CIDOB opinion

E-ISSN 2014-0843

GUERRA DIGITAL A UCRAÏNA

Carme Colomina, investigadora principal, CIDOB
@carmecolomina

La d'Ucraïna és la primera guerra viralitzada, amb un nombre d'actors en línia sense precedents prenent part a la confrontació. Les grans plataformes tecnològiques han esdevingut, a més, instruments del conflicte: recollint i compartint dades amb governs, controlant la informació, apuntant-se als boicots internacionals, eliminant comptes de xarxes socials, o actuant com a eines de mobilització i emocionalitat. Ucraïna es pot convertir en el primer front bèl·lic on mesuren les seves forces les dues grans tendències globals de digitalització i les seves plataformes: el tecnoautoritarisme de Rússia i la Xina, i el model nord-americà del Silicon Valley.

720

MAIG
2022

*Una versió d'aquest article es va publicar prèviament a *Esglobal*.

Si els mapes sempre són essencials en qualsevol conflicte, a la guerra d'Ucraïna hi ha tota una batalla d'imatges i (des)informació lliurant-se a les xarxes socials. Un nombre d'actors en línia sense precedents estan prenent part en aquesta confrontació asimètrica, des de voluntaris d'Anonymus a rastrejadors digitals, els equips de ciberdefensa de l'OTAN, o el recent creat equip cibernètic de resposta ràpida de la Unió Europea, dirigit des de Lituània. Les grans plataformes tecnològiques -sense distinció d'origen, des del Silicon Valley, a Rússia o la Xina- s'han convertit en instruments del conflicte: recollint i compartint dades amb governs, piratejant webs o controlant la informació, apuntant-se als boicots internacionals, eliminant comptes de xarxes socials, o actuant com a eines de mobilització i emocionalitat. Però, sobretot, la d'Ucraïna és la primera guerra viralitzada; retransmesa en temps real a partir de fragments d'imatges que, en pocs segons, intenten reflectir amenaces, pors, heroïcitats i devastació.

Durant les primeres setmanes, *The Washington Post* va poder rastrejar el moviment de les tropes russes a Ucraïna utilitzant només vídeos pujats a TikTok per usuaris que anaven compartint imatges de tancs i soldats de manera cada vegada més viral, fins al punt que *The New Yorker* va batejar la invasió d'Ucraïna com "la primera guerra de Tik Tok". L'aplicació xinesa amb més de mil milions d'usuaris, convertida en la xarxa social de les coreografies virals familiars en plena pandèmia, ara s'ha erigit en font d'informació per a centenars de milers de joves, que segueixen les imatges de la guerra d'Ucraïna lliscant el dit pels telèfons mòbils. Avançant indiscriminadament entre l'emocionalitat, les escenes bèl·liques i els mems, la realitat i la ficció es barregen. Un dels vídeos sobre Ucraïna que més ha circulat per les xarxes, amb més de set milions de visualitzacions, on es veuen soldats fatigats acomiadant-se de les seves famílies, va resultar ser una escena d'una pel·lícula ucraïnesa del 2017.

Tik Tok s'ha convertit en una font de galvanització de suport per als ucraïnesos, però també en un terreny fèrtil per a la proliferació de comptes fraudulents que distribueixen contingut fals amb l'objectiu d'aconseguir diners ràpids a través de vídeos que demanaven donacions per a la causa ucraïnesa . Els creadors de contingut en aquesta xarxa poden rebre obsequis virtuals, com roses i pandes digitals, durant les transmissions en viu i convertir-los en Diamants, una moneda de TikTok que després es pot bescanviar per diners reals. TikTok cobra una comissió del 50 per cent sobre els diners gastats en regals virtuals. Tot el sistema ha quedat en evidència pels deficients controls de moderació de contingut i el negoci que hi ha darrere de la viralització de certs vídeos.

Confrontació tecnològica

Els gegants tecnològics dels Estats Units també exerceixen actors privats en aquesta guerra, alineats amb l'estratègia occidental, ja sigui per a la pressió política (com Apple suspenent les vendes d'iPhone i altres productes a Rússia) o per a la captura i control tant de dades com d'informació (des del mapeig a la censura). Davant la consciència que Google Maps podia ser emprat com una eina de guerra més, tant pel bàndol rus com per l'ucraïnès, a l'hora de confeccionar les estratègies militars, Google va decidir desactivar temporalment aquesta funcionalitat en aquesta part del món. A més, el paquet de sancions aprovades pels Estats Units i la Unió Europea incloïa un boicot a les exportacions tecnològiques. Microsoft, Apple, Samsung, Oracle o Cisco s'han negat, des de llavors, a vendre serveis a Rússia, o han tancat les operacions que tenien en aquest país.

Aquesta col·laboració també s'estén al terreny de la seguretat. A mitjans de gener, mentre Rússia concentrava tropes i armament a la frontera russa a l'est d'Ucraïna, un atac informàtic batejat com el WhisperGate va inhabilitar durant hores unes 70 pàgines webs del govern ucraïnès, que van acabar mostrant un missatge que comminava a "tenir por i esperar el pitjor". Després del *hackeig*, Microsoft va decidir compartir la seva anàlisi i els detalls tècnics de l'atac, així com recomanacions als afectats per augmentar la capacitat de resistència.

Una altra empresa de ciberseguretat fundada a Kíev el 2017, Hacken, ha armat un exèrcit de fins a 10.000 hackers a 150 països diferents, segons les seves pròpies declaracions, dedicats a irrompre a les plataformes de mitjans russos i a amplificar les narratives ucraïneses del conflicte a través de les xarxes socials.

Si aquesta és, com afirma el centenari filòsof francès, Edgar Morin, "la primera ciberguerra en la història de la humanitat", Ucraïna es pot convertir en el primer front bèl·lic on mesuren les seves forces les dues grans tendències globals de digitalització: el tecnoautoritarisme i el model nord-americà del Silicon Valley, on les corporacions privades despleguen l'anomenat "capitalisme de vigilància" que denuncia Shoshana Zuboff.

Molt abans de la invasió, el món digital ja havia començat a bifurcar-se en una confrontació tecnològica marcada per la rivalitat entre la Xina i els Estats Units. La "sobirania" russa d'internet ja es construïa sobre la censura de la informació i la persecució de l'oposició política. Els aliats del Kremlin controlaven VKontakte, el Facebook rus, i des del

2019 la llei sobre la sobirania d'internet ja obligava tots els proveïdors de serveis en línia a passar pels filtres del censor digital Koscomnadzor. I malgrat això, la guerra ha accelerat i aprofundit l'abast d'aquest teló d'acer digital que pretén aïllar els russos de qualsevol narrativa que s'allunyi de l'argumentari oficial del Kremlin per a la construcció del *casus belli*.

En un escenari tan polaritzat de guerra informativa, on la censura i l'emocionalitat narrativa s'han convertit en una part essencial del relat de bèl·lic, l'aposta comunitària per la supressió de determinats mitjans, així com la instrumentalització dels grans monopolis digitals a favor de la seva pròpia estratègia, plantegen també contradiccions amb la idea de llibertat d'expressió defensada pels uns i els altres.

El mateix fundador i CEO de la xarxa de missatgeria encriptada russa, Telegram, Pável Dúrov, ha advertit als internautes que "dubtin de tota la informació" que puguin trobar a la plataforma i ha demanat explícitament als usuaris que no s'utilitzi l'eina per "exacerbar conflictes i incitar a la discòrdia interètnica". Telegram ha esdevingut un instrument perfecte per mesurar el xoc de narratives sobre la guerra. La plataforma s'ha posicionat en els darrers temps com una eina d'informació molt útil per als periodistes a Ucraïna, sobretot per a la creació de canals de notícies especialment adreçats a una audiència menor de 25 anys que ha deixat d'escoltar la ràdio o veure la televisió tradicional. A diferència de WhatsApp, Telegram no limita el nombre d'usuaris en un mateix canal i, alhora, com que no hi ha gairebé moderació de continguts, també ha funcionat com a espai de mobilització del suport a les tropes russes, com demostra la capacitat de penetració del canal "Intel Slava Z".

Si, com prediuen els experts, l'estancament militar sobre el terreny pot accelerar la ciberguerra, a curt termini, l'estratègia russa continua centrada en la censura i el control del relat: al poder de la coneguda com a granja de *trolls* russa, la Internet Research Agency amb seu a Sant Petersburg, i en la seva capacitat per crear contingut i orquestrar reaccions organitzades.

Al súmmum de la confusió, una investigació de Pro Publica ha demostrat com, a la guerra d'Ucraïna, s'ha donat fins i tot la paradoxa d'utilitzar falsos verificadors que aparentment desmentien *fakes* inexistents. Els investigadors van identificar almenys una dotzena de vídeos denunciant suposades campanyes de propaganda ucraïnesa que mai no es van produir. L'objectiu, segons els experts, seria implantar el dubte davant de qualsevol imatge posterior que denunciés l'impacte de suposats atacs russos.

Dilemes ètics i estratègics

La batalla pel control del relat també es lliura des de la mateixa Unió Europea, conscient des de fa temps de la capacitat de penetració i influència russa sobre l'opinió pública europea. A petició de Brussel·les, Google, Meta i Twitter van decidir prendre mesures contra els comptes vinculats al Kremlin per evitar la disseminació de desinformació, i especialment l'accés a continguts de canals oficials russos com ara RT i Sputnik; Apple va retirar l'app de RT News de la botiga, i YouTube va bloquejar el canal de notícies rus. Però, anunciar la prohibició de les emissions de RT i Sputnik a la Unió Europea no només és políticament arriscat sinó també difícil d›imposar legalment.

En un escenari tan polaritzat de guerra informativa, on la censura i l'emocionalitat narrativa s'han convertit en una part essencial del relat de bèl·lic, l'aposta comunitària per la supressió de determinats mitjans, així com la instrumentalització dels grans monopolis digitals a favor de la seva pròpia estratègia, plantegen també contradiccions amb la idea de llibertat d'expressió defensada pels uns i els altres.

La guerra híbrida expandeix l'impacte disruptiu d'una confrontació que va més enllà dels avenços militars russos i la capacitat de resistència ucraïnesa. Es desplega a través de la desinformació i en cada intent d'infecció amb programari maliciós d'infraestructures i vies de comunicació. *Bots*, *trolls* o *troians*, tot s'hi val per debilitar l'enemic.