larga duración, Greenhill distingue entre intenciones *coercitivas*, es decir, cuando las migraciones se utilizan como instrumento de política exterior para presionar a otros estados; intenciones de *apropiación*, cuando el objetivo es anexionar determinados territorios o consolidar el poder; o intenciones por razones *económicas*, buscando obtener una ganancia financiera.

No cabe duda de que las intenciones de Turquía, Marruecos y Bielorrusia, en los episodios antes mencionados, son claramente coercitivas al instrumentalizar la migración para inducir cambios y obtener concesiones de la UE. El presidente tur-

co, Recep Tayyip Erdogan, pedía más ayuda financiera para la acogida de refugiados y apoyo a las operaciones militares turcas en el norte de Siria. Marruecos respondía ante lo que consideraba una falta de lealtad por la hospitalización en Logroño del líder del Frente Polisario Brahim Ghali y, en el fondo, exigía connivencia con la cuestión de la soberanía marroquí sobre el Sahara Occidental. Bielorrusia, con Rusia detrás, presionaba para que la UE no se inmiscuyera en sus asuntos interiores.

Ante estos «chantajes», la UE se ha escandalizado cada vez. Por un lado, se ha ruborizado por el uso «indecente» y «cínico» de los refugiados con fines políticos por parte de terceros países. Por otro lado, no ha dudado en calificar la llegada de miles de personas (familias y menores incluidos) como una grave «amenaza híbrida» que afecta a la «seguridad» y, por ello, en declararse «en guerra», tanto en la retórica como con el despliegue de los ejércitos nacionales en frontera. La UE ha respondido con contundencia, e incluso con unión – donde no acostumbra a haberla –, sin darse cuenta de que, en el fondo, en toda esta historia no es sino víctima de sí misma. En muchos sentidos, además.

Primero, la UE es víctima de sí misma al sobrerreaccionar. Lo que asegura el éxito del chantaje es el miedo (o casi obsesión) a otra «crisis migratoria». Al final, da igual cuántos sean. Lo que importa es el miedo: de una parte, del electorado hacia los migrantes, y de los gobiernos hacia la división y el caos que la UE y los estados miembros escenifican en cada ocasión. Hay expertos que aseguran que la invasión rusa de Ucrania perseguía también desestabilizar la UE con una nueva «ola» de refugiados. Sin embargo, esta vez, a pesar de que no se trata de miles sino de millones, no ha habido sobreactuación. La proximidad de los refugiados y, sobre todo, una guerra vivida como propia (con la percepción de un enemigo común) explica por qué en esta ocasión esta táctica no convencional no ha funcionado.

Segundo, la instrumentalización de las migraciones no es sino la otra cara de la externalización del control migratorio y de la protección internacional a los estados vecinos. Al forzar a su vecindario a controlar las fronteras comunitarias y acoger aquellos refugiados que ya no están dispuestos a recibir, automáticamente la UE y los estados miembros se han puesto en sus manos. A cambio de control y contención, les ofrecieron incentivos, desde los fondos de ayuda al desarrollo hasta posibles acuerdos en materia comercial o de visados. Ahora son ellos los que quieren imponer sus condiciones. Aunque pocos quieran admitirlo, fueron la UE y los estados miembros quienes empezaron con la instrumentalización de las migraciones. Además, el cómo lo hicieron no es baladí.

En los últimos años, hemos visto como la UE ha recurrido a fórmulas cada vez más informales. Así, los acuerdos bilaterales han ido dando paso a otras formas de acuerdo más flexibles y *ad hoc*, que se insertan en marcos más amplios de cooperación. No es de extrañar que dichas negociaciones se hayan hecho sobre todo a nivel de los estados miembros y no tanto de la UE, que siempre precisa fórmulas mucho más estandardizadas. El resultado ha sido más flexibilidad y capacidad de negociación a cambio de menos transparencia. Esto no debería ir en detrimento del control necesario por parte de los poderes legislativos y judiciales de cada país y a nivel europeo. El mal llamado acuerdo entre la UE y Turquía de 2016, con el que se intentó contener las llegadas irregulares a Grecia, es el mejor ejemplo de los riesgos de esta informalidad: el Tribunal de Justicia de Luxemburgo se declaró incompetente para valorarlo al ser un pacto informal entre Turquía y los estados miembros.

ENTENDER LAS MIGRACIONES COMO AMENAZAS HÍBRIDAS ORQUESTADAS POR TERCEROS PAÍSES NO HA HECHO SINO PROPORCIONAR EL RELATO PERFECTO. AUNQUE LOS MIGRANTES SEAN PERCIBIDOS COMO VÍCTIMAS, SU PAPEL COMO ARMAS DE PRESIÓN EN MANOS DE LOS GOBIERNOS DE PAÍSES VECINOS LES CONVIERTE AL MISMO TIEMPO EN EL PRINCIPAL *ENEMIGO*.

Tercero y último, la UE cae víctima de sí misma cuando, por todo ello, está dispuesta a renunciar a sus propios fundamentos. Declararse en guerra ante la instrumentalización de las migraciones (entendidas como tácticas híbridas) por parte de los países vecinos es abrir la puerta a la excepción. A finales de 2021, Polonia decretó el estado de emergencia, con todo lo que esto implica en términos de suspensión de derechos fundamentales, uso ilimitado de la fuerza por parte del Ejército y militarización de amplias zonas sin acceso de la prensa ni de las ONGD. No es nuevo. También ha pasado en Grecia con las devoluciones en caliente, que vulneran de manera flagrante la legalidad y han sido una constante en los últimos años. En cada ocasión, el uso político de las migraciones por parte de terceros países se ha usado como justificación para limitar derechos fundamentales reconocidos por las legislaciones nacionales, europeas e internacionales.

Esta deriva no es solo propia de algunos países fronterizos. En diciembre 2021, la Comisión Europea publicó una propuesta de reglamento para dotar a los estados miembros de un marco legislativo para responder a tales situaciones. Según el documento, la instrumentalización de migrantes tendría lugar cuando «un tercer país instiga flujos migratorios irregulares hacia la Unión (…) con la intención de desestabilizar a la Unión o a un Estado miembro, y siempre que la naturaleza de tales acciones pueda poner en peligro funciones esenciales

del Estado, incluida su integridad territorial, el mantenimiento del orden público o la salvaguardia de su seguridad nacional». Las medidas propuestas pasan por limitar los puestos fronterizos, ampliar los plazos, aumentar las medidas de control migratorio y facilitar el retorno inmediato en las fronteras externas e internas de la UE. Tal y como han señalado numerosas organizaciones internacionales (ECRE, Amnistía Internacional, entre otras), tales medidas podrían normalizar el estado de excepción y socavar así los derechos fundamentales de migrantes, refugiados y solicitantes de asilo.

¿Cuáles son las consecuencias de considerar las migraciones como amenaza híbrida? En su libro *After Europe* (2017), Ivan Krastev señalaba que bien podría ser que las crisis migratorias, no por lo que son sino por lo que generan, acaben representando el inicio del fin del liberalismo europeo. Después de 2015, nuestro miedo a otra crisis migratoria ha hecho que estemos dispuestos a aceptar lo inaceptable. Y este es el verdadero problema. De puertas hacia dentro, podríamos acabar aceptando la normalización de los estados de excepción y, por lo tanto, la vulneración de derechos fundamentales. En este sentido, entender las migraciones como amenazas híbridas orquestadas por terceros países no ha hecho sino proporcionar el relato perfecto. Aunque los migrantes sean percibidos como víctimas, su papel como *armas* de presión en manos de los gobiernos de países vecinos les convierte al mismo tiempo en el principal *enemigo*. Da igual cuantos sean. En tanto que son percibidos como una amenaza a la seguridad nacional, más por lo que representan que por lo que son, nadie duda en que la respuesta debe ser lo más contundente posible.

De puertas hacia fuera, la instrumentalización de las migraciones, primero desde Europa y ahora desde el exterior, nos ha hecho rehenes (y, por lo tanto, mudos) ante las presiones de países terceros. Ahí es donde radica la principal sorpresa y temor. Esto, tal vez, es lo verdaderamente nuevo. Así, la asimetría del poder –o condicionalidad en palabras de Cassarino (2007)– se ha invertido: ahora son los países vecinos quienes imponen sus condiciones. Es consecuencia de que el número de llegadas irregulares dependa de ellos. El ejemplo más reciente de esta subordinación es el reconocimiento por parte del Gobierno español de la soberanía marroquí sobre el Sáhara Occidental. Cabe preguntarse hasta qué punto no era este el objetivo último de la cooperación marroquí. El problema añadido es que, en contextos regionales complejos, responder a las exigencias de unos puede implicar levantar las suspicacias de otros. Así es como la respuesta de Argelia al cambio de posición del Gobierno español no se ha hecho esperar. No solo es difícil decidir qué es lo primero – si Marruecos o Argelia, si las migraciones o el precio del gas–, sino que, además, las migraciones son fluidas y los que no lleguen por un lado acabarán llegando por otro.

Esto no quiere decir que no haya alternativa. La hay, pero para ello se deben cambiar las condiciones de base. Esto implica dejar de sobrerreaccionar en cada ocasión. La crisis de refugiados ucranianos es un buen ejemplo en este sentido. La alternativa pasa también por revertir el proceso de externalización del control migratorio, de manera que las migraciones dejen de ser moneda de cambio en las relaciones internacionales. Necesitamos una política exterior que no sea puramente transaccional, que no imponga los intereses de unos sobre otros y que trabaje en la consecución de objetivos comunes a medio y largo plazo. Necesitamos también unas políticas migratorias que aborden las causas y regulen los flujos, más allá de medidas de pura contención. Si no, estas políticas estarán siempre abocadas al fracaso, porque la contención solo reduce las llegadas en un momento y geografía determinados. Cuando los factores que empujan y atraen los flujos migratorios se mantienen, siempre se acaba encontrando un paso. Finalmente, la alternativa no puede ser la reducción de derechos para aquellos que a pesar de todo acaben llegando. Por dos razones fundamentales: porque el cumplimiento del estado de derecho es condición *sine qua non* de toda democracia; y porque la exclusión de hoy es el conflicto del mañana. Al contrario de lo que propugna la extrema derecha, «nuestra» seguridad depende de «sus» derechos.

Referencias

Cassarino, J.P. «Informalising Readmission Agreements in the EU Neighbourhood». *The International Spectator*, vol. 42, nº. 2 (2007), p.179-196. (en línea) [Fecha de consulta 09.08.2018] https://halshs.archives-ouvertes.fr/hal-01232695/document

Greenhill, Kelly M. *Weapons of Mass Migration: Forced Displacement, Coercion, and Foreign Policy*. Nueva York: Cornell University Press, 2010.

Krastev, Ivan. *After Europe*. Filadelfia: University of Pennsylvania Press, 2017.

CÓMO LAS DEMOCRACIAS PUEDEN SUPERAR LOS DESAFÍOS HÍBRIDOS Y LA DESINFORMACIÓN

La desinformación se ha convertido en una amenaza cotidiana para el mundo interconectado en el que vivimos, aunque sus efectos pueden ser infravalorados debido a la falta de instrumentos con los que medir su impacto. Uno de los problemas centrales de este desafío es, precisamente, que mientras nuestro mundo ha ido cambiando, muchas de las instituciones en cuya protección confiamos han permanecido inalteradas. Este artículo plantea cómo la noción de «democracia» puede sobrevivir en este nuevo mundo digital y formula recomendaciones sobre cómo las instituciones pueden adaptarse y crecer. Además, presenta nuevas ideas en torno a la medición de la desinformación, tanto respecto a su difusión como a su impacto.

John Kelly
Investigador invitado, The German Marshall Fund

CIDOB REPORT
08- 2022

La nueva guerra está en todas partes

En los últimos años, han aparecido nuevos términos para describir la sensación de conflicto permanente que se percibe en todo el mundo: guerra híbrida, guerra cibernética, zona gris, información errónea, desinformación, mala información, operaciones de influencia y agentes malintencionados; son sólo algunas de las expresiones que han ido ganando aceptación en el léxico sobre conflictos y que intentan definir esta nebulosa de distintas tipologías de confrontación entre estados que ha comenzado a ser norma en tiempos de paz. Son conceptos que, en su mayoría, se incluyen en la idea de *guerra híbrida*.

La paz, tal como la conocemos, se define como la ausencia de guerra. Al mismo tiempo, la guerra, en nuestra idea tradicional, es un conflicto cuya naturaleza es cinética, lo que supone ataques armados, envíos de tropas y confrontación bélica. En cambio, la guerra híbrida ha transformado

nuestra noción de la época de paz. Según la OTAN, los conflictos híbridos desdibujan la línea que separa la guerra de la paz, mientras aumenta la opacidad o la ambigüedad sobre el origen de posibles ataques híbridos mediante la fusión de instrumentos convencionales y no convencionales, difuminándose el umbral de la guerra (véase Bargués y Bourekba en este volumen).

Aunque no esté especificado en esos términos, el concepto de guerra híbrida es tan antiguo como las desgastadas páginas de Sunzi que, hace más de dos mil años, ya advirtió que las destrezas bélicas podían incluir la idea de someter «al enemigo sin darle batalla» (véase Arco Escriche en este volumen). Sin embargo, más allá de que este pasaje se interprete, mayoritariamente, como una defensa de que la política y otros medios deberían evitar la guerra, es evidente que la estrategia de declarar o alimentar un conflicto al margen de las batallas cinéticas ha persistido a lo largo del tiempo.

Timothy Snyder (2018), en su libro *El camino hacia la no libertad*, observó que el riesgo de definir una guerra como híbrida es que, en este caso, el conflicto, por su naturaleza no convencional y no cinética, puede percibirse como una «guerra menor» o algo menos que una guerra normal. En cambio, este autor sostiene que ese tipo de conflicto armado debería considerarse como una «guerra aumentada», puesto que crea un ambiente de confrontación permanente, incluso sin la presencia del elemento cinético.

Todas estas nociones de guerra híbrida muestran, en conjunto, sólidos elementos para empezar a precisar un concepto intencionadamente vago. Definida en términos sencillos, la guerra híbrida se podría considerar como la agresión de una entidad (sea un Estado o una facción) hacia otra a través del uso de herramientas de poder no cinéticas con el objetivo de crear un resultado estratégico. Sin embargo, todavía es necesario elaborar más este concepto para aprehender la totalidad de su alcance actual. En concreto, hay que profundizar en los factores que determinan cuándo un Estado se considera a sí mismo *en* una guerra híbrida, qué forma debería adoptar su respuesta, y si existen parámetros que propicien que el arte de gobernar de forma convencional o el ejercicio de poder entre estados se conviertan en una guerra híbrida.

La desinformación como amenaza

La guerra híbrida es como un pulpo en el que cada tentáculo representa una táctica de guerra nueva, no convencional. De todos ellos, el tentáculo más fuerte sería el uso de la información como arma de desestabilización: a medida que la guerra híbrida se ha ido haciendo más común,

ha aumentado notablemente la propagación de lo que se clasifica como información errónea, desinformación y mala información (MDM, por su sigla en inglés). Según la Agencia de Ciberseguridad y Seguridad de las Infraestructuras de Estados Unidos (CISA), aunque las diferencias entre estos términos sean sutiles, es fundamental entenderlas. Así, la *desinformación* sería la información creada deliberadamente para perjudicar o manipular a una persona, grupo social, organización o país; la *información errónea*, la información falsa elaborada sin la intención de hacer daño y, finalmente, la *mala información* el uso de información veraz fuera de contexto con la finalidad de engañar. La protagonista de estas tácticas híbridas es, sin duda, la desinformación.

La desinformación es una amenaza en auge surgida al amparo de unas plataformas digitales y redes sociales que han crecido prácticamente sin ningún tipo de control, dominando los flujos de información. No obstante, a medida que ha ido creciendo la desinformación, también lo han hecho las tácticas para cuantificarla y luchar contra ella, por lo que ya se pueden tomar medidas para mitigar los efectos de sus contenidos.

LA DESINFORMACIÓN ES UNA AMENAZA EN AUGE SURGIDA AL AMPARO DE UNAS PLATAFORMAS DIGITALES Y REDES SOCIALES QUE HAN CRECIDO PRÁCTICAMENTE SIN NINGÚN TIPO DE CONTROL, DOMINANDO LOS FLUJOS DE INFORMACIÓN. NO OBSTANTE, A MEDIDA QUE HA IDO CRECIENDO LA DESINFORMACIÓN, TAMBIÉN LO HAN HECHO LAS TÁCTICAS PARA CUANTIFICARLA Y LUCHAR CONTRA ELLA, POR LO QUE YA SE PUEDEN TOMAR MEDIDAS PARA MITIGAR LOS EFECTOS DE SUS CONTENIDOS.

Tradicionalmente, se ha identificado y considerado la desinformación poniendo el foco en la producción de contenido falso, en la cantidad de contenido creado «publicado, compartido o visualizado», o en indicadores tales como el número de *bots* que se pueden identificar en Twitter. Si bien estas medidas son eficaces para calcular el número de fuentes de desinformación, no miden el impacto del contenido –veraz, o no– diseminado. Aunque es importante considerar ambos indicadores, es crucial comprender la eficacia de estas campañas desinformativas.

En este ámbito de la producción de contenidos, la Unión Europea (UE) aprobó en abril de 2022 un nuevo paquete legislativo digital para reforzar la respuesta de la Unión a la desinformación: la Ley de Mercados Digitales (DMA, por sus siglas en inglés) y la Ley de Servicios Digitales (DSA, por sus

siglas en inglés), que incluyen un actualizado Código de Buenas Prácticas en materia de Desinformación cuyo objetivo es detener la propagación de la desinformación en las plataformas tecnológicas haciendo responsable al propietario de la plataforma (Meta, Twitter, etc.) de la difusión de contenido falso. Dicho Código aborda esta cuestión aumentando las obligaciones en materia de presentación de informes por parte de estos gigantes digitales sobre las acciones emprendidas para luchar contra la desinformación, exhortándoles a promover la verificación de datos y a aumentar la transparencia en la publicidad política, entre otras medidas. Las sanciones por no cumplir con estas normas caen dentro del ámbito de la DSA que, por primera vez, impone multas de hasta el 6% de los ingresos anuales a nivel global de estas empresas en caso de inacción.

Más allá de este esfuerzo por crear un marco normativo que ponga ciertos límites al fenómeno, avanzan también nuevas medidas analíticas para aumentar el conocimiento sobre cómo se propaga la desinformación, así como sus efectos sociales y políticos. Una propuesta eficaz para medir el impacto de las campañas desinformativas consiste en analizar si, a la larga, la desinformación conduce a la acción, o si el contenido se reproduce también más allá de la plataforma donde se origina. El analista Ben Nimmo (2020), en un estudio para la Brookings, propuso la creación de una «escala de disrupción» que midiese el impacto de una campaña de desinformación. Esta escala va del uno al seis, calculando si el contenido se origina en una única plataforma, si se mueve a través de diversas fuentes (ya sean redes sociales o medios de comunicación tradicionales), si es amplificada por celebridades o personajes conocidos y, finalmente, si llama a la acción, a la violencia o provoca respuestas políticas. Esta escala, usada juntamente con los indicadores identificativos de la fuente original de la desinformación, puede ayudar a los investigadores a entender el qué, el dónde, el quién y el cómo de la desinformación y sus tácticas para arraigarse y proliferarse. Sin embargo, todas estas mediciones son inútiles si, paralelamente, no se consigue restablecer la confianza en la democracia. La desinformación contribuye a la polarización y a la erosión institucional y de los procesos democráticos. Hay formas de luchar contra eso.

¿Cómo sobrevive la democracia a las amenazas híbridas?

La guerra híbrida y la desinformación debilitan los pilares sobre los cuales descansan nuestras democracias, violando los principios y los derechos sobre los cuales fueron fundadas. Sin duda, aunque ese es el objetivo de estas tácticas, estas amenazas se han vuelto tan complejas que dan lugar a una pregunta: ¿habrá que replantearse el concepto de democracia? La respues-

ta simple es no; sin embargo, será necesario que la democracia, sus instituciones y normativa sigan progresando para mantenerse relevantes en la era digital. De la misma forma que se interpretan los textos religiosos para los tiempos modernos, hay que interpretar y desarrollar las democracias para que sigan siendo entidades poderosas capaces de proteger a sus ciudadanos. En este sentido, referente a la regulación de la industria tecnológica, se pueden dar fácilmente pasos en varias direcciones para generar cambios desde este mismo momento.

Hasta 2014, el famoso mantra de Mark Zuckerberg para Facebook era el bien conocido «muévete rápido y rompe cosas». Esta frase, que significaba dar vía libre a los desarrolladores y directores de Facebook para probar, crear y fracasar, se convirtió en la lógica del Silicon Valley. Muchas empresas tecnológicas –como Uber y WeWork– fueron pioneras en el llamado capitalismo de plataforma con resultados dispares. Sin embargo, lo que faltó en el esfuerzo para «avanzar rápidamente y romper cosas» fue, a menudo, la vigilancia o la capacidad de anticiparse a los posibles usos indebidos de estas tecnologías. Así, si bien el mantra de Zuckerberg quizá haya tenido éxito en la industria tecnológica, su respuesta no ha podido ser más radicalmente opuesta en los lentos, metódicos y deliberativos ideales de la democracia. Desde el principio, las democracias se concibieron incorporando mecanismos de control, cuya finalidad era la moderación de sus acciones para adoptar decisiones bien fundadas al servicio de la ciudadanía. No pretendía ser un proceso rápido o disruptivo, por lo que, ante el desafío arrollador de una industria que puede crear tecnologías completamente nuevas en cuestión de días, la democracia se encuentra en una confrontación muy desigual.

Las democracias son tan relevantes hoy como cuando nació la primera democracia en Atenas hace más de 2.500 años. Sin embargo, muchas de ellas han seguido funcionando bajo las rigurosas pretensiones de sus documentos constitutivos, sin haberse actualizado para adaptarse a un mundo en constante cambio. En Estados Unidos, por ejemplo, la Constitución con la que se fundó el país fue concebida como una «Constitución viva», para poder irse actualizando a medida que el mundo evolucionaba. En la práctica, sin embargo, esto ha demostrado ser falso, tanto en Estados Unidos como en otros países. Tal como ya escribió Walter Lippmann en 1919, las democracias son influenciadas por la información de la que disponen, y estas deben esforzarse por «controlar su entorno» cuando trabajan en nuevos espacios informativos. Es facultad de las democracias progresar para controlar este nuevo entorno. Sin embargo, las democracias tienden a ser reactivas en lugar de proactivas, por lo que han tardado casi tres décadas en crear un marco que regule este nuevo mundo tecnológico.

En general, las democracias solo intervienen cuando una nueva esfera de influencia se vuelve peligrosa. Ello ocurrió en Estados Unidos, cuando la industria automovilística empezó a crecer sin limitaciones y se acabó creando la Administración Nacional de Seguridad del Tráfico en las Carreteras en 1970; o cuando la contaminación empezó a extenderse sin restricciones por todo el país y se estableció la Agencia de Protección Ambiental, también en 1970. En la actualidad, ante la capacidad disruptiva de la desinformación, amplificada por la industria tecnológica, ha llegado el momento de tomar medidas para eliminar riesgos. Mark Zuckerberg, el defensor original del moverse rápido y romper cosas (que posteriormente transformó en «muévete rápido con una infraestructura estable»), afirma que el Gobierno debe desempeñar un papel más activo en la regulación de Internet, y ha propuesto cuatro simples medidas que contribuirían a hacer de las redes sociales e Internet un lugar más seguro: a) la regulación de contenidos nocivos, b) la garantía de la integridad electoral, c) los controles de privacidad y c) la portabilidad de datos.

Por su parte, la UE está abriendo un camino en la creación de un entorno digital más seguro con las mencionadas DMA y DSA. La adopción, por parte de los principales aliados de la UE, de este marco legislativo garantizaría una regulación internacional coherente para prevenir «agujeros digitales» donde agentes maliciosos puedan operar. Asimismo, 61 países ya han firmado un documento titulado «Declaración sobre el futuro de internet», propuesto por la administración Biden, que establece una visión global de Internet en la que se protegen los derechos humanos, se modera la competencia, se asegura la infraestructura y se garantiza el acceso universal a la conectividad, entre otros temas (Engler, 2022). Este documento podría representar también un primer paso firme para alcanzar estos objetivos si los firmantes garantizasen el cumplimiento de las normas en cuestión y, sobre todo, si se consensuase este acuerdo como marco jurídico en lugar de su condición actual de documento no vinculante.

Como se ha mencionado, existen muchos caminos para hacer que las instituciones democráticas sobrevivan y se desarrollen en el entorno digital actual. En primer lugar, la existencia de unas definiciones más firmes de lo que es una guerra híbrida, junto con los parámetros que especifiquen qué significa *estar* en un conflicto híbrido, contribuirían a sortear los espacios grises que estas tácticas pretenden crear. En segundo lugar, el uso de datos para medir la eficacia de los actos dentro de un conflicto, como la difusión de la desinformación, nos puede ayudar a evaluar el riesgo y la reacción. Finalmente, la implementación de normas y reglamentos actualizados puede contribuir a proteger a la ciudadanía y brindar a las instituciones la libertad necesaria para trabajar dentro del nuevo contexto de amenazas. Las democracias fueron creadas para crecer y adaptarse: ha llegado el momento de que ello se lleve a cabo.

Referencias

Bilal, Arsalan. «Hybrid Warfare – New Threats, Complexity, And 'Trust' As the Antidote». *NATO Review* (30 de noviembre de 2021) (en línea) [Fecha de consulta: 6.7.2022] https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html

Sunzi. *El arte de la guerra,* Alianza editorial, 2022.

Snyder, Timothy. *El camino hacia la no libertad.* Barcelona: Galaxia Gutenberg, 2018.

Nimmo, Ben. «The Breakout Scale: Measuring the Impact Of Influence Operations». *Brookings Foreign Policy* (septiembre de 2020) (en línea) [Fecha de consulta: 6.7.2022] https://www.brookings.edu/wp-content/uploads/2020/09/Nimmo_influence_operations_PDF.pdf

Lippmann, Walter. «The Basic Problem of Democracy». *The Atlantic* (noviembre de 1919) (en línea) [Fecha de consulta: 6.7.2022] https://www.theatlantic.com/magazine/archive/1919/11/the-basic-problem-of-democracy/569095/

Engler, Alex. «The Declaration for the Future of the Internet is for Wavering Democracies, not China and Russia». *Brookings* (6 de mayo de 2022) (en línea) [Fecha de consulta: 6.7.2022] https://www.brookings.edu/blog/techtank/2022/05/09/the-declaration-for-the-future-of-the-internet-is-for-wavering-democracies-not-china-and-russia/

ATAQUES HÍBRIDOS A INFRAESTRUCTURAS CRÍTICAS

El ciberespacio es el último campo de batalla para explotar las vulnerabilidades conocidas y, sobre todo, desconocidas de un supuesto enemigo o rival. Las ciberarmas son programas informáticos maliciosos diseñados para atacar a un sistema ciberfísico esencial, con el objetivo de alterar su funcionamiento normal o destruirlo. Estos tipos de ataques contra una infraestructura crítica no requieren inversiones multimillonarias como la fabricación de armas de guerra convencionales, y su capacidad de réplica es muy efectiva. Pero, ¿cómo se producen? ¿Quién los genera y cómo se distribuyen? ¿A quién sirven? Y, ¿cómo podemos defendernos?

Manel Medina Llinàs
Director del Máster en Cybersecurity Management, UPC-School; coordinador de la Oficina Técnica de Formación de la Agència de Ciberseguretat de Catalunya

CIDOB REPORT
08- 2022

A los tradicionales campos de batalla –tierra, mar y aire–, hace unos años se añadió el espacio orbital, y hace poco que se habla ya del ciberespacio. En los escenarios tradicionales, las armas pueden verse desde aviones o satélites, y los estados y las grandes coaliciones como la OTAN tienen bien controladas las del otro bando. Pero las ciberarmas son casi intangibles y pueden cruzar una frontera, no ya en un microchip de memoria, sino a través de las redes de datos. Esto hace que sea difícil saber qué capacidad destructiva tiene nuestro contrincante en caso de ciberguerra.

Pero empecemos por saber qué es una *ciberarma*. Hasta hace menos de una década, se consideraba ciberarma cualquier programa informático malicioso, capaz de atacar a nuestro enemigo en cualquier momento. Para no ser descubierta e inutilizada antes del ataque, normalmente, la ofensiva se basaba en uno o varios métodos de explotación de una vulnerabilidad de algún pro-

grama instalado en los sistemas informáticos de la víctima, lo que se conoce como *vulnerabilidad de día cero* (*zero-day*). Los más puristas dicen que para ser considerada ciberarma, esta debe ser «destructiva», es decir, causar daños materiales a infraestructuras críticas y/o personas. Por tanto, estas ciberarmas las tenemos que buscar, escondidas en los llamados *sistemas ciberfísicos* o *Internet de las cosas* (IoT), como sistemas de control industrial (ICS), ferroviarios, telecomunicaciones, suministros esenciales (agua, luz, gas), o sanitarios, entre otros. Esta particularidad, y el hecho de que muchos de estos sistemas no estén adecuadamente actualizados, hace que incluso puedan ser atacados con vulnerabilidades conocidas.

Una amenaza asequible y persistente

Muchas ciberarmas pretenden permanecer ocultas, imperceptibles, esperando la orden de destruir el objetivo. Se trata de la llamada «amenaza persistente avanzada» (APT, por sus siglas en inglés). En muchos casos, además, es difícil identificar al equipo desarrollador; pero, entre los más potentes, figuran divisiones o compañías del ejército o unidades de ciberinteligencia de gobiernos. Aunque, como ocurre con las armas físicas, también hay fabricantes de ciberarmas y organizaciones criminales que las venden en mercados más o menos ocultos. Recientemente ha irrumpido en el debate público y mediático la empresa israelí NSO, que vende sus ciberarmas a estados, como el *software* espía Pegasus, teóricamente diseñado para apoyar la lucha antiterrorista. Las ciberarmas no debemos buscarlas solo en la ciberguerra, sino también en herramientas de vigilancia, identificación biométrica, etc., con impacto en la cadena de suministro y, potencialmente, recopilando datos de usuarios y ciudadanos.

Las ciberamenazas son más «asequibles», no requieren inversiones multimillonarias como la fabricación de artefactos o armas de guerra. Descubrir nuevas vulnerabilidades y desarrollar nuevas herramientas de explotación de estas es mucho más barato y, sobre todo, es replicable centenares o millares de veces sin apenas coste adicional. Por lo tanto, las pueden desarrollar organizaciones «grises», que las comercializan tanto a gobiernos, de forma abierta, como a grupos criminales, de forma oculta.

Pero el catálogo de las ciberarmas incluye, además, un instrumento, en apariencia, menos belicoso: la desinformación, que puede ser empleada también para atacar a infraestructuras críticas. Llegando a través de los canales de información convencionales (redes sociales, medios de comunicación, etc.), la desinformación se dirige, de manera selectiva, a las personas que tienen capacidad de gestión de la infraestructura, y puede ser complementada con el ciber(contra)espionaje. Los *softwares* espía empleados por los

departamentos de inteligencia también pueden ser atacados, y generar informaciones falsas al enemigo que nos espía, incitándole a tomar decisiones que le pueden llevar a una trampa de difícil salida, bloqueando la infraestructura o perdiendo su control. Sin embargo, la desinformación más habitual en entornos ciberfísicos, como forma de ataque, consiste en alterar los datos que proporcionan los sensores de sistemas físicos. La intención es provocar decisiones de reacción equivocadas por los propios sistemas de gestión de la infraestructura, intentando, por ejemplo, corregir un problema inexistente, con lo que se estará creando otro en sentido contrario, que no será detectado. Esto sucedió en el ataque Stuxnet, en el que un virus (ciberarma) destruyó las centrifugadoras de uranio iraníes, modificando los datos de las revoluciones por minuto registrados por unos que mostrasen normalidad, para evitar ser detectado. Esta modificación de los datos de los sensores se puede realizar de diversas formas: a) reemplazando un sensor por otro engañoso, o introduciendo uno fraudulento, b) modificando su *software* para que proporcione lecturas falsas, o c) modificando los datos en el servicio de almacenamiento de estos (en un servidor o en la nube). Si la transmisión, el almacenamiento o el procesado de los datos no están adecuadamente protegidos, es muy fácil alterarlos sin ser advertidos, hasta que el daño sea irreparable o inevitable.

LAS CIBERARMAS PUEDEN ESTAR ESCONDIDAS EN CUALQUIER SITIO: UN CHIP, UN PROGRAMA, UNA TARJETA DE MEMORIA, O ALMACENADAS EN LA NUBE. UNA CIBERARMA ESTÁ FORMADA POR BITS, QUE SE PUEDEN OCULTAR DE CUALQUIER MANERA Y SON INDETECTABLES; PUEDEN ESTAR LATENTES DURANTE AÑOS EN UNA CENTRAL DE PRODUCCIÓN DE ENERGÍA O EN UN CENTRO DE CONTROL DE TRÁFICO FERROVIARIO O AÉREO, O EN EL DESPACHO DE UN GOBERNANTE O DIRECTIVO, SIN QUE NADIE SE DÉ CUENTA.

Las ciberarmas pueden estar escondidas en cualquier sitio: un chip, un programa, una tarjeta de memoria, o almacenadas en la nube. Una ciberarma está formada por bits, que se pueden ocultar de cualquier manera y, por lo tanto, son indetectables; pueden estar latentes durante años en una central de producción de energía o en un centro de control de tráfico ferroviario o aéreo, o en el despacho de un gobernante o directivo, sin que nadie se dé cuenta, como de hecho ya denunció el informe Mandiant en 2014. Esta investigación desveló decenas de organizaciones que habían sido infiltradas por el equipo de desarrollo de programas informáticos de ciberespionaje chino APT1 y en las que estas ciberarmas se habían mantenido ocultas una media de 229 días, llegando en algunos casos a estar instaladas varios años.

En una ciberguerra, se invaden los ordenadores o dispositivos de control de las infraestructuras de un país, pero ello no se sabrá hasta que alguien «pulse un botón» y despierte a los agentes (programas maliciosos) dormidos en sus madrigueras, y estos empiecen a actuar, deteniendo las infraestructuras que permitan el funcionamiento del país.

La guerra híbrida es una guerra con una capa adicional de operaciones remotas. A diferencia de las guerras convencionales, en las que el ejército invasor puede verse en las calles, los preparativos de un ciberataque son imperceptibles, porque no hay movimientos de tropas en la frontera. En el ciberespacio no hay fronteras.

El peligro de la proliferación de ciberarmas

Una vez vistos el escenario y las armas, vamos a ver los peligros a los que nos enfrentan estas nuevas amenazas cibernéticas y los factores que las hacen atractivas y peligrosas.

La ciberguerra «está servida»: las ciberarmas están siendo desplegadas por Internet frente a nuestros ojos, aunque estos no puedan verlas. Armas más potentes que un lanzamisiles o un tanque se comercializan inadvertidamente para la mayoría de los ciudadanos y también de los países, porque son tan solo «bits de datos». Como con las armas tradicionales, existen compras «legales», realizadas por gobiernos, y otras «ilegales», llevadas a cabo por particulares o grupos criminales con interés en espiar a un enemigo comercial o estratégico, para suplantarle y tomar el control de la infraestructura, o destruirla, como hizo BlackEnergy, que desconectó y destruyó los programas de control de las plantas de producción de energía eléctrica ucranianas el 23 de diciembre de 2015.

Las ciberarmas pueden ser producidas por cibermafias, por unidades cibernéticas de ejércitos convencionales, o por empresas al servicio de gobiernos. Lo que preocupa a los gobernantes es que diseñar y construir una ciberarma está al alcance de cualquier pequeño país u organización, ya que su producción no requiere materias primas, disponibles en los mercados, pero que son más caras. La guerra híbrida es preferible a la tradicional porque es más rentable. Rusia y otros países europeos distribuyen este tipo de ciberarmas, muchas veces producidas en proyectos de colaboración público-privada. Los gobiernos y las grandes organizaciones multinacionales generan las herramientas, y la cadena de suministro no ha sido analizada todavía.

Cuando se produzca un ciberataque híbrido, no sabremos quién lo ha ordenado, quién lo ha perpetrado o cuándo empezó su preparación. En al-

gunos casos, su autoría puede ser muy evidente; por ejemplo, a raíz de la presentación en la Berlinale de 2016 del documental Zero Days, sobre el ataque Stuxnet, se denunció la coordinación entre Estados Unidos e Israel –aunque ellos no lo han reconocido– del ciberataque (mencionado anteriormente) para destruir las centrifugadoras de enriquecimiento de uranio iraníes. En otros casos, la determinación de la autoría es más difícil. Recientemente, la guerra de Ucrania también se está librando en el ciberespacio, y Moscú y Kíev se han acusado mutuamente de ataques de falsa bandera. Por ejemplo, en los ataques a servicios web gubernamentales ucranianos en enero de 2022, los atacantes dejaron pistas falsas incriminando a disidentes ucranianos y polacos, para desviar la atención de Rusia como atacante. Por ello, establecer el origen del ataque es esencial.

Para identificar el autor de un ciberataque, hay que analizar el código de la ciberarma en busca de comentarios o nombres que puedan indicar el país o el idioma empleado por el desarrollador. Pero este puede conocer dicha técnica y dejar pistas falsas en el idioma del contrincante al que pretende suplantar con un ataque de falsa bandera. Para complicarlo aún más, aunque el desarrollador no haya intentado ocultar su identidad o ideología, el atacante real puede ser diferente de quien ha desarrollado la herramienta de explotación, si esta se distribuye en el mercado soterrado. Otra técnica de detección es mirar la procedencia del ataque, aunque los indicios tampoco son concluyentes, ya que se pueden usar servidores intermedios que oculten el origen de la agresión como los de la red Tor[1]. Todo lo comentado hasta ahora abre multitud de posibilidades de injerencia a varios niveles, y requiere el despliegue de estrategias de defensa basadas en «desconfiar de todo».

LAS CIBERARMAS PUEDEN SER PRODUCIDAS POR CIBERMAFIAS, POR UNIDADES CIBERNÉTICAS DE EJÉRCITOS CONVENCIONALES, O POR EMPRESAS AL SERVICIO DE GOBIERNOS.

Estrategias de defensa frente a ataques híbridos

Podemos distinguir dos grandes tipos de ataques híbridos: a) los que afectan a la (des)información, con el objetivo de provocar decisiones incorrectas, y b) los que afectan directamente a sistemas físicos.

1. La red Tor está formada por multitud de servidores en todo el mundo, que se pueden ir encadenando para evitar que se pueda detectar el origen real de una conexión.

Si empezamos a analizar las actividades de desinformación como las noticias falsas que circulan por la red e influyen en las percepciones y opiniones públicas, podemos concluir que su efectividad en la desestabilización social puede ser más eficaz incluso que los ataques a bases de datos de control de una infraestructura. La desinformación puede producir violencia, y es otra forma de iniciar conflictos o ataques a infraestructuras.

Las estrategias de ataques de desinformación se basan en la creación y posterior distribución de noticias a través de redes de usuarios influyentes o falsos (bot social), para aumentar su difusión entre burbujas de usuarios afines. La defensa frente a este tipo de ataques es la identificación y el bloqueo de los agentes distribuidores de noticias falsas, pero los administradores de las redes sociales no siempre están dispuestos a colaborar, dados los beneficios de publicidad que pueden proporcionar las campañas de difusión de este tipo de noticias. Por otro lado, los ataques híbridos más directos a infraestructuras críticas provenientes del ciberespacio plantean el problema de la falta de experiencia de los responsables de seguridad física, la falta de colaboración de los empleados, y la incredulidad de los directivos para concebir, planificar e implantar las medidas de ciberprotección adecuadas.

Los países de la OTAN, a pesar de haber declarado su predisposición a reaccionar a ciberataques en julio de 2021, no están tomando en consideración las actividades de Rusia respecto a ataques híbridos. Por ejemplo, la interrupción del servicio del gaseoducto más importante de Estados Unidos –Colonial Pipeline– o los ataques a través de suministradores de infraestructuras con el procedimiento SolarWinds, en 2020, o ataques de Ransomware generalizados a otros países de la OTAN, han sido orquestados por Rusia, directamente o a través de cibermercenarios, pero la Alianza Atlántica sigue sin reaccionar. Tal vez una de las razones sea la nueva Directiva NIS2 de la Unión Europea, donde se describe cómo enfrentarse a los ciberataques, aunque esta directiva diferencia claramente entre servicios críticos y esenciales[2], y se incide en que solo estos últimos se consideran objeto de defensa.

2. Los servicios críticos son aquellos que permiten un funcionamiento normal de la sociedad, pero cuya falta no paraliza totalmente sus actividades. Por ejemplo, el transporte público se podría sustituir por un sistema de vehículos compartidos, como sucedió en algunos países durante el confinamiento más duro de la pandemia, para trasladar a personal sanitario. Los servicios esenciales son aquellos sin los cuales la sociedad no funciona, como la electricidad o las telecomunicaciones.

En definitiva, los gobiernos están tomando medidas administrativas y legales para incentivar la ciberprotección, especialmente en sus infraestructuras esenciales y críticas, y no solo en estas, sino también en las de sus proveedores, y en toda su cadena de suministro de componentes fundamentales para el servicio. Los gestores de estas infraestructuras deberán identificar los servicios y activos más valiosos y los más vulnerables, para protegerlos de la forma más eficiente posible. Y, finalmente, también se tendrá que planificar el mantenimiento operativo de los mecanismos de protección instalados y formar adecuadamente a todo el personal implicado. De ello dependerá el funcionamiento de un país. Si la reconstrucción después de un ciberataque generalizado (ciberguerra) puede ser relativamente rápida, un ataque híbrido puede ser más complicado de recuperar, sobre todo si el daño causado a la infraestructura es irreparable y se debe reconstruir con componentes caros o difíciles de encontrar en el mercado.

Referencia

McWhorter, Dan. «APT1: Exposing One of China's Cyber Espionage Units». *The Mandiant Intelligence Center* (2021) (en línea) https://www.mandiant.com/resources/apt1-exposing-one-of-chinas-cyber-espionage-units

RESILIENCIA HÍBRIDA EN ÉPOCAS INCIERTAS: LA GUERRA DE RUSIA Y LA SOCIEDAD UCRANIANA

Se pueden extraer dos conclusiones respecto a la guerra actualmente en curso en Ucrania: por un lado, se sobrevaloraron las capacidades de Rusia para librar una guerra híbrida y la mayoría de los componentes no militares del poder ruso se revelaron deficientes; por el otro, se subestimó la magnitud y el alcance de la capacidad de resistencia de los ucranianos ante la agresión. Esta resistencia se vertebra a partir de una combinación de numerosas formas y prácticas de resiliencia como característica social de autosuficiencia, autonomía y autoorganización, que difieren de una gestión vertical de la respuesta a una emergencia. Se trata de una «resiliencia híbrida» que se basa en una forma de gobernanza descentralizada, en la sostenibilidad de las redes sociales, en una política informativa fiable y en una firme adhesión pública a la idea de una «guerra justa».

Yulia Kurnyshova
Investigadora posdoctoral, Austrian Institute for International Affairs

Andrey Makarychev
Investigador asociado, CIDOB; profesor de Ciencias Políticas, Universidad de Tartu (Estonia)

CIDOB REPORT
08- 2022

Aunque, desde 2014, Moscú ha tratado de integrar herramientas híbridas en su política contra Ucrania, la invasión militar de Ucrania ha terminado siendo un tipo de guerra más bien convencional, cuyo objetivo es la destrucción física de las infraestructuras ucranianas tanto militares como no militares, en lugar de diversificar las herramientas estratégicas para minimizar el componente de poder duro en la estrategia general rusa. Los dos elementos principales del concepto de guerra híbrida –«guerra no lineal» y «control reflexivo»– fueron integrados en la fase inicial del conflicto, cuando Rusia se anexionó Crimea y se declaró la guerra en el Dombás por intermedio de terceros. Sin embargo, dichas estrategias parece que se han desvanecido en 2022. El Kremlin no ha logrado usar de una forma efectiva el poder institucional y comunicativo;

su propaganda de guerra tiene una influencia limitada en el espacio de información occidental; y sus ciberataques no han conseguido un cambio de juego, habiendo sido el poder blando destruido por la brutalidad de la invasión.

Al mismo tiempo, se ha subestimado la magnitud y el alcance de la resiliencia de la población en Ucrania. Este país, al que Occidente frecuentemente ha considerado como de la periferia, dependiente de Rusia y débil, que no opuso mucha resistencia a la anexión de Crimea y la ocupación del Dombás en 2014, ha recuperado su subjetividad a través de la capacidad para sobrevivir y reaccionar contra un invasor que dispone de más recursos. Al respecto, este artículo sostiene que es la resiliencia híbrida el punto esencial de la supervivencia de Ucrania como nación, a través de la subjetividad política y la acción de su sociedad civil, y destaca los componentes clave del modelo ucraniano de resiliencia.

Resiliencia: genealogía del concepto

La literatura existente generalmente considera la resiliencia como un proceso de adaptación de la sociedad a sacudidas complejas. En términos generales, la resiliencia implica adaptación, colaboración y autosuficiencia de individuos y comunidades. En este sentido, se «traslada la responsabilidad a las comunidades y se promueve el autogobierno reflexivo a través de estrategias de sensibilización, gestión del riesgo y adaptabilidad» (Humbert y Joseph, 2019: 216); «las personas resilientes no quieren que los gobiernos garanticen y mejoren su bienestar porque han sido instruidas para creer en la necesidad de garantizarlo y mejorarlo por sí mismas» (Reid, 2018: 648); por consiguiente, individuos y grupos son, en última instancia, responsables de su propia adaptabilidad frente a las transgresiones externas, entre ellas, las intervenciones extranjeras.

No obstante, refutamos la opinión de los autores que creen que en tiempos excepcionales la resiliencia «desincentiva la ciudadanía activa» e incluso pone «en peligro el concepto de espacio público» (Juntunen y Hyvönen, 2014: 196). Por el contrario, la experiencia ucraniana demuestra que la resiliencia es profundamente política, ya que «tiene por objeto capacitar a las personas para que sean los agentes de su propia reducción de vulnerabilidad con la finalidad de tomar las decisiones adecuadas y evitar una mala adaptación a un entorno nuevo» (Grove, 2014: 244). Por lo tanto, las prácticas cotidianas de resiliencia «crean sujetos» (Cavelty *et al*., 2015: 9): las organizaciones de la sociedad civil, los grupos de base y las redes son fuentes esenciales para una estrategia de supervivencia y seguridad humana.

Resiliencia híbrida: la experiencia ucraniana

Los datos sociológicos de una encuesta reciente indican un alto nivel de resiliencia entre la población ucraniana: 3,9 puntos sobre un máximo de 5. En esta clasificación, la resiliencia se compone de dos indicadores: salud física y bienestar y confort psicológico, incluyendo el interés por la vida, el sentimiento de utilidad, la capacidad para tomar decisiones y planificar el futuro, así como la ausencia de remordimiento por el pasado. Sin embargo, este artículo considera la resiliencia desde una perspectiva más amplia y destaca seis características esenciales que convierten la experiencia de la resiliencia ucraniana durante la guerra en un fenómeno híbrido.

LAS INSTITUCIONES PÚBLICAS UCRANIANAS HAN SEGUIDO FUNCIONANDO EN GRAN MEDIDA DURANTE LA GUERRA EN CURSO, INCLUSO EN LAS REGIONES MÁS AFECTADAS POR LAS ACTIVIDADES MILITARES DE RUSIA. SU RESILIENCIA NO HABRÍA SIDO POSIBLE SIN LA AYUDA PROLONGADA DE LA UE, INCLUIDA LA TRANSFERENCIA A UCRANIA DE LAS PRÁCTICAS EUROPEAS DE BUENA GOBERNANZA.

En primer lugar, la necesidad de resiliencia surgió del sentimiento de vulnerabilidad frente a la agresión rusa, que los dirigentes del país tradujeron en una visión de autonomía. La guerra en Ucrania no empezó el 24 de febrero de 2022, sino en 2014, con la anexión de Crimea y el inicio de la infiltración militar rusa en el Dombás. Después de luchar por Ilovaisk, el aeropuerto de Donetsk y Debaltseve en 2014, Ucrania comprendió su debilidad, lo que creó una especie de trauma colectivo que fue aún más doloroso debido a la lentitud de los países occidentales en introducir fuertes sanciones punitivas contra Rusia. Las restricciones impuestas no lograron detener la guerra en el Dombás ni impedir futuras ofensivas del Kremlin, pero entretanto han alimentado un sentimiento de frustración hacia los aliados occidentales en Ucrania. La Unión Europea (UE) acogió favorablemente las «aspiraciones europeas» de Ucrania, pero sin claras perspectivas de una integración plena, planteando interrogantes entre los ucranianos sobre la fórmula de asociación más viable y el escenario de integración europea más plausible.

Volodímir Zelenski ganó la presidencia porque consiguió captar mejor esos sentimientos generalizados que su predecesor Petro Poroshenko. Tras afirmar que Ucrania, en su calidad de «país europeo, empieza con cada uno de nosotros», Zelenski abordó las cuestiones de los valores y la reforma de po-

líticas sin considerar a la UE como el principal punto de referencia. Poniendo mucho menos énfasis en cuestiones de identidad étnica y lingüística, causantes de divisiones, el pragmático programa del presidente recibió un amplio apoyo en todo el país, ya que captó claramente la demanda pública de autosuficiencia y resiliencia.

En segundo lugar, las instituciones públicas ucranianas han seguido funcionando en gran medida durante la guerra en curso, incluso en las regiones más afectadas por las actividades militares de Rusia. Su resiliencia no habría sido posible sin la ayuda prolongada de la UE, incluida la transferencia a Ucrania de las prácticas europeas de buena gobernanza. La descentralización y las reformas de autogobierno han sido elementos fundamentales del compromiso de Ucrania con los agentes políticos y sociales extranjeros (organizaciones no gubernamentales y educativas, centros de estudio y medios de comunicación), que han tenido un impacto visible en los responsables de la toma de decisiones ucranianos. En particular, la pandemia de la COVID-19 ha fortalecido de forma sustancial la preparación de Ucrania ante futuros problemas, incluida la creciente habilidad de las autoridades públicas a nivel regional y municipal para desempeñar sus funciones a distancia bajo las estrictas condiciones de supervisión y control.

LAS REDES SOCIALES Y LA SOCIEDAD CIVIL HAN SIDO ESENCIALES PARA LA RESILIENCIA A NIVEL LOCAL. EN LAS FASES INICIALES DE LA INVASIÓN RUSA HUBO UNA FUERTE DEPENDENCIA DE LAS ONG Y LOS ORGANISMOS NOVELES DE SOCORRO, COMO LOS VOLUNTARIOS, EN LUGAR DEL GOBIERNO CENTRAL. ADEMÁS, LAS ONG UCRANIANAS A MENUDO HAN SUSTITUIDO A LAS ORGANIZACIONES INTERNACIONALES Y HAN SUMINISTRADO AYUDA A LAS CIUDADES ASEDIADAS O FACILITADO LA EVACUACIÓN DE CIVILES.

En tercer lugar, la guerra mostró mecanismos mediante los cuales el capital social y las redes familiares se vuelven elementos útiles para una resiliencia híbrida. Estos mecanismos incluyen la eliminación de los obstáculos a la acción colectiva, así como la creación de garantías informales y apoyo mutuo. Los vínculos entre parientes, vecinos y comunidades sirven como motor esencial de creación de resiliencia y, según una encuesta, el 94% de las personas encuestadas afirma tener relaciones pacíficas con sus familiares, el 89% con los vecinos y el 67% con los desconocidos. Los miembros de familias extendidas de las regiones devastadas por la guerra han encontrado refugio en la parte occidental de Ucrania. Los barrios donde los residentes podían confiar en la ayuda y asistencia mu-

tua pudieron superar mejor los problemas comunes (como los saqueos), y la probabilidad de que las personas desplazadas regresaran en algún momento a sus hogares era mayor. Estas prácticas de resiliencia de base son componentes importantes del desarrollo de Ucrania como sociedad abierta, moderna e interconectada, en la que la clase media ya ha demostrado ser capaz de asumir una responsabilidad social y económica, tanto en crisis anteriores, incluida la revolución del Maidán, como actualmente en la guerra con Rusia.

En cuarto lugar, las redes sociales y la sociedad civil han sido esenciales para la resiliencia a nivel local. En las fases iniciales de la invasión rusa, hubo una fuerte dependencia de las ONG y los organismos noveles de socorro, como los voluntarios, en lugar del Gobierno central. Además, las ONG ucranianas a menudo han sustituido a las organizaciones internacionales y han suministrado ayuda a las ciudades asediadas o facilitado la evacuación de civiles. La mayoría de ONG nacionales y locales, redes religiosas, organizaciones de la sociedad civil y un número considerable de redes de voluntarios de reciente creación están proporcionando ayuda humanitaria vital en la mayoría de las ciudades afectadas por la guerra.

En quinto lugar, también la resiliencia informativa es importante. El hecho de que la invasión a gran escala rusa fuera precedida por una guerra híbrida ha ayudado a Ucrania a adquirir cierta experiencia en contrarrestar la propaganda rusa. Antes de la guerra, los medios de comunicación ucranianos se caracterizaban por su diversidad y pluralismo de opiniones y, a diferencia de Rusia, desde la invasión a gran escala Ucrania no ha introducido la censura militar, aunque a veces la cobertura adolece de un optimismo excesivo. Los medios digitales gratuitos crean oportunidades para que los voluntarios, los defensores de los derechos humanos y los periodistas registren los crímenes de guerra. El elevado nivel de apoyo emocional a Ucrania en muchos medios de comunicación occidentales –y la simbólica identificación con el país– constituye una fuerza movilizadora adicional para la resistencia doméstica.

En sexto lugar, las dimensiones ética y valórica de la resiliencia son de la máxima importancia: la diferencia fundamental es que Ucrania está librando una guerra de legítima defensa (para su supervivencia y su futuro), mientras que Rusia está librando una guerra de agresión (de expansión y recuperación del pasado). Para Ucrania, se trata ante todo de una guerra justa de liberación, que moviliza y une la nación en aras de la defensa de la independencia del país. Para Rusia, se trata de una guerra neoimperialista encaminada a restablecer el imperio de antaño, basada en las ideas de zonas de influencias y gestión de gran potencia.

El papel de la UE

La UE ha desempeñado un papel esencial en los seis factores mencionados que contribuyen a la resiliencia híbrida de Ucrania tras el reinicio de la guerra en febrero de 2022. Esto no es sorprendente, dado que fue en gran medida la UE la que produjo y promovió discursos y prácticas de resiliencia hacia las zonas próximas del este y del sur del país. Desde 2014, los programas de asistencia de Occidente han desempeñado un papel decisivo en la facilitación de las reformas en Ucrania y en la creación de condiciones favorables para la integración económica y social. El Acuerdo de Asociación UE-Ucrania concertado en 2014 es el más amplio de la UE con un país tercero. Ucrania ha recibido 14.000 millones de euros de fondos europeos, un nivel de apoyo financiero sin precedentes, que contribuyó de manera importante a la reificación de las prácticas de resiliencia, definida por la Unión en su Estrategia Global, como la capacidad de «los estados y las sociedades para reformarse, así como para resistir y recuperarse de crisis internas y externas».

El 18 de marzo de 2020, la Comisión Europea presentó la «Política de la Asociación Oriental más allá de 2020. Reforzar la resiliencia: una Asociación Oriental eficaz para todos», que destacaba los resultados positivos obtenidos en tres de las cuatro esferas prioritarias (fortalecimiento de la economía, fortalecimiento de la conectividad, fortalecimiento de la sociedad) en el plan de trabajo «Veinte resultados para 2020». Con respecto a la esfera prioritaria del fortalecimiento de la gobernanza, el documento abogaba por la necesidad de mejorar significativamente los resultados en la esfera de la gobernanza relacionada con la lucha contra la corrupción y el empoderamiento de la sociedad civil. La descentralización y las reformas de autogobierno en Ucrania han sido dos de los pilares de este proceso. Además, la asistencia de la UE ha contribuido decisivamente al apoyo a la sociedad civil, a la libertad de prensa y al activismo de base en Ucrania. Si la UE sigue priorizando el fortalecimiento de la resiliencia facilitando la responsabilidad local y una participación comunitaria que incluya toda la sociedad, Ucrania emprenderá el camino correcto para una rápida recuperación, después del conflicto, basada en las normas y valores europeos de democracia, transparencia y buena gobernanza.

La resiliencia se ha convertido en el eje vertebrador para una nueva subjetividad ucraniana en Europa como nación capaz de luchar no sólo por su propia independencia e integridad territorial, sino también por la seguridad europea en un contexto más amplio.

Referencias

Cavelty, Myriam Dunn; Mareile Kaufmann y Kristian Søby Kristensen. «Resilience and (in)security: Practices, subjects, temporalities». *Security Dialogue*, vol. 46, nº. 1, p. 3-14 (2015).

Grove, Kevin. «Agency, affect, and the immunological politics of disaster resilience». *Environment and Planning D: Society and Space*, nº. 32 (2014), p. 240-256.

Humbert, Clemence y Jonathan Joseph. «Introduction: the politics of resilience: problematising current approaches». *Resilience*, vol. 7, nº. 3 (2019), p. 215–223.

Juntunen, Tapio y Ari-Elmeri Hyvönen. «Resilience, Security, and the Politics of Processes». *Resilience: International Policies, Practices, and Discourses*, vol. 2, nº. 3 (2014), p. 195-209.

Reid, Julian. «Neoliberalism, Development and Resilience». En: Konings, Martijn; Primrose, David; Cahill, Damien y Cooper, Melinda. *The SAGE Handbook on Neoliberalism*. Londres: SAGE publishing , 2018.

LAS ESTRATEGIAS DE LA OTAN EN RESPUESTA A LOS CONFLICTOS HÍBRIDOS

La Organización del Tratado del Atlántico Norte (OTAN) tiene una larga relación con lo híbrido. Mientras que, inicialmente, la Alianza Atlántica vinculó lo híbrido con una forma de lucha que integraba elementos convencionales e irregulares, la actual concepción se basa en el empleo coordinado y sincronizado de distintos resortes de poder bajo el umbral del conflicto. Lo híbrido se ha consolidado como una amenaza para la seguridad aliada. El Concepto Estratégico aprobado en la Cumbre de Madrid de junio de 2022 alerta del empleo de amenazas híbridas por parte de China o Rusia y sus efectos, hasta el punto de poder motivar la invocación del Artículo 5 del Tratado de Washington.

Guillem Colom Piella
Profesor titular de Ciencia Política, Universidad Pablo de Olavide (Sevilla)

CIDOB REPORT
08- 2022

Los orígenes

Influida por la popularidad que estaba consiguiendo entre la comunidad estratégica estadounidense tras la guerra entre Israel y Hezbolá de 2006 y el nombramiento del general James Mattis como jefe del Mando Aliado de Transformación, la OTAN empezó a interesarse por la guerra híbrida en 2007. Entendiendo que esta forma de combatir «en la que los adversarios integrarán operacional y tácticamente medios convencionales, irregulares, terroristas y criminales» (OTAN, 2009: 55) caracterizaría las guerras del siglo XXI, se hacía necesario adaptar los medios y capacidades aliados para operar efectivamente en estos ambientes más ambiguos y difusos. En este sentido, no parece extraño que lo híbrido se integrara en la doceava revisión del planeamiento de capacidades, se introdujera en las campañas de experimentación militar, o constituyera una de las recomendaciones del Proyecto de Futuros Múltiples para orientar la transformación aliada a largo plazo.

Aunque en 2010 los mandos militares de la OTAN (2010b) publicaron un concepto básico para clarificar el término y orientar este desarrollo de capacidades, lo híbrido continuaba siendo algo restringido al ámbito militar. Ello explicaría porque, a pesar de que el «informe Albright» mencionó una vez lo híbrido (ibídem, 2010a), el Concepto Estratégico de 2010 no lo incluyó. En cambio, sí mencionó otros riesgos como el terrorismo, el extremismo, la criminalidad transnacional o los ciberataques, que habían adquirido un enorme protagonismo tras los disturbios y saqueos de Estonia de 2007 y que acabarían estrechamente vinculados con lo híbrido. La Cumbre de Chicago de 2012 tampoco mencionó esta amenaza.

A pesar del interés militar que generaba lo híbrido, no existía ningún consenso sobre el concepto. De hecho, los documentos de esta organización utilizaban indistintamente guerra, amenaza, estrategia o táctica para referirse a la complejidad de los conflictos del siglo XXI. Unos conflictos para los que una organización político-militar como la OTAN no estaba preparada y que debían abordarse desde un enfoque integral que incrementara la coherencia entre las acciones militares aliadas y las labores civiles de otros actores en operaciones de gestión de crisis. En efecto, para muchos, la intervención en Libia (2011) podría ser un ejemplo de estos conflictos ajenos a la dicotomía regular-irregular (con fuerzas gubernamentales, guerrilleros y mercenarios operando en frentes ambiguos), y cuya resolución satisfactoria solo podría alcanzarse mediante un «Enfoque Integral» con mejores instrumentos de gestión de crisis y mayor capacidad para prestar apoyo militar a la estabilización y reconstrucción posconflicto.

La eclosión de lo híbrido

Fue necesario esperar hasta la anexión rusa de Crimea (2014) para que lo híbrido se popularizara entre la clase política y la opinión pública aliada. En esa península, unidades militares no marcadas y actores locales tomaron el terreno bajo la atónita mirada de la comunidad internacional. Explotando los clivajes sociopolíticos de la región y lanzando una campaña multicanal de desinformación dentro y fuera de Ucrania, Moscú fue capaz de ocultar sus objetivos y negar de manera plausible su responsabilidad hasta haber consumado la invasión. La intervención rusa en el Donbas (2014-) ratificaría esta difuminación de la frontera entre la paz y la guerra por una amplia zona gris donde la desinformación y los ciberataques tendrían su hábitat natural. Desde entonces, estas herramientas asimétricas, ambiguas, difícilmente atribuibles y capaces de impactar sobre el conjunto de la sociedad se observan en la OTAN o en la Unión Europea de manera complementaria.

Los sucesos de Ucrania mediaron para que lo híbrido se situara al frente de la agenda aliada. Calificados por el secretario general de la OTAN, Jens Stoltenberg, como «el reverso tenebroso de nuestro Enfoque Integral» (ibídem, 2015), estos nuevos retos «que emplean de manera integrada una amplia gama de acciones militares, paramilitares y civiles abiertas o encubiertas» (ibídem, 2014: párr. 13) ocuparon un lugar destacado en la Cumbre de Gales. En este encuentro se acordó desarrollar herramientas para disuadir y responder a las denominadas «amenazas de guerra híbrida» y reforzar las capacidades nacionales. Varias de las iniciativas allí expuestas –el refuerzo de la comunicación estratégica, la realización de ejercicios con escenarios híbridos, la mejora de la coordinación con otras organizaciones o la elaboración de un plan para contrarrestarla– se consolidarían después. Establecido en Riga en enero de 2014, el Centro de Excelencia de la OTAN en Comunicaciones Estratégicas se convirtió en uno de los pilares de la organización para combatir la desinformación y la propaganda. Meses después, arrancó el primer ejercicio con un escenario que contenía amenazas híbridas para instruir a los políticos, funcionarios y militares aliados en estas situaciones ambiguas susceptibles de paralizar la toma de decisiones. Muchos de ellos acabarían contando con la participación europea y se convertirían en un área de cooperación fundamental entre ambas organizaciones.

AUNQUE LA ALIANZA ATLÁNTICA EMPEZÓ A INTERESARSE POR LA GUERRA HÍBRIDA EN 2007, FUE NECESARIO ESPERAR HASTA LA ANEXIÓN RUSA DE CRIMEA (2014) PARA QUE LO HÍBRIDO SE POPULARIZARA ENTRE LA CLASE POLÍTICA Y LA OPINIÓN PÚBLICA ALIADA.

En 2015, la OTAN presentó la estrategia para contrarrestar las amenazas híbridas. Articulada en torno a la *preparación* (para identificar, evaluar, comunicar y atribuir cualquier actividad en la zona gris), la *disuasión* (reforzando la resiliencia de las sociedades aliadas, adaptando el proceso de toma de decisiones y mejorando el alistamiento de las fuerzas para reducir el impacto de estas amenazas e incrementar las opciones de respuesta aliadas) y la *defensa* (aumentando la capacidad de respuesta aliada), esta estrategia orientó los esfuerzos de adaptación políticos y militares de la OTAN para combatir la amenaza híbrida.

Estas iniciativas se ratificaron y se ampliaron en la Cumbre de Varsovia (2016). Considerando la guerra híbrida como «una combinación amplia, compleja y adaptativa de medios convencionales y no convencionales, medidas militares, paramilitares y civiles abiertas y encubiertas empleadas de manera integrada por estados y actores no estatales para alcanzar sus objetivos» (ibídem 2016: párr. 72), en este encuentro se tomaron varios acuerdos.

Primero, aumentar la resiliencia de las sociedades e infraestructuras de los veintiocho para reducir el área de exposición a las estrategias hibridas e incrementar la disuasión por negación. Al igual que sucede con la ciberdefensa, se trata de una responsabilidad de los estados miembros, siendo la función de la OTAN la provisión del apoyo necesario. Tampoco debe extrañarnos, ya que cada sociedad posee vulnerabilidades específicas, cada zona gris se hace a medida para explotarla, y varios de estos instrumentos híbridos (informativos, económicos, culturales, legales, ambientales, etc.) escapan del ámbito de actuación aliado. En cualquier caso, en 2018 se constituyeron los grupos de apoyo antihíbridos para asistir técnicamente a aquellos países –como, por ejemplo, Montenegro en 2019– que necesitaran prepararse o responder a amenazas híbridas.

Segundo, declarar que un acto híbrido podría motivar la invocación del Artículo 5 del Tratado de Washington, según el cual un ataque contra cualquier miembro de la OTAN implica un ataque contra todos ellos. Aunque esta decisión refuerza la defensa colectiva, posibilita la disuasión por castigo e incrementa la credibilidad de este proceso –alterando el cálculo estratégico del adversario–, su implementación puede ser más complicada de lo que parece a simple vista. Al igual que los ciberataques, las estrategias híbridas son ambiguas, para dificultar su detección y atribución, y operan bajo el umbral de respuesta de su víctima. El país afectado debe atribuir la autoría (aunque se pueda comunicar conjuntamente) y su valoración se realizará caso por caso. Consecuentemente, puede ser difícil alcanzar el consenso necesario para invocar el Artículo 5, por lo que se deba optar por el mecanismo de consultas del Articulo 4, que permite a cualquier miembro de la Alianza Atlántica que vea amenazada la integridad territorial, independencia política o seguridad iniciar una ronda de consultas con el resto de los aliados. Además, la OTAN carece de instrumentos no militares para responder de manera graduada, lo que reduce su abanico de respuestas frente a los ataques híbridos.

LA ESTRATEGIA ALIADA PARA COMBATIR LAS AMENAZAS HÍBRIDAS SE FUNDAMENTA EN SU IDENTIFICACIÓN, DISUASIÓN Y DEFENSA.

Tercero, colaborar con otros actores que afronten problemas similares. Desde 2016, la OTAN ha incrementado las relaciones con Finlandia y Suecia (con amplia experiencia en contrarrestar amenazas híbridas desde un Enfoque Integral), Ucrania y Georgia (conocedoras de las actividades rusas bajo el umbral del conflicto), y con varios países del Indo-Pacífico que experimentan la zona gris china. Sin embargo, la colaboración más estrecha y provechosa se ha producido entre la OTAN y la UE. Precisamente, la declaración conjunta que ambas organizaciones firmaron en Varsovia en 2016 identi-

ficó siete áreas de cooperación, incluyendo la lucha contra las amenazas híbridas, la ciberseguridad y la ciberdefensa. Desde entonces, han colaborado para mejorar asuntos como la conciencia situacional, la comunicación estratégica, la respuesta a crisis, la resiliencia o la ciberseguridad. Aunque la disparidad de miembros, de culturas organizativas y de herramientas disponibles dificulta una cooperación más estrecha, tanto de forma bilateral como mediante el Centro de Excelencia Europeo para Contrarrestar las Amenazas Híbridas, la OTAN y la UE han realizado importantes avances en la detección, atribución, respuesta y resiliencia conjunta en esta materia.

Una mirada hacia el futuro

En definitiva, entre las cumbres de Gales y Varsovia, la OTAN sentó los pilares para contrarrestar estas estrategias. Basándose en los estudios previos sobre la guerra híbrida, desde el bienio 2014-2016 esta organización ha realizado importantes avances para combatir esta amenaza. Las capacidades de detección y alerta temprana, la inteligencia de amenazas, la colaboración con otros actores, el intercambio de información sensible entre sus miembros y con la UE, la flexibilización de los procesos de toma de decisiones, la respuesta a crisis, la comunicación estratégica, la ciberdefensa, el apoyo a la resiliencia nacional o la adaptación de la disuasión a estos ambientes más ambiguos para controlar la escalada son varios de ellos.

Y, aunque la invasión de Ucrania ha puesto de manifiesto que la disuasión y la defensa de sus miembros frente cualquier amenaza convencional o nuclear continúa siendo la principal razón de ser de la OTAN, la protección y resiliencia de sus sociedades frente a estas amenazas mucho más ambiguas también constituirá una de las principales líneas de acción futuras de esta organización. Tal y como se observó con el Enfoque Integral y su carencia de capacidades específicas para fines civiles, la OTAN es una organización político-militar que dispone de un catálogo de herramientas mucho más limitado que el de la UE. Sin embargo, su capacidad para ofrecer disuasión y respuestas creíbles en el espectro alto de la amenaza la convierte en un buen complemento a una UE capaz de desplegar una amplia gama de instrumentos civiles.

Si en la declaración final de la Cumbre de Londres (2019) apenas se mencionó lo híbrido, la Cumbre de Madrid de junio de 2022 estuvo monopolizada por la invasión de Ucrania y la amenaza de Rusia para la estabilidad euroatlántica. No obstante, las amenazas híbridas y la necesidad de contrarrestarlas también tuvieron un papel destacado en este encuentro y en el Concepto Estratégico que allí se aprobó. La preparación, disuasión y defensa ante el empleo coercitivo de herramientas políticas, económicas, energéticas o

informativas por parte de actores estatales como China o Rusia, no estatales o *proxies*, susceptibles de motivar la invocación del Artículo 5 del Tratado de Washington, se han convertido en una de las líneas de actuación futuras de la OTAN. Tampoco debe extrañarnos, ya que en la próxima década veremos un incremento del revisionismo estratégico y la proliferación de zonas grises donde lo híbrido continuará teniendo un papel fundamental.

Referencias

OTAN-Allied Command Transformation. *Multiple Futures Project. Navigating Towards 2030*. Norfolk: OTAN, 2009, p. 55.

OTAN. «Assured Security, Dynamic Engagement. Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO» (17 de mayo de 2010a) (en línea) https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2010_05/20100517_100517_expertsreport.pdf

OTAN. «BI-SC Input to a New Capstone Project for The Military Contribution to Countering Hybrid Threats» (25 de agosto de 2010b) (en línea) https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf

OTAN. «Declaración final de la Cumbre de Gales» (5 de septiembre de 2014), parr. 13 (en línea) https://www.nato.int/cps/en/natohq/official_texts_112964.htm

OTAN. «Palabras de Jens Stoltenberg en la apertura del Seminario de Transformación de la OTAN» (25 de marzo de 2015) (en línea) https://www.nato.int/cps/en/natohq/opinions_118435.htm

OTAN. «Declaración final de la Cumbre de Varsovia» (9 de julio de 2016), parr. 72. (en línea) https://www.nato.int/cps/en/natohq/official_texts_133169.htm

VENCER SIN LIBRAR BATALLA: ESTRATEGIAS DE ZONA GRIS DE CHINA EN ASIA ORIENTAL

La hibridez de China en los conflictos de Asia Oriental no es una novedad. Hablamos de una actualización de una tradición histórica basada en la filosofía de Sunzi y el pasado revolucionario del Partido Comunista Chino (PCCh) para adaptarse a una realidad definida por la competición entre potencias, revoluciones tecnológicas y el auge de contextos informatizados. A través de acciones en la zona gris, donde los límites entre la paz y el conflicto se vuelven difusos, China persigue sus intereses a expensas de un conflicto abierto con Estados Unidos y otros actores regionales.

Inés
Arco Escriche
Investigadora, CIDOB

CIDOB REPORT
08- 2022

En 1999, la publicación del libro *Unrestricted Warfare* escrito por dos coroneles del Ejército Popular de Liberación de China, Qiao Liang y Wang Xiangsui, sentenciaba cómo la efectividad del uso de «la fuerza militar para obligar al enemigo a someterse a la voluntad propia» había llegado a su fin, tras analizar la estrategia estadounidense durante la primera guerra del Golfo. En su lugar, las guerras contemporáneas se caracterizaban por una amalgama de tácticas políticas, económicas, culturales, diplomáticas y militares junto con fuerzas armadas y no convencionales para doblegar al enemigo –una definición similar al concepto occidental de *guerra híbrida*–.

Aunque este libro, y el análisis que contiene, se ha considerado como la conceptualización china para este tipo de conflictos, lo cierto es que algunos de los principios que rigen las amenazas híbridas contemporáneas son descritos ya por Sunzi en *El Arte de la Guerra* (2019 [siglo v a.C]) hace más de dos mil años. Para este filósofo chino, las

guerras se caracterizan por su constante mutación, y la victoria requiere de respuestas adaptativas a cada situación para neutralizar al adversario mediante la búsqueda constante de la ventaja relativa. Esta visión insta al empleo de un enfoque asimétrico mediante el uso ilimitado de tácticas previsibles e imprevisibles simultáneamente –por ejemplo, tropas regulares e irregulares–, con el objetivo de confundir, desmoralizar y, en última instancia, disuadir al enemigo de entrar en guerra. Para Sunzi, «la excelencia suprema es vencer al enemigo sin librar batalla».

La puesta en práctica de las enseñanzas de esta obra es claramente visible en la historia de China y sus respuestas a los conflictos. En la época imperial, la estrategia frente a amenazas exteriores consistía en el uso de múltiples tácticas no convencionales: des del empleo de mercenarios de origen enemigo contra su propio pueblo para dividirlo, hasta ofrendas, tributos y sobornos al adversario, incluyendo también la construcción de fortificaciones, como la Gran Muralla, para disuadir ataques de pueblos nómadas norteños. Solo si fracasaban las tres estrategias previas, se recurría al despliegue militar. Más recientemente, el PCCh consiguió la victoria en la guerra civil china (1945-1949) mediante la combinación de propaganda, milicias revolucionarias y guerras informativas dirigidas a explotar las debilidades de las fuerzas nacionalistas del Kuomintang (KMT). En la actualidad, el equivalente a esas tácticas podrían ser las guerras cibernéticas, la utilización de milicias, el apoyo a insurgencias locales, la firma de contratos comerciales lucrativos y paquetes de ayuda al desarrollo o la construcción de islas artificiales en el Mar de la China Meridional, bajo fines –teóricamente– «defensivos» (Baker, 2015).

Entonces, en el caso de China, si la estrategia híbrida es milenaria, ¿qué hay de *nuevo*?

Primero, la creciente rivalidad y competición con Estados Unidos a nivel regional e internacional, su inferioridad militar, así como la necesidad de mantener su narrativa de «desarrollo pacífico» favorecen la proliferación de tácticas híbridas. Estas prácticas están calculadas milimétricamente para mantenerse por debajo de los límites de una agresión abierta, obteniéndose pequeñas victorias a la vez que se evita un conflicto frontal con Estados Unidos y sus aliados en la región (Mazarr *et al*., 2018). Segundo, los nuevos avances tecnológicos han permitido la emergencia de nuevas tácticas informativas y cibernéticas, como la desinformación o los ciberataques y, en un futuro próximo, de formas innovadoras de guerra dirigidas por inteligencia artificial. Tercero, surge la necesidad de responder a las guerras híbridas, dada la certeza de una nueva tipología de guerra, donde la opinión pública, las instituciones o los sistemas legales pueden ser instrumentalizados como

armas. Desde 2003, el ejército chino lleva preparándose para ello a través de la doctrina de «las tres guerras», basada en el uso de tácticas propias de guerras psicológicas, mediáticas y legales que complementen las medidas diplomáticas, económicas y militares existentes –incluyendo el uso de fuerza militar en tiempos de paz–. Su objetivo es cultivar un entorno estratégico favorable en su vecindario, promover y defender sus intereses fundamentales de soberanía e integridad territorial en tiempos de paz, mientras se preparan para una posible guerra (PLA Daily, 2004).

Mientras en otros contextos el auge de estas técnicas ha sido definido como «conflictos híbridos» (véase el capítulo de Bargués y Bourekba en este volumen), la ausencia de violencia y de la utilización de fuerza militar directa hasta la fecha enmarcaría las operaciones chinas en la «zona gris», aunque no se trate de un concepto popular en el país asiático. Este elemento es clave: China se siente cómoda tanteando los límites de la paz y desafiando el *statu quo* en zonas grises, donde el conflicto se prolonga durante años sin cruzar el límite de una agresión directa, aunque, también, sin victoria clara.

LA FALTA DE CONCRECIÓN SOBRE QUÉ TERRITORIO ESTÁ BAJO JURISDICCIÓN CHINA, UNIDO AL RESTO DE MEDIDAS COERCITIVAS Y PSICOLÓGICAS, HA CONSEGUIDO EL OBJETIVO PRIMORDIAL DE LA ESTRATEGIA: LA DISUASIÓN DE ACCIONES DE OTROS ACTORES REGIONALES EN LA ZONA –AUNQUE NO DE ESTADOS UNIDOS, QUE REALIZA SISTEMÁTICAMENTE «OPERACIONES DE LIBRE NAVEGACIÓN»– Y EL CONTROL EFECTIVO DE ESE TERRITORIO SIN USAR LA FUERZA.

Geopolítica en la zona gris: del Mar de la China Meridional a Taiwán

En Asia, la geografía y la centralidad de los mares para la seguridad y las relaciones entre los actores regionales han permitido la emergencia de ciertas formas autóctonas de tácticas de zona gris. En concreto, se observa una predilección de China por el empleo de estrategias no convencionales en disputas sobre su soberanía donde existe la sombra de Estados Unidos, pero también una superioridad militar que actúa como disuasión frente a los poderes regionales, como en el conflicto del Mar de la China Meridional y las relaciones con Taiwán.

En el Mar de la China Meridional, Beijing reclama el control de territorios marítimos, delimitados por la «línea de nueve puntos», que representan cerca del 90% de las aguas –incluyendo las islas Paracelso, Spratly y el atolón de Scarborough–, disputados por Vietnam, Malasia, Indonesia, Brunéi y Filipinas. Para asentar sus reclamos históricos en la última década, ha articulado

una estrategia de zona gris cuidadosamente diseñada basada en la unión de fuerzas civiles y milicias marítimas, la construcción de infraestructuras de uso dual –es decir, obras de ingeniería civil pero que pueden ser utilizadas con fines militares como puertos y aeródromos–, tácticas informativas y la reinterpretación de leyes internacionales.

Para empezar, mediante el despliegue de fuerzas civiles –como la guardia costera o buques oceanográficos– y milicias marítimas formadas por pescadores junto a la marina, China va rodeando islotes gradualmente para ocupar el territorio a través de hechos consumados, como en el incidente del atolón de Scarborough, en 2012, o el atolón Ayungin, en las Spratly, en 2013. En concreto, estos pescadores chinos, aparentemente no vinculados al Gobierno ni a las fuerzas armadas, han protagonizado episodios de acoso a embarcaciones extranjeras, impidiendo el acceso a aguas territoriales o el desarrollo de actividades comerciales bajo el pretexto de «hacer cumplir la ley» por iniciativa propia (Lendon, 2021). Además, estas acciones sirven para ejercer presión psicológica y tantear progresivamente los límites y las respuestas de otros contendientes a sus acciones, como en marzo de 2021, cuando 220 buques pesqueros anclaron cerca del arrecife Whitsun, perteneciente a Filipinas, debido «al mal tiempo». Una vez bajo su control, China ha ido implementando lo que se ha denominado como «estrategias anti-acceso y de denegación de área» en la primera cadena de islas del Mar de la China Meridional, a través de la construcción de islas artificiales vertiendo arena, y de obras de ingeniería civil de uso dual (civil y militar) en los islotes ocupados, que le han permitido extender su control en la región, disuadir el acceso de fuerzas militares rivales y aumentar la proyección de poder chino, a la vez que ofrece un mayor margen de maniobra para sus fuerzas armadas en caso de una confrontación militar (CSIS, 2017). Por ejemplo, con la instalación de misiles antibuque y tierra-aire en tres arrecifes –Fiery Cross, Subi y Mischief–, China ha ejercido un control *de facto* desde 2018 sobre las islas Spratly al ser capaz de oponerse a cualquier movimiento por aire o mar en el archipiélago.

Paralelamente, China ha tratado de legitimar parte de estas demandas mediante acciones en el plano informativo, con la articulación de campañas a favor de sus reclamos territoriales mediante la difusión del mapa con la línea de nueve puntos, incluso en películas para niños (Reuters, 2019), y la instrumentalización de la jurisdicción internacional y nacional a su favor. Aunque Beijing defiende vehementemente el cumplimiento de la Convención de las Naciones Unidas sobre el Derecho del Mar (UNCLOS, por sus siglas en inglés), sus acciones parecen insinuar que esas reglas no se aplican totalmente en la región. En 2016, rechazó la opinión del Tribunal Internacional de la Haya a favor de Filipinas, justificando una inconsistencia con el

principio de soberanía y contestando parte de la UNCLOS, defendiendo el derecho de regular, oponerse o impedir la navegación en las aguas bajo su jurisdicción. En la misma línea, China aprobó en 2021 dos nuevas leyes nacionales –la Ley de Guardacostas y la Nueva Ley de Seguridad Marítima–, en las que se definen medidas de control de las embarcaciones y las condiciones que amparan el uso de la fuerza por parte de la guardia costera china contra barcos extranjeros en las «aguas bajo jurisdicción china». La falta de concreción sobre qué territorio está bajo jurisdicción china, unido al resto de medidas coercitivas y psicológicas, ha conseguido el objetivo primordial de la estrategia: la disuasión de acciones de otros actores regionales en la zona –aunque no de Estados Unidos, que realiza sistemáticamente «operaciones de libre navegación»– y el control efectivo de ese territorio sin usar la fuerza.

PESE AL ABANICO DE TÁCTICAS UTILIZADAS PARA PERSEGUIR SUS OBJETIVOS, LOS RESULTADOS DE LA ESTRATEGIA CHINA EN LA ZONA GRIS HAN SIDO AGRIDULCES. SI BIEN CHINA HA CONSEGUIDO AVANZAR PROGRESIVAMENTE SUS OBJETIVOS TERRITORIALES EN EL MAR DE LA CHINA MERIDIONAL, TAMBIÉN HA EROSIONADO SU LEGITIMIDAD EN LA REGIÓN MIENTRAS AUMENTA EL RIESGO DE UN CONFLICTO CON ESTADOS UNIDOS.

La singularidad del caso taiwanés –debido a su soberanía contestada, la cuestión identitaria, el apoyo estadounidense y la historia y los vínculos con la China continental– implica el uso de otras tácticas para explotar debilidades específicas. En este caso, Beijing utiliza la economía, la diplomacia, la prensa y desinformación basadas en la atracción, la coerción y el desconcierto de la sociedad taiwanesa con el fin de alimentar una mayor polarización respecto su futuro y las relaciones con el continente.

En el ámbito de la economía, China ha propuesto un paquete de medidas para atraer a taiwaneses a estudiar, invertir y trabajar en la China continental, especialmente con el objetivo de cosechar apoyos de una parte de la sociedad taiwanesa, incluidos políticos, empresarios y figuras clave. Es más, en periodos electorales o de mayor tensión, China no duda en recurrir a formas de coerción comercial para ejercer influencia sobre las políticas de la isla y fomentar la rivalidad entre los dos partidos principales, el Partido Progresista Democrático (DPP) y el KMT. El caso más reciente fue la restricción de importación de piñas taiwanesas en 2021 por motivos de «seguridad alimentaria». Una táctica bien familiar para los lituanos, quienes han sufrido restricciones comerciales similares por parte de Beijing después de que Taiwán abriera una oficina de representación en el país báltico en noviembre de 2021.

Estas tácticas han sido complementadas con una guerra informativa, activa desde los años cincuenta del siglo pasado, por medio de la propaganda, la financiación de medios de comunicación taiwaneses para la publicación de noticias favorables a China y, más recientemente, la difusión de noticias falsas y campañas de desinformación a través de redes sociales, llegando a decantar la balanza a favor de candidatos más favorables a China, como el populista Han Kuo-yu, en 2018 (Huang, 2020).

Sin embargo, aunque la mejor estrategia posible sigue siendo «someterla sin luchar» y usar la zona gris como una «mejor alternativa a un ataque militar», según Cui Lei (2021), la llegada al poder de Tsai Ing-wen (DPP) en 2016 ha ido acompañada de una posición más asertiva, con amenazas de una «reunificación por la fuerza», rotaciones militares alrededor de Fujian e incursiones en la zona de defensa aérea de Taiwán dirigidas a desalentar a la isla de cualquier acción secesionista.

Donde el gris se puede volver negro

Pese al abanico de tácticas utilizadas para perseguir sus objetivos, los resultados de la estrategia china en la zona gris han sido agridulces. Si bien China ha conseguido avanzar progresivamente sus objetivos territoriales en el Mar de la China Meridional, también ha erosionado su legitimidad en la región mientras aumenta el riesgo de un conflicto con Estados Unidos. En Taiwán, el éxito también es esquivo: a finales de 2021, más de un 62% de la población de Taiwán se definía como taiwanesa –frente a un 2% como china– y más del 80% se oponía a la reunificación (NCCU, 2022). Esta situación demuestra cómo el resultado final tiene muchos matices, aunque las tácticas híbridas y los conflictos en la zona gris hayan sido considerados especialmente efectivos para el progreso de los intereses y objetivos de ciertos actores.

Por estas razones es necesario preguntarnos bajo qué circunstancias China podría dar un salto a la «zona negra» e iniciar una guerra convencional. El primer caso sería un aumento voluntario de las tensiones y el uso de fuerza militar por parte de China, por ejemplo, con la invasión de Taiwán –un caso que tendría paralelismos con la invasión rusa en Ucrania–. Aunque se trata de un escenario poco probable en la actualidad, una posibilidad más realista sería un incremento de tensiones estratégicas en cualquiera de los dos conflictos que acabe en un simple error de cálculo y termine provocando una confrontación directa o un conflicto abierto debido a la acumulación de actividades que rocen el límite de la paz y la guerra, como hemos visto en las tensiones en la frontera con India en verano de 2020. Por ahora, la influencia de Sunzi sigue guiando la estrategia de China.

Referencias

Aspinwall, Nick. «Taiwan Rebukes Beijing's New 26 Measures for Cross-Strait exchanges ». *The Diplomat* (9 de noviembre de 2019) (en línea) [Fecha de consulta: 26.07.2022]: https://thediplomat.com/2019/11/taiwan-rebukes-beijings-new-26-measures-for-cross-strait-exchanges/

Baker, Benjamin D. «Hybrid warfare with chinese characteristics». *The Diplomat* (23 de septiembre de 2015) (en línea) [Fecha de consulta: 26.07.2022]: https://thediplomat.com/2015/09/hybrid-warfare-with-chinese-characteristics/

CSIS. «Chinese Power Projection Capabilities in the South China Sea». CSIS, 2017 (en línea) [Fecha de consulta: 26.07.2022]: https://amti.csis.org/chinese-power-projection/

Cui Lei. «Mainland China is in no position to take Taiwan by force». *EastAsiaForum*, 2021 (en línea) [Fecha de consulta: 26.07.2022]: https://www.eastasiaforum.org/2021/02/26/mainland-china-is-in-no-position-to-take-taiwan-by-force/

Huang, Paul. «Chinese cyber-operatives boosted Taiwan's insurgent candidate». *Foreign Policy*, 2020 (en línea) [Fecha de consulta: 26.07.2022]: https://foreignpolicy.com/2019/06/26/chinese-cyber-operatives-boosted-taiwans-insurgent-candidate/

Lendon, Brad. «Beijing has a navy it doesn't even admit exists, experts say. And it's swarming parts of the South China Sea». *CNN,* 2021 (en línea) [Fecha de consulta: 26.07.2022]: https://edition.cnn.com/2021/04/12/china/china-maritime-militia-explainer-intl-hnk-ml-dst/index.htmlMazarr, Michael J.; Heath, T. R. & Cevallos, A. *China and the International Order*. Santa Monica, CA: RAND Corporation, 2018.

National Chengchi University (NCCU). «Taiwanese/Chinese Identity (1992/06~2021/12)». Election Study Center, NCCU, 2022 (en línea) [Fecha de consulta: 26.07.2022]: https://esc.nccu.edu.tw/PageDoc/Detail?fid=7800&id=6961

PLA Daily. «El ejército popular de liberación de China empieza el estudio y el entrenamiento de las "Tres Guerras"». Sina.cn, 2004. (en línea) [Fecha de consulta: 26.07.2022]: http://mil.news.sina.com.cn/2004-07-16/1738210714.html

Qiao, L. & Wang, X. *Unrestricted warfare*. Brattleboro: Echo Point Books & Media, 2015.

Reuters. «Abominable: Anger grows over controversial map in Chinese children's film». *The Guardian,* 2019 (en línea) [Fecha de consulta: 26.07.2022]: https://www.theguardian.com/world/2019/oct/18/abominable-anger-grows-over-controversial-map-in-chinese-childrens-film

Sunzi. *L'Art de la guerra*. Barcelona: Publicacions de l'Abadia de Montserrat, 2019.

INSEGURIDAD EN EL MAGREB: SE AMPLIA EL CATÁLOGO DE AMENAZAS

Un conflicto congelado que ha entrado en una etapa de deshielo, una rivalidad entre las principales potencias regionales cada vez más ostensible y una suma de factores domésticos e internacionales que aumentan la percepción de inseguridad de las elites gobernantes. Así podría resumirse el estado de las relaciones intramagrebíes y la poco halagüeña perspectiva de futuro para su seguridad y la de sus vecinos.

Eduard Soler i Lecha
Investigador sénior, CIDOB

CIDOB REPORT
08- 2022

A finales de los años ochenta y principios de los noventa del siglo XX se abrió una pequeña ventana de esperanza. Coincidiendo con el fin de la Guerra Fría, los dirigentes de Marruecos y Argelia se tendieron la mano, se creó la Unión del Magreb Árabe (UMA) a imagen y semejanza de la Unión Europea y, poco después, en el Sáhara Occidental, Marruecos y el Frente Polisario decretaron el alto el fuego y se puso en marcha la MINURSO, la misión de Naciones Unidas para el Referéndum del Sáhara Occidental, que debería contribuir a resolver el conflicto.

Sin embargo, la esperanza para la paz en la región duró poco. El desgarro de la década sangrienta en Argelia, el cierre de la frontera entre los dos países en 1994, el bloqueo de las negociaciones sobre el Sáhara con el fracaso de dos planes promovidos por el exsecretario de Estado estadounidense, James Baker, como enviado personal del secretario general de Naciones Unidas, así como la manifiesta disfuncionalidad de la UMA hicieron de la integración magrebí poco más que un espejismo.

En el momento de escribir estas líneas, preocupa el aumento de la violencia en el Sáhara y el rápido deterioro de las relaciones entre Marruecos y Argelia. A una frontera cerrada desde 1994 se le ha sumado la ruptura diplomática y el cierre del espacio aéreo argelino, sucedidos en agosto y septiembre de 2021, respectivamente. El ataque, supuestamente por parte de Marruecos, contra un convoy argelino que cubría la ruta entre Mauritania y Argelia, el 1 de noviembre de ese año, transitando por la zona controlada por el Frente Polisario, según informó el medio digital *Menadefense*, encendió todas las alarmas. No es buena señal que publicaciones como el *Atlas Stratégique de la Méditerranée et su Moyen-Orient*, de la francesa Fondation Méditerranéenne d'Études Stratégiques, consagrase su atención a las capacidades militares de Marruecos y Argelia, y al escenario de un enfrentamiento armado entre ambos países.

Para complicar aún más las cosas, en el otro extremo del Magreb, Libia lucha para salir de la espiral de conflicto en la que lleva instalada desde 2011. Y, en el sur, el Sahel se consolida como una de las principales preocupaciones para la seguridad regional. Es significativo que en ambos escenarios, Marruecos y Argelia estén proyectando su influencia, bien sea ofreciendo mediación, articulación de foros de diálogo regional o iniciativas de cooperación bilateral. Aunque la competición argelino-marroquí no es responsable del alto grado de inestabilidad en Libia y en el Sahel, esta tampoco ayuda a encontrar vías para reducir la tensión.

Una de las características de la inseguridad en el Magreb es que el recurso a amenazas híbridas convive con demostraciones de fuerza más propias de un enfrentamiento convencional. El Magreb ejemplifica cómo dichas amenazas no están sustituyendo a las convencionales, sino que pueden precederlas o incluso favorecerlas. El conflicto del Sáhara Occidental, los nexos con otros espacios de conflicto, así como los intentos de deslegitimar o debilitar el régimen de un país rival ayudarán a comprender mejor esta interrelación.

El conflicto del Sáhara: ¿quién es quién?

¿Quiénes son las partes enfrentadas en este conflicto? No hay una respuesta unánime a esta pregunta, lo cual es un claro indicador de la naturaleza híbrida de este conflicto y de la distinta percepción sobre las amenazas. Argelia sostiene que el enfrentamiento es entre Marruecos y el Frente Polisario. En cambio, Rabat argumenta que este último actúa como un *proxy* de Argelia. En otras palabras, en el relato marroquí, Argelia es una de las partes del conflicto, aunque el relato argelino lo rechace de pleno.

El conflicto del Sáhara está a punto de cumplir su 50 aniversario. Desde 1991 a noviembre de 2020 encajaba en la categoría de conflicto congelado. Habían cesado las hostilidades. El conflicto no se había resuelto, pero se prolongaba por otras vías y con otras modalidades en vez de la militar. Aunque los efectivos seguían desplegados, ganaba protagonismo la competición diplomática para arrancar o revertir reconocimientos a la República Árabe Saharaui Democrática (RASD).

Ante la falta de avances y con las bases del Polisario cada vez más frustradas, era cuestión de tiempo que la situación empeorase. En noviembre de 2020, se pudo confirmar que el conflicto ya no estaba en el congelador. El Polisario anunció el fin del alto el fuego como respuesta a la operación de Marruecos para retomar el control del paso de Guerguerat, fronterizo con Mauritania. Poco después, el presidente estadounidense, Donald Trump, reconocía la soberanía marroquí sobre el Sáhara, dando aliento a una política más asertiva por parte de Marruecos, que luego alimentaría las crisis diplomáticas con Alemania y España en 2021. Sobre el terreno, un dron marroquí liquidó al jefe de la gendarmería del Polisario en abril de 2021, tal como reconocieron fuentes saharauis. Ocasionalmente, se han producido hostigamientos en la zona que separa los territorios controlados por ambas partes sin que pueda llegarse a hablar de un retorno a la guerra. La situación podría cambiar si el Polisario hace efectiva su amenaza de lanzar ataques contra las ciudades saharauis bajo control marroquí.

La confusión sobre quiénes son las partes en conflicto –¿lo es Argelia?– así como la carrera armamentística en la que se han enzarzado las dos potencias magrebíes aumentan los riesgos del deshielo del conflicto en el Sáhara. Si el Polisario cumpliese sus amenazas, ¿lo entendería Marruecos como una especie de ataque híbrido dirigido desde Argel? Y si es así, ¿cuál sería su reacción? ¿Y cómo respondería Argelia si se producen nuevos incidentes contra sus nacionales en las zonas controladas por el Polisario y, más aún, si el enfrentamiento llegase a Tinduf? Son escenarios muy delicados, pero no desdeñables y ahondan en la tesis de que lo híbrido se propaga: lo convencional y lo no convencional se retroalimentan.

La porosidad de las fronteras y de los escenarios del conflicto

Una de las dinámicas más inquietantes de la seguridad en el Magreb son las crecientes interconexiones con otros escenarios de conflicto. Tras la caída de Muamar el Gadafi en 2011, el nexo de inseguridad entre el Magreb y el Sahel se hizo especialmente visible a través de los grupos criminales, el tráfico de armas y personas, las milicias y los grupos terroristas que operaban aprovechando las fronteras porosas. El conflicto en el norte de Mali en

2012 fue la prueba definitiva. Una década atrás, la evolución del Magreb contribuyó a la desestabilización del Sahel. Ahora, el flujo de inseguridad puede producirse en la dirección inversa. Conscientes de esta situación, tanto Marruecos como Argelia han desplegado su caja de herramientas para ser vistos por los países del Sahel –y también por las principales potencias globales con intereses en esa región– como un actor imprescindible. Al hacerlo, Rabat y Argel han añadido una dimensión más a esta relación de competición y abierta hostilidad.

DURANTE LA ÚLTIMA DÉCADA, EL MAGREB SE HA CONVERTIDO EN UN ESPACIO DE COMPETICIÓN ENTRE POTENCIAS REGIONALES DE ORIENTE MEDIO. UNA COMPETICIÓN QUE SE JUEGA TANTO ENTRE POTENCIAS TRADICIONALES COMO EGIPTO Y TURQUÍA, COMO ENTRE PAÍSES MÁS PEQUEÑOS, PERO CON RECURSOS Y AMBICIÓN, COMO SON EMIRATOS ÁRABES UNIDOS Y QATAR. LIBIA SE HA CONVERTIDO EN EL ESCENARIO POR EXCELENCIA DE ESTA COMPETICIÓN REGIONAL.

El otro nexo es el que liga el Magreb con Oriente Medio. Durante la última década, el Magreb se ha convertido en un espacio de competición entre potencias regionales de Oriente Medio. Una competición que se juega tanto entre potencias tradicionales como Egipto y Turquía, como entre países más pequeños, pero con recursos y ambición, como son Emiratos Árabes Unidos y Qatar. Libia se ha convertido en el escenario por excelencia de esta competición regional, en la medida que estos cuatro países han apoyado o bien al Gobierno de Trípoli o bien al mariscal Khalifa Haftar. A menudo, unos y otros han justificado su apoyo político, financiero o militar en términos de seguridad nacional. No obstante, ocasionalmente también han evidenciado que su apoyo a grupos rivales en Libia corresponde a visiones opuestas sobre el futuro de la región y, específicamente, sobre el papel que pueden desempeñar grupos afines a los Hermanos Musulmanes.

Sin embargo, el cambio más notable, y quizás el que tenga más trascendencia, es la normalización de relaciones entre Marruecos e Israel. Este acercamiento se ha producido en el marco de los llamados *Acuerdos de Abraham*, impulsados por la Administración estadounidense. En diciembre de 2020, y a pesar de haber perdido las elecciones, Donald Trump dio la bienvenida al anuncio de normalización al mismo tiempo que reconocía, a través de dos tuits consecutivos, la soberanía marroquí sobre el Sáhara Occidental.

La llegada al poder de Joe Biden no ha alterado esta apuesta, y el acercamiento entre Marruecos e Israel ha sido rubricado con las visitas del minis-

tro de Exteriores israelí, Yair Lapid, y también del ministro de Defensa, Benny Gantz, a Rabat. Durante la visita de este último a la capital marroquí, se firmó el primer acuerdo en materia de seguridad y defensa de ambos países. Por su parte, las autoridades argelinas expresaron su rechazo a la cooperación de Marruecos con Israel.

A la hora de encarar sus complicadas relaciones de vecindad, las autoridades argelinas siempre habían confiado en su superioridad militar. Sin embargo, la entrada en escena de Israel, en temas tan diversos como la inteligencia o la construcción de drones, ha despertado una fuerte inquietud en Argelia, sobre todo en relación con enfrentamientos no convencionales.

Para acabar de complicar las cosas, hay que señalar que, desde hace años, Marruecos acusa a Irán de estar proporcionando apoyo al Polisario a través de Hezbolá. Más recientemente, responsables israelíes han argumentado que Argelia e Irán forman parte de un mismo bloque regional. El Magreb no sólo está más dividido, sino que cada vez más actores de fuera de la región lo ven como un espacio donde proyectar sus rivalidades.

La batalla de la legitimidad y el catálogo de represalias

Desde sus independencias respectivas, Marruecos y Argelia han construido modelos políticos muy distintos, tanto en lo que respecta a su organización interna como a sus apoyos internacionales. Marruecos se erigía como una monarquía conservadora con buenas relaciones con Occidente, mientras que la Argelia republicana aspiraba a ser referente de los revolucionarios del mundo entero. No es el único ni quizás el principal factor que explique la mala relación y la desconfianza entre las élites gobernantes de ambos países, pero hay que tenerlo en cuenta. Además, en la batalla de narrativas, como detalla Tilila Sara Bakrim, no solo participan las élites gobernantes, sino también sus respectivos campos mediáticos.

A pesar de ello, Miguel Hernando de Larramendi ha dado cuenta de cómo las primaveras árabes generaron un sentimiento de vulnerabilidad compartida, y eso produjo una reactivación temporal de las relaciones bilaterales entre Argelia y Marruecos. Sin embargo, a medida que el temor a la flaqueza ante las protestas de su propia población fue temperándose resurgió la rivalidad.

En el período previo a la pandemia, tanto Marruecos como Argelia vivieron el resurgir de las protestas. En el primero, estas estaban muy localizadas en el norte del país y, concretamente, en la región del Rif. En el segundo, la extensión era mayor y el movimiento del Hirak**,** iniciado en 2019, forzó la renuncia del presidente Abdelaziz Buteflika. Sin embargo, lejos de generar

condiciones para un acercamiento, este tipo de protestas aumentaron las suspicacias e incluso las acusaciones de que el país vecino se inmiscuía en asuntos internos e intentaba contribuir a la desestabilización.

Esta situación llegó a su paroxismo durante el verano de 2021. El embajador marroquí en Naciones Unidas, Omar Hilale, distribuyó un documento en el que descalificaba al Polisario y la RASD como «república quimérica autoproclamada desde la capital argelina» y criticaba que Argelia se erigiese como ferviente defensor del derecho a la autodeterminación a pesar de negar «este mismo derecho al pueblo de la Cabilia, uno de los pueblos más antiguos de África». El diplomático marroquí añadía que «el valeroso pueblo cabila merece, más que ningún otro, disfrutar plenamente de su derecho a la libre determinación». El apoyo al independentismo cabila, articulado entorno al Mouvement pour l'autodétermination de la Kabylie (MAK), a quien Hilale propuso invitar a las reuniones del Comité para la Descolonización de Naciones Unidas, generó un fuerte rechazo por parte de las autoridades argelinas y, en última instancia, fue el argumento esgrimido para justificar la ruptura de relaciones diplomáticas. Antes de tomar esta decisión, Argel acusó al MAK y, por lo tanto, indirectamente a Marruecos, de haber propiciado los incendios forestales que afectaron a la Cabilia en agosto de 2021. Es difícil, pensar en una amenaza más híbrida que ésta.

LA CRECIENTE HOSTILIDAD ENTRE MARRUECOS Y ARGELIA, ASÍ COMO LA DESCONGELACIÓN DEL CONFLICTO EN EL SÁHARA OCCIDENTAL ESTÁN TENIENDO UN FUERTE IMPACTO SOBRE ESPAÑA. POR AHORA, SE HA MATERIALIZADO EN FORMA DE CRISIS DIPLOMÁTICAS, PROCESOS JUDICIALES CONTRA ANTIGUOS MIEMBROS DEL GOBIERNO, SOSPECHAS DE ESPIONAJE, EL USO DE LA ENERGÍA Y LAS MIGRACIONES COMO ARMA POLÍTICA Y REPRESALIAS COMERCIALES Y EN MATERIA DE MOVILIDAD.

Poco después, en octubre de 2021, el Gobierno argelino cerró uno de los dos gaseoductos que conectan Argelia con la península ibérica, concretamente el Magreb-Europa cuya construcción se inició a principios de los años noventa, durante un breve período de mejora en las relaciones entre Argel y Rabat, y que discurre por el norte de Marruecos antes de desembocar en Andalucía. A cambio de los derechos de paso, Marruecos recibía una especie de peaje en forma de gas a precios inferiores a los del mercado, gas que tenía un papel importante en la producción de electricidad. Argelia no ha llegado a decir que el cierre del gaseoducto responda a un intento de debilitar a Marruecos. Formalmente, además, no se ha roto ningún contrato, sino que este ha expirado. Aun así,

los efectos y las percepciones no son muy distintas y, por lo tanto, refuerzan la dimensión híbrida de los instrumentos que se despliegan en la competición intramagrebí.

La proliferación y diversificación de amenazas raramente se limitan a un espacio geográfico. Tienden a arrastrar a sus vecinos y estos también acaban sufriendo las repercusiones de cualquier escalada del conflicto. La creciente hostilidad entre Marruecos y Argelia, así como la descongelación del conflicto en el Sáhara Occidental están teniendo un fuerte impacto sobre España. Por ahora, se ha materializado en forma de crisis diplomáticas, procesos judiciales contra antiguos miembros del Gobierno, sospechas de espionaje, el uso de la energía y las migraciones como arma política y represalias comerciales y en materia de movilidad. Autores como Javier Jordán afirman que Marruecos emplea estrategias híbridas en sus relaciones con el Estado español. Aunque el catálogo de este tipo de amenazas se despliega primordialmente entre los propios países del Magreb, vecinos como España acaban sufriéndolas, y su normalización es un riesgo compartido por todos los socios europeos.

Referencias

Fondation Méditerranéenne d'Etudes Stratégiques. *Atlas stratégique de la Méditerranée et du Moyen-Orient* (edición 2022), París: Institut FMES, 2022 (en línea) [Fecha de consulta: 6.7.2022] https://fmes-france.org/atlas-strategique-de-la-mediterranee-et-du-moyen-orient-edition-2022/

Hernando de Larramendi, Miguel. «Doomed regionalism in a redrawn Maghreb? The changing shape of the rivalry between Algeria and Morocco in the post-2011 era». *The Journal of North African Studies*, vol. 24, nº 3 (2019), p. 506-531 (en línea) [Fecha de consulta: 6.7.2022] https://ruidera.uclm.es/xmlui/bitstream/handle/10578/25340/Doomed%20regionalism%20in%20a%20redrawn%20Maghreb.%20The%20changing%20shape%20of%20the%20rivalry%20between%20Algeria%20and%20Morocco%20in%20the%20post-2011%20era.pdf?sequence=1&isAllowed=y

Jordán, Javier. «Ceuta y Melilla: ¿emplea Marruecos estrategias híbridas contra España?». *Global Strategy* (24 de marzo de 2021) (en línea) [Fecha de consulta: 6.7.2022] https://global-strategy.org/ceuta-y-melilla-emplea-marruecos-estrategias-hibridas-contra-espana/

Sara Bakrim, Tilila. «Rivalité Maroc-Algérie: la guerre des récits». *Note de la FRS*, n°18/2022 (abril de 2022) (en línea) [Fecha de consulta: 6.7.2022] https://www.frstrategie.org/publications/notes/rivalite-maroc-algerie-guerre-recits-2022

Soler i Lecha, Eduard. «La otra África: rivalidades superpuestas en el Magreb». *IDEES*, nº 56 (enero de 2022), (en línea) [Fecha de consulta: 6.7.2022] https://revistaidees.cat/es/la-otra-africa-rivalidades-superpuestas-en-el-magreb/

CIDOB

BARCELONA
CENTRE FOR
INTERNATIONAL
AFFAIRS

Con el apoyo de:

En un momento de incertidumbre y contestación de las normas internacionales, los conflictos son cada vez más difusos, como el espacio que separa la guerra y la paz. Una mayor dependencia y conectividad entre actores se aprovecha para explotar las vulnerabilidades de los demás. Las tácticas se diversifican y aumenta la preocupación ante las amenazas híbridas. Los ciberataques, la desinformación, la manipulación de procesos electorales o la instrumentalización de los movimientos migratorios se despliegan en numerosas partes del mundo. Las amenazas no convencionales alimentan la incertidumbre, erosionan valores y normas, y tensionan las relaciones internacionales.

Este *CIDOB Report* analiza el auge de las amenazas híbridas. El propósito es conocer sus distintas tácticas y formas, así como los diferentes escenarios en los que se despliegan, además de examinar su impacto y las respuestas que se están dando para abordar los múltiples retos que plantean.