

Análisis de la actualidad internacional

La guerra informativa china: mucho más que APT y propaganda

AUTOR: Guillem Colom,
director de THIBER, the
cybersecurity think tank



Es probable que este año 2020 observemos la popularización de los conceptos de “zona gris” o “guerra informativa”. Aunque estas ideas todavía poseen valor analítico para describir realidades concretas, muy probablemente acabarán perdiendo su capacidad explicativa. Atendiendo a la misión de *THIBER, the cybersecurity think tank* de estudiar con rigor la ciberseguridad y la ciberdefensa, a continuación realizaremos un breve análisis de la concepción de guerra informativa china, que probablemente se convertirá en el nuevo *hype* de 2020.

No, la guerra informativa china no es lo mismo que la rusa. Para Pekín, ésta constituye uno de los pilares de los conflictos posmodernos, un componente transversal de las guerras futuras y una de las competencias que debe dominar el Ejército de Liberación Popular. Basada inicialmente en la emulación de los conceptos estadounidenses, ésta se ha

configurado desde la década de 1990. Teniendo como punto de partida la identificación de las lecciones de la Guerra del Golfo y el auge de la Revolución en los Asuntos Militares (RMA), su desarrollo se ha producido siguiendo los debates occidentales sobre la transformación de la guerra y dialogando con su cultura estratégica.

Asumiendo que 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. Esta transformación 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”.

Fundamentada en varias tradiciones – la guerra informatizada, la guerra política, la guerra revolucionaria o enseñanzas de Sun Tzu y de Mao Tse-Tung – y desarrollada en el marco de la RMA con características chinas, la guerra informativa china es objeto de importantes debates fuera del país.

El diccionario terminológico del Ejército de Liberación Popular la define 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 interrupción de la capacidad del adversario para transmitir la información con el objeto de establecer las condiciones necesarias para disuadir, combatir y ganar conflictos.*”. Ello requiere la ejecución de una amplia gama de actividades en el plano político (librando las guerras de opinión pública, psicológica y legal) 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.

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. 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. Al difuminar la frontera entre la paz y la

No, la guerra informativa china no es lo mismo que la rusa. Para Pekín, ésta constituye uno de los pilares de los conflictos posmodernos, un componente transversal de las guerras futuras y una de las competencias que debe dominar el Ejército de Liberación Popular.



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 actividades psicológicas, propagandísticas, electrónicas o cibernéticas que no sólo apoyen la consecución de la ventaja informativa en caso de crisis o conflicto, sino también apoyar el desarrollo nacional en todas sus dimensiones.


Para llevar a cabo estos cometidos, la guerra informativa china combina actividades ofensivas, defensivas y de explotación 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) y la disuasión informativa. Enmarcada dentro de la concepción china que combina disuasión, persuasión y coerción, ésta se vale de la dependencia global de internet para demostrar su ventaja informativa y los potenciales efectos de una potencial escalada.

Por otro lado, las operaciones de información chinas en redes sociales son mucho menos sofisticadas y potencialmente disruptivas que las medidas activas digitales rusas. 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 acti-

Al difuminar la frontera
entre la paz y la
guerra mediante el
establecimiento de una
amplia zona gris, China
considera legítimo emplear
actividades psicológicas,
propagandísticas,
electrónicas o cibernéticas

vidades informativas en redes sociales son especialmente activas tanto en el interior del país como en su área de influencia directa, tal y como puso de manifiesto la ofensiva *online* que China lanzó en 2019 contra las protestas de Hong Kong. No obstante, no puede descartarse 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.

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 – para demostrar sus capacidades. 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.



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