La guerra informativa china en la zona gris

Guillem Colom Piella
Doctor en Seguridad Internacional

Los conceptos «amenaza híbrida» o «zona gris» se han popularizado para definir las actividades que realizan países como Rusia, China, Irán o Corea del Norte para proyectar su influencia exterior, negando de forma plausible su responsabilidad, dificultando la respuesta del adversario y evitando cruzar el umbral del conflicto armado. La zona gris, definida como la franja que separa la paz de la guerra abierta es, por naturaleza, ambigua. Esta ambigüedad es la que permite a potencias revisionistas como las arriba mencionadas proyectar su poder más allá de sus fronteras sabiendo que, si sus actividades pueden ser negadas de forma plausible y no afectan intereses vitales de la víctima, difícilmente tendrán una respuesta clara y efectiva. Observadas de forma aislada, estas acciones que pueden abarcar el apoyo a la oposición política, la coerción económica, las actividades de influencia, ciberataques, acciones agresivas de inteligencia, disuasión militar coercitiva o una política de hechos consumados difícilmente constituirán un *casus belli* porque siempre intentarán situarse bajo el umbral del conflicto. Sin embargo, su efecto agregado a largo plazo mediante la «táctica del salami» –concatenando acciones que proporcionan pequeñas ganancias– sí podría alterar las correlaciones de fuerzas existentes[1].

Aunque muchas de estas actividades se realizan en el mundo físico (desde las tradicionales incursiones de pesqueros chinos en islas en disputa con Japón hasta los recientes ataques sobre petroleros saudíes en el Golfo Pérsico), cada vez más se realizan también en el mundo virtual. Ello se debe a la ambigüedad, anonimidad, asimetría, economía y ubicuidad propias

del ciberespacio. Estas características permiten a muchos actores proyectar su poder de manera asimétrica dificultando la atribución de sus acciones, impidiendo la asignación de responsabilidades legales, imposibilitando cualquier represalia contra ellos y comprometiendo la credibilidad de las herramientas disuasorias del actor que ha sido atacado. Inicialmente, sucesos como los ciberataques rusos sobre Estonia (2007) y Georgia (2008) o el ciberespionaje chino (que culminó con la famosa atribución de la *Amenaza Persistente Avanzada* 1 (APT-1) en 2013)[2], motivaron que el foco de atención estratégico se centrara en las actividades de explotación y los potenciales efectos disruptivos que podría tener un ciberataque contra servicios, sistemas o redes. De ahí el interés de la comunidad internacional en determinar qué tipo de ciberataque podría constituir un *casus belli* y en plantear un enfoque «clásico» a la disuasión por negación y castigo. Sin embargo, la expansión del califato islámico en Iraq, Irán o Yemen, la ocupación de Crimea, la invasión del este de Ucrania o las operaciones de influencia en los pasados comicios presidenciales estadounidenses demostraron que el entorno *online* también posibilitaba otras actividades de mucho menor perfil, pero igualmente susceptibles de afectar la seguridad nacional. La propaganda multicanal, el perfilado de usuarios para reforzar su filtro burbuja, la viralización de noticias falsas o la filtración

de información personal comprometida también podían servir para explotar las divisiones existentes en las sociedades e influir sobre sus opiniones públicas. Además, las campañas rusas en Crimea, Ucrania o Siria no solo volvieron a poner de manifiesto la relevancia de la guerra electrónica en los conflictos modernos, sino también demostraron el potencial empleo del espacio radioeléctrico para realizar actividades en la zona gris, desde interferir comunicaciones, degradar sistemas de defensa aérea, suplantar las señales de GPS hasta obstaculizar actividades de inteligencia[3].

¿Qué tienen en común las ciberoperaciones de explotación, defensa o ataque, las operaciones de influencia en el ciberespacio o las actividades en el espacio radioeléctrico? Todas ellas se ejecutan en el espacio informativo, que engloba el ciberespacio y cuyos efectos se pueden observar en el ámbito lógico, físico y cognitivo. Aunque el espacio informativo como nuevo dominio de la guerra se popularizó con el auge de la Revolución en los Asuntos Militares (RMA) a principios de la década de 1990[4], con el paso a la transformación a finales de la década fue reemplazado –quizás por la penetración global de Internet, su impacto en la economía mundial o la creciente dependencia sobre los servicios e infraestructuras que lo posibilitaban– por el ciberespacio como un dominio eminentemente técnico y como quinto dominio de la guerra…al menos para Occidente[5].

Condicionada por su cultura estratégica e historia política, China entiende que la información es una herramienta esencial para proyectar el poder nacional, uno de los pilares de la soberanía nacional y uno de los principales activos a proteger para mantener la estabilidad del binomio estado-partido. Esta concepción que prima la protección del espacio informativo nacional y la proyección de la influencia exterior –algo que tradicionalmente se realizaba vía propaganda política– es anterior a la llegada de Internet. Sin embargo, en la década de 1990 China alertó de que las nuevas tecnologías eran una amenaza a la seguridad por su potencial desestabilizador y por la dependencia tecnológica y debilidad estratégica que se generaba con Estados Unidos. En consecuencia, no solo consideró necesario restringir el acceso a Internet –aunque también lo necesitaba para entrar a la economía mundial siguiendo los saltos planteados por Deng Xiaoping años atrás– e intentar que la comunidad internacional apoyara su control y regulación para proteger la seguridad nacional, sino también crear un ecosistema cibernético propio y potencialmente aislado del resto del mundo. Paralelamente, sus estrategas militares entendieron que la información –y no las armas de precisión o los sensores tal y como inicialmente asumía Occidente en plena euforia revolucionaria– podía ser el pilar de esta RMA que prometía transformar la guerra[6]. En consecuencia, asumieron que la guerra informativa sería uno de los pilares de su transformación militar, el fundamento de los conflictos futuros y el marco general donde no solo se emplaza el ciberespacio, sino el entorno donde se ejecuta cualquier actividad física, lógica y

cognitiva vinculada con el uso de la información como vector, objetivo o medio. Además, China ha integrado con gran éxito las actividades informativas en estrategias multidimensionales para proyectar el poder y los intereses nacionales en la zona gris del conflicto. Teniendo en cuenta estos elementos, a continuación se explicará brevemente cómo China concibe la guerra informativa y cómo la utiliza en la zona gris del conflicto.

Para Pekín, la guerra informativa (*xinxi zhan*) es uno de los pilares de los conflictos postmodernos, un componente trasversal de las «tres» guerras futuras (sin contacto, no-linear y asimétrica) y una de las competencias que debe dominar el Ejército de Liberación Popular. Basada inicialmente en la emulación de los conceptos estadounidenses[7], la guerra informativa china se ha ido configurando desde la década de 1990. Teniendo como principal punto de partida la identificación de las lecciones de la Guerra del Golfo y el auge de la RMA, su desarrollo se ha producido siguiendo los debates occidentales sobre la transformación de la guerra y dialogando con su cultura estratégica.

Asumiendo que en la Era de la Información el poder nacional se mide en términos informativos, los líderes chinos concluyeron hace un cuarto de siglo que el auge y caída de las potencias estaría determinado por la capacidad para generar, obtener, transmitir, analizar y explotar la información. En consecuencia, China debía adaptarse a la era de la información apoyando el desarrollo nacional (legitimando así el Partido Comunista chino), creando su propio ecosistema de innovación tecnológica, y preparando al Ejército de Liberación Popular para la guerra informatizada (*xinxihua zhanzheng*). Esta transformación cuyos pilares fueron establecidos por el premier Yang Zemin tras la espectacular victoria de la coalición liderada por Estados Unidos en la Operación Tormenta del Desierto se lograría reduciendo la entidad de sus fuerzas, mecanizando sus unidades e informatizando sus procesos. Ello permitiría al país combatir eficazmente en «guerras locales en ambientes de alta tecnología» y, posteriormente, en «guerras locales en ambientes informatizados»[8].

Fundamentada en varias tradiciones –desde la guerra informatizada que la enmarca, la guerra política que la permea, la guerra revolucionaria que todavía la inspira o enseñanzas de Sun Tzu y de Mao Tse-Tung que la integran en su cultura estratégica[9]– y desarrollada en el marco de la RMA con características chinas[10], la guerra informativa china es objeto de importantes debates fuera del país. Aunque existe abundante literatura extranjera y varias fuentes tanto oficiales como oficiosas del país vienen haciendo referencia al concepto desde los noventa, la doctrina militar se mantiene clasificada y su guerra informativa continúa siendo una incógnita para los estrategas occidentales. Muchos de ellos centran su interés en las ciberoperaciones –que China define como guerra en redes (*wangluo zhan*)–,

las operaciones psicológicas o las actividades de denegación y engaño, subrayar su carácter asimétrico y discutir sobre si esta permitiría triunfar en conflictos sin la necesidad de combatir cuerpo a cuerpo[11]. Sin embargo, la guerra informativa china es más compleja y amplia.

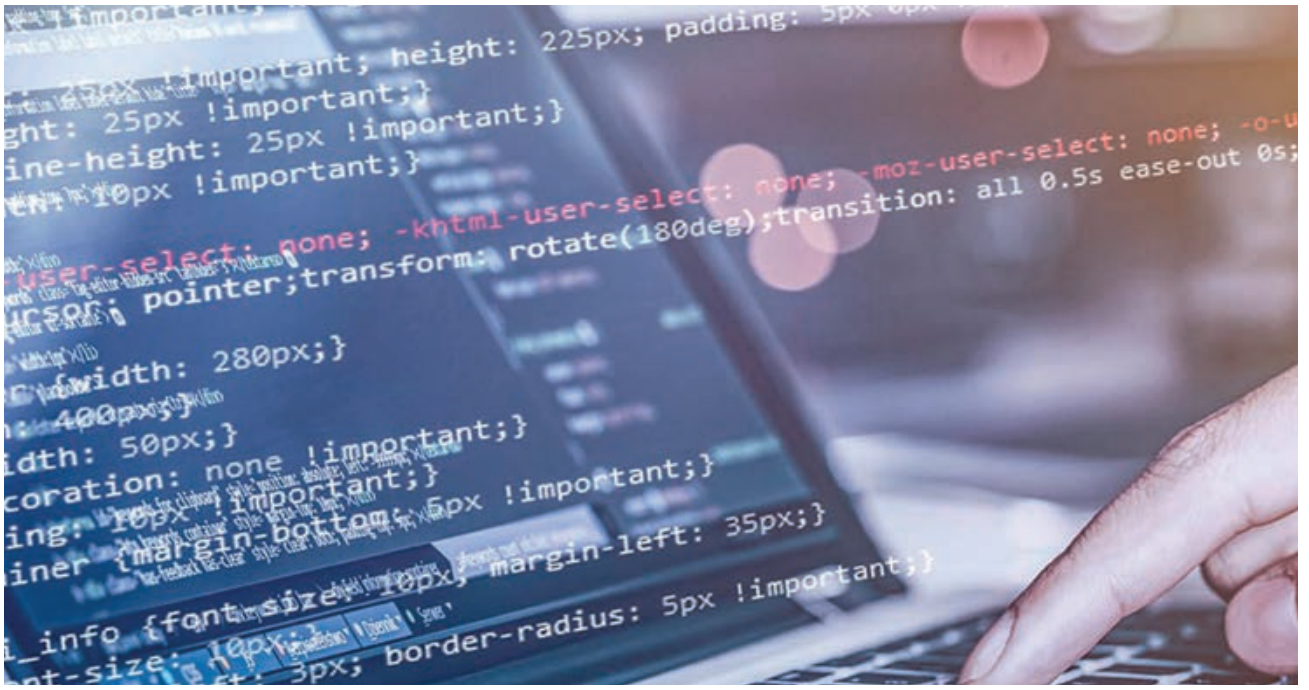
El diccionario terminológico militar del Ejército de Liberación Popular define la guerra informativa como aquellas «…actividades realizadas por los contendientes en el dominio informativo. Incluye la protección de los recursos informativos, el logro de la iniciativa en la producción, transmisión y gestión de la información o la disrupción de la capacidad del adversario para transmitir la información con el objeto de establecer las condiciones necesarias para disuadir, combatir y ganar conflictos»[12]. Ello requiere la ejecución de una amplia gama de actividades físicas, lógicas y cognitivas en el plano político (librando las llamadas tres guerras: de opinión pública, psicológica y legal)[13] y militar (mediante guerra electrónica, guerra en redes o ciberguerra, guerra psicológica, guerra de mando y control y guerra de inteligencia) para lograr la supremacía informativa[14]. Mientras el planeamiento de las primeras recae en la Comisión Militar Central del Partido Comunista Chino, la ejecución de las segundas es realizada por la Fuerza de Apoyo Estratégico del Ejército de Liberación Popular, encargada de las actividades espaciales, ciberespaciales, electrónicas y psicológicas.

Sin embargo, la misma naturaleza, ubicuidad, interconexión, globalidad y variedad de actores que interactúan en el espacio informativo obliga a que estas acciones deban realizarse tanto en tiempo de paz como en periodo de guerra, y tanto contra objetivos militares como civiles[15].

En consecuencia, los estrategas chinos entienden que actividades como las operaciones psicológicas, la propaganda política, la guerra legal o la penetración en las redes adversarias para detectar vulnerabilidades deben realizarse contra toda la sociedad tanto en tiempo de paz como antes del arranque de las hostilidades. En otras palabras, al difuminar la frontera entre la paz y la guerra mediante el establecimiento –al menos para nuestra concepción– de una amplia zona gris que se solapa con la competición pacífica, China considera legítimo emplear múltiples actividades psicológicas, propagandísticas, electrónicas o cibernéticas que no solo apoyen la consecución de la ventaja informativa en caso de crisis o conflicto, sino también apoyar –utilizando su propio enfoque integral– el desarrollo nacional en todas sus dimensiones[16].

Para llevar a cabo estos cometidos, la guerra informativa china combina una amplia gama de actividades ofensivas, defensivas y de explotación[17] junto con la protección de sus propios recursos informativos (que también supone la protección de su población frente a injerencias externas que puedan degradar la legitimidad del Partido Comunista chino)[18] y la disuasión informativa. Enmarcada dentro de la concepción china (*weishe*) que combina disuasión, persuasión y coerción, esta se vale de la dependencia global de internet para demostrar su ventaja informativa y los potenciales efectos de una potencial escalada.

Finalmente, se estima que las operaciones de información chinas en redes sociales son mucho menos sofisticadas y potencialmente disruptivas que las medidas activas digitales rusas[19]. Centradas en la difusión de narrativas que apoyen



una imagen positiva del país y contribuyan a justificar sus actividades en el exterior (desde la deslegitimación de Taiwán a la defensa de sus alteraciones del *statu quo* internacional), el control y ataque de la disidencia o la desinformación y propaganda, estas actividades sirven principalmente para apoyar las guerras psicológica, propagandística, legal y de opinión pública. A pesar de su poca madurez, las actividades informativas en redes sociales son especialmente activas tanto en el interior del país como en su área de influencia directa, tal y como ha puesto de manifiesto la ofensiva *online* que China lanzó a mediados de 2019 contra las protestas de Hong Kong[20]. No obstante, no puede descartarse que las lecciones aprendidas por el Kremlin tanto en las campañas militares de Crimea, Ucrania, Siria y de las actividades de influencia en procesos políticos extranjeros sirvan para que China amplíe sus capacidades en esta materia –tal y como está haciendo al intentar reforzar su presencia en Twitter– y plantee un enfoque más global y potencialmente disruptivo.

En conclusión, tal y como se ha explicado en las páginas anteriores, la zona gris es, por su propia naturaleza, ambigua. Esta ambigüedad es la que está facilitando que actores como China adopten estrategias multidimensionales –popularizadas como «amenazas híbridas»– para proyectar su poder negando de forma plausible su autoría, degradando la disuasión y reforzando su posición relativa en el mundo del siglo XXI. Aunque muchas de estas actividades se realizan en el plano físico, otras se realizan en el plano virtual buscando efectos en las dimensiones física, lógica o cognitiva.

Considerando la guerra informativa como el fundamento de las guerras del siglo XXI, la condición básica para poder combatir en conflictos informatizados y una herramienta susceptible de utilizarse en todo el espectro del conflicto, la guerra informativa china es mucho más amplia que la desinformación, los ciberataques o la propaganda. Con una doble vertiente –una propagandística en apoyo a la guerra política y otra militar para el logro de la ventaja informativa sobre cualquier adversario– la guerra informativa china también se emplea profusamente en actividades de explotación con APT para apoyar el desarrollo nacional y actividades específicas de disuasión informativa –incluyendo, también el *spoofing* del GPS de buques adversarios[21]– para demostrar las capacidades chinas en este dominio. No descartemos que aprenda de las lecciones rusas en materia de subversión y desestabilización en la red, del desempeño de su guerra electrónica en Siria, Ucrania o los países bálticos a la vez que continúa explotando la apertura, interconexión y dependencia occidental de Internet para proyectar su poder en la zona gris y apoyar su desarrollo nacional en un juego internacional de suma cero. ■

NOTAS

[1]Para una visión general del concepto, véase: JORDÁN, JAVIER (2018), «El conflicto internacional en la zona gris: una propuesta teórica desde la perspectiva del realismo ofensivo», *Revista Española de Ciencia Política*, núm. 48, págs. 129-151, mientras que para las zonas grises chinas, es fundamental la lectura de: MORRIS, LYLE et alt. (2019), *Gaining Competitive Advantage in the Gray Zone: Response Options for Coercive Aggression Below the Threshold of Major War*, Santa Monica: RAND Corporation y GREEN, MICHAEL (2017), *Countering Coercion in Maritime Asia: The Theory and Practice of Gray Zone Deterrence*, Washington DC: CSIS.

[2]MANDIANT (2013), *APT-1. Exposing one of China's Cyber Espionage Units*, Alexandria: Mandiant [en línea] https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

[3]Descuidada desde el fin de la Guerra Fría, la guerra electrónica no solo ha experimentado un renacimiento a raíz de las actividades rusas en Crimea, Ucrania o Siria, sino que la digitalización de las comunicaciones ha motivado una creciente convergencia entre el espacio cibernético y el radioeléctrico. Ello ha llevado al desarrollo de las *cyberspace electromagnetic activities* (CEMA).

[4]Condicionada por los efectos revolucionarios de la aplicación de las tecnologías de la información en el ámbito militar, la RMA popularizó el concepto de guerra informativa. Se asumía que esta forma de conflicto propia de la Era de la Información permitiría dañar, degradar o destruir los sistemas de información del adversario para paralizar o confundir su ciclo de toma de decisiones o paralizar su capacidad para combatir. Esta idea culminó en el concepto de guerra de mando y control, que utilizaría guerra electrónica, operaciones psicológicas, seguridad operativa y engaño para degradar los procesos de toma de decisiones del adversario (COLOM, GUILLEM (2008), *Entre Ares y Atenea, el debate sobre la Revolución en los Asuntos Militares*, Madrid: IUGM-UNED).

[5]Sin embargo, las doctrinas aliadas de operaciones de información –más restringidas que la guerra informativa planteada en los noventa en plena euforia revolucionaria– contemplan las ciberoperaciones como uno de sus componentes.

[6]LIANG, QIAO y XIANGSUI, WANG (2004), *Unrestricted warfare: China's master plan to destroy America,* Nueva York: Filament Books.

[7]Sin embargo, es posible hallar una obra china de 1985 que ya vinculaba la revolución de la información con el surgimiento de la guerra informativa (MULVENON, JAMES, «The PLA and Information Warfare», en: MULVENON, JAMES y YANG, RICHARD (eds.) (1999), The People's Liberation Army in the Information Age, Washington DC: RAND Corporation, p. 177).

[8]Para comprender estos cambios en la concepción estratégica china, es muy recomendable la lectura de la siguiente obra: MCREYNOLDS, Joe (ed.) (2017), *China's Evolving Military Strategy*, Washington DC: The Jamestown Foundation.

[9]FERGUSON, ROBYN (2011), *Information Warfare with Chinese Characteristics: China's Future of Information Warfare and Strategic Culture*, Forth Leavenworth: U.S. Army Command and General Staff College.

[10]NEWMYER, JACQUELINE (2010), «The Revolution in Military Affairs with Chinese Characteristics», Journal of Strategic Studies, vol. 33 núm. 4, págs. 483-504. De hecho, el General Wang Pufeng, considerado el «padre» de la guerra informativa china, vinculó ambas ideas cuando en la obra seminal «Guerra Informativa y Revolución en los Asuntos Militares» de 1995 (PUFENG, WANG (1995), *Xinxi zhanzheng yu junshi geming*, Pekín: Junshi Kexueyuan).

[11]YOSHINARA, TOSHI (2001), *Chinese Information Warfare. A phantom menace of emerging threat?*, Carlisle Barracks: Strategic Studies Institute.

[12]ACADEMIA DE CIENCIAS MILITARES DEL EJÉRCITO DE LIBERACIÓN POPULAR (1997), *Chinese People's Liberation Army Military Terminology*, Pekín: AMS Publishing House, págs. 764-766.

[13]Como bien resume Dean Cheng, el autor de uno de los mejores trabajos publicados sobre guerra infor-

mativa china, estas actividades de guerra política «… strive to shake the enemy's will, question their motives, induce divides and splits within the enemy's ranks, and constrain their activities […] erode an adversary's will and thus reduce the ability to sustain any resistance to more kinetic operations.» (CHENG, DEAN (2017), *Cyber dragon: Inside China's information warfare and cyber operations*, Santa Barbara: Praeger, pág. 42).

[14]Recuérdese, no obstante, que la guerra informativa apoya a las operaciones integradas que, desde una perspectiva informatizada, integran distintas fuerzas, dominios y actividades, siendo las armas de precisión de largo alcance un elemento muy relevante de apoyo para lograr el dominio informativo.

[15]A modo de ejemplo, aunque podrían relacionarse muchas actividades informativas en la zona gris, la decisión china de crear una Zona de Identificación de Defensa Aérea (ADIZ) que cubría las islas Diaoyu/Senkaku (cuya soberanía está disputada por Japón, China y Taiwán) y se solapaba con Zonas Económicas Exclusivas reclamadas por China, Japón y Corea del Sur, combinaba guerra legal con guerra psicológica y guerra informativa (WORTZEL, LARRY (2014), *The Chinese People's Liberation Army and Information Warfare*, Carlisle Barracks: Strategic Studies Institute).

[16]En consecuencia, el popular ciberespionaje industrial chino –realizado mayoritariamente por unidades vinculadas con el Ejército de Liberación Popular– no solo debe interpretarse como un medio para la obtención de información relevante para el desarrollo nacional, sino también como una herramienta para conocer al potencial adversario (JOHNSON, DEREK (2019, 6 de mayo), «How China uses cyber theft and information warfare», *Federal Computer Week* [en línea] https://fcw.com/articles/2019/05/06/china-information-warfare-dod-report.aspx

[17]Más concretamente se refieren a operaciones de información de reconocimiento, ofensivas y defensivas (recuérdese que la doctrina occidental tiende actualmente a integrarlas dentro de la ciberoperaciones), operaciones de salvaguarda de la operación y operaciones de disuasión informativa, integrando a su vez cada una de ellas una amplia gama de actividades físicas, lógicas, electrónicas y cognitivas.

[18]CHENG, *op. cit.*, págs. 53-78 y MAZARR, MICHAEL et alt. (2019), «Hostile Social Manipulation: Chinese Activities», en: *Hostile Social Manipulation. Present Realities and Emerging Trends*, Santa Barbara: RAND Corporation, págs. 105-166.

[19]COLOM, GUILLEM (2019), «¿Por qué hablamos de desinformación cuando es guerra informativa?», *Revista de Aeronáutica y Astronáutica*, núm. 888, págs. 850-855.

[20]MAZARR, op cit., pp. 113-126, y para los aspectos más actuales vinculados con las protestas de Hong Kong, véase: UREN, TOM; THOMAS, ELISE y WALLIS, JACOB (2019), *Tweeting through the Great Firewall*, Canberra: International Cyber Policy Centre – Australian Strategic Policy Institute.

[21]WOODY, CHRISTOPHER (2017, 24 de Agosto), «The Navy's 4th accident this year is stirring concerns about hackers targeting US warships», *Business Insider* [en línea] https://www.businessinsider.com/hacking-and-gps-spoofing-involved-in-navy-accidents-2017-8?IR=T