CIDOB opinion

E-ISSN 2014-0843

# GUERRA DIGITAL EN UCRANIA

**Carme Colomina,** investigadora principal, CIDOB
@carmecolomina

***La de Ucrania es la primera guerra viralizada, con un número de actores online sin precedentes tomando parte en la confrontación. Las grandes plataformas tecnológicas se han convertido, además, en instrumentos del conflicto: recogiendo y compartiendo datos con gobiernos, controlando la información, apuntándose a los boicots internacionales, eliminando cuentas de redes sociales, o actuando como instrumentos de movilización y emocionalidad. 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.***

720

MAYO
2022

*Una versión de este artículo se publicó previamente en *Esglobal*.

Si los mapas siempre son esenciales en cualquier conflicto, en la guerra de Ucrania hay toda una batalla de imágenes y (des)información librándose en las redes sociales. Un número de actores online sin precedentes están tomando parte en esta confrontación asimétrica, desde voluntarios de Anonymus a rastreadores digitales, los equipos de ciberdefensa de la OTAN, o el recién creado equipo cibernético de respuesta rápida de la Unión Europea, dirigido desde Lituania. Las grandes plataformas tecnológicas -sin distinción de origen, desde el Silicon Valley, a Rusia o China- se han convertido en instrumentos del conflicto: recogiendo y compartiendo datos con gobiernos, hackeando webs o controlando la información, apuntándose a los boicots internacionales, eliminando cuentas de redes sociales, o actuando como instrumentos de movilización y emocionalidad. Pero, sobre todo, la de Ucrania es la primera guerra viralizada; retransmitida en tiempo real a partir de fragmentos de imágenes que, en pocos segundos, intentan reflejar amenazas, miedos, heroicidades y devastación.

Durante las primeras semanas, *The Washington Post* pudo rastrear el movimiento de las tropas rusas en Ucrania utilizando solo videos subidos a TikTok por usuarios que iban compartiendo imágenes de tanques y soldados de manera cada vez más viral, hasta el punto que *The New Yorker* bautizó la invasión de Ucrania como "la primera guerra de Tik Tok". La aplicación china con más de mil millones de usuarios, convertida en la red social de las coreografías virales familiares en plena pandemia, se ha erigido ahora en fuente de información para centenares de miles de jóvenes, que siguen las imágenes de la guerra de Ucrania deslizando el dedo por sus teléfonos móviles. Avanzando indiscriminadamente entre la emocionalidad, las escenas bélicas y los memes, la realidad y la ficción se mezclan. Uno de los vídeos sobre Ucrania que más ha circulado por las redes, con más de siete millones de visualizaciones, donde se ven soldados fatigados despidiéndose de sus familias, resultó ser una escena de una película ucraniana de 2017.

Tik Tok se ha convertido en una fuente de galvanización de apoyo para los ucranianos, pero también en un terreno fértil para la proliferación de cuentas fraudulentas que distribuyen contenido falso con el objetivo de conseguir dinero rápido a través de vídeos que pedían donaciones para la causa ucraniana. Los creadores de contenido en esta red pueden recibir obsequios virtuales, como rosas y pandas digitales, durante las transmisiones en vivo y convertirlos en Diamantes, una moneda de TikTok que luego se puede retirar como dinero real. TikTok cobra una comisión del 50 por ciento sobre el dinero gastado en regalos virtuales. Todo el sistema ha quedado en evidencia por los deficientes controles de moderación de contenido y el negocio que hay detrás de la viralización de ciertos videos.

## Confrontación tecnológica

Los gigantes tecnológicos de Estados Unidos ejercen también de actores privados en esta guerra, alineados con la estrategia occidental, ya sea para la presión política (como Apple suspendiendo las ventas de iPhone y otros productos en Rusia) o para la captura y control tanto de datos como de información (desde el mapeo a la censura). Ante la consciencia de que Google Maps podía ser empleado como una herramienta de guerra más, tanto por el bando ruso como por el ucraniano, a la hora de confeccionar las estrategias militares, Google decidió desactivar temporalmente esta funcionalidad en esta parte del mundo. Además, el paquete de sanciones aprobadas por Estados Unidos y la Unión Europea incluye un boicot a las exportaciones tecnológicas. Microsoft, Apple, Samsung, Oracle o Cisco se han negado, desde entonces, a vender servicios en Rusia o han cerrado sus operaciones en ese país.

Esta colaboración se extiende también al terreno de la seguridad. A mediados de enero, mientras Rusia concentraba tropas y armamento en la frontera rusa al este de Ucrania, un ataque informático bautizado como el WhisperGate inhabilitó durante horas unas 70 páginas webs del gobierno ucraniano, que acabaron mostrando un mensaje que conminaba a "tener miedo y esperar lo peor". Después del hackeo, Microsoft decidió compartir su análisis y los detalles técnicos del ataque, así como recomendaciones a los afectados para aumentar su capacidad de resistencia.

Otra empresa de ciberseguridad fundada en Kíev en 2017, Hacken, ha armado un ejército de hasta 10.000 hackers en 150 países distintos, según sus propias declaraciones, dedicados a irrumpir en las plataformas de medios rusos y a amplificar las narrativas ucranianas del conflicto a través de las redes sociales.

Si esta es, como afirma el centenario filósofo francés, Edgar Morin, "la primera ciberguerra en la historia de la humanidad", Ucrania puede convertirse en el primer frente bélico donde miden sus fuerzas las dos grandes tendencias globales de digitalización: el tecnoautoritarismo y el modelo estadounidense del Silicon Valley, donde las corporaciones privadas despliegan el llamado "capitalismo de vigilancia" que denuncia Shoshana Zuboff.

Mucho antes de la invasión, el mundo digital ya había empezado a bifurcarse en una confrontación tecnológica marcada por la rivalidad entre China y Estados Unidos. La "soberanía" rusa de internet ya se construía sobre la censura de la información y la persecución de la oposición polí-

tica. Los aliados del Kremlin controlaban VKontakte, el Facebook ruso, y desde 2019 la ley sobre la soberanía de internet ya obligaba a todos los proveedores de servicios online a pasar por los filtros del censor digital Koscomnadzor. Y, a pesar de ello, la guerra ha acelerado y profundizado el alcance de este telón de acero digital que pretende aislar a los rusos de cualquier narrativa que se aleje del argumentario oficial del Kremlin para la construcción de su *casus belli*.

*En un escenario tan polarizado de guerra informativa, donde la censura y la emocionalidad narrativa se han convertido en una parte esencial del relato de bélico, la apuesta comunitaria por la supresión de determinados medios, así como la instrumentalización de los grandes monopolios digitales en favor de su propia estrategia, plantean también contradicciones con la idea de libertad de expresión defendida por unos y otros.*

El mismo fundador y CEO de la red de mensajería encriptada rusa, Telegram, Pável Dúrov, ha advertido a los internautas que "duden de tota la información" que puedan encontrar en la plataforma y ha pedido explícitamente a los usuarios que no se utilice la herramienta para "exacerbar conflictos e incitar a la discordia interétnica". Telegram se ha convertido en un instrumento perfecto para medir el choque de narrativas sobre la guerra. La plataforma se ha posicionado en los últimos tiempos como una herramienta de información muy útil para los periodistas en Ucrania, sobre todo para la creación de canales de noticias especialmente dirigidos a una audiencia menor de 25 años que ha dejado de escuchar la radio o ver la televisión tradicional. A diferencia de WhatsApp, Telegram no limita el número de usuarios en un mismo canal y, al mismo tiempo, como no hay casi moderación de contenidos, también ha funcionado como espacio de movilización del apoyo a las tropas rusas, como demuestra la capacidad de penetración del canal "Intel Slava Z".

Si, según los expertos, el estancamiento militar sobre el terreno puede acelerar la ciberguerra, a corto plazo, la estrategia rusa sigue centrada en la censura y el control del relato: en el poder de la conocida como granja de *trolls* rusa, la Internet Research Agency con sede en San Petersburgo, y en su capacidad para crear contenido y orquestar reacciones organizadas.

En el súmmum de la confusión, una investigación de Pro Publica ha demostrado como, en la guerra de Ucrania, se ha dado incluso la paradoja de utilizar falsos verificadores que aparentemente desmentían *fakes* inexistentes. Los investigadores identificaron al menos una docena de vídeos denunciando supuestas campañas de propaganda ucraniana que nunca se produjeron. El objetivo, según los expertos, sería implantar la duda ante cualquier imagen posterior que denunciara el impacto de supuestos ata-

ques rusos.

## Dilemas éticos y estratégicos

La batalla por el control del relato se libra también desde la propia Unión Europea, consciente desde hace tiempo de la capacidad de penetración e influencia rusa sobre la opinión pública europea. A petición de Bruselas, Google, Meta y Twitter decidieron tomar medidas contra las cuentas vinculadas al Kremlin para evitar la diseminación de desinformación, y especialmente el acceso a contenidos de canales oficiales rusos como RT y Sputnik; Apple retiró la app de RT News de su tienda y YouTube bloqueó el canal de noticias ruso. Anunciar la prohibición de las emisiones de RT y Sputnik en la Unión Europea no solo es políticamente arriesgado sino también difícil de imponer legalmente.

En un escenario tan polarizado de guerra informativa, donde la censura y la emocionalidad narrativa se han convertido en una parte esencial del relato de bélico, la apuesta comunitaria por la supresión de determinados medios, así como la instrumentalización de los grandes monopolios digitales en favor de su propia estrategia, plantean también contradicciones con la idea de libertad de expresión defendida por unos y otros.

La guerra híbrida expande el impacto disruptivo de una confrontación que va más allá de los avances militares rusos y la capacidad de resistencia ucraniana. Se despliega a través de la desinformación y en cada intento de infección con software malicioso de infraestructuras y vías de comunicación. *Bots*, *trolls* o *troyanos*, todo vale para debilitar al enemigo.