ieee.es
Instituto Español de Estudios Estratégicos

Documento
Opinión

70/2022 11 de julio de 2022

Fernando Frías Sánchez *

Inteligencia de Fuentes Abiertas: despejando (un poco) la niebla

Inteligencia de Fuentes Abiertas: despejando (un poco) la niebla

Resumen:

Si bien las guerras se caracterizan tanto por la confusión como por la abundancia de noticias falsas, rumores y bulos, las nuevas tecnologías han puesto a disposición de todos los usuarios múltiples herramientas de adquisición de información, gracias a las cuales se puede hacer un seguimiento mucho más exacto de lo que está pasando y lo que no está pasando, en este caso en la invasión rusa de Ucrania. La llamada OSINT (*open source intelligence,* inteligencia de fuentes abiertas) supone una revolución en el tratamiento informativo de los conflictos.

Palabras clave:

OSINT, guerra, conflictos, información, desinformación, inteligencia, análisis.

NOTA:** Las ideas contenidas en los ***Documentos de Opinión son responsabilidad de sus autores, sin que reflejen necesariamente el pensamiento del IEEE o del Ministerio de Defensa.

Open Source Intelligence: clearing (a little) the fog

Abstract:

Although wars are characterized both by confusion and by the abundance of false news, rumours and hoaxes, new technologies have made available to all users multiple information acquisition tools, thanks to which it is possible to know more exactly what is happening and what is not happening, in this case in the Russian invasion of Ukraine. The so-called OSINT (Open Source Intelligence) represents a revolution in the informative treatment of conflicts.

Keywords:

OSINT, war, conflicts, information, disinformation, intelligence, análisis.

Cómo citar este documento:

FRÍAS SÁNCHEZ, Fernando. *Inteligencia de Fuentes Abiertas: despejando (un poco) la niebla*. Documento de Opinión IEEE 70/2022. https://www.ieee.es/Galerias/fichero/docs_opinion/2022/DIEEEO70_2022_FERFRI_Inteligencia.pdf y/o enlace bie[3] (consultado día/mes/año)

> La guerra implica una incertidumbre; tres cuartas partes de las cosas sobre las que se basa la acción bélica yacen ofuscadas en la bruma de una incertidumbre más o menos intensa. Por tanto, aquí se precisa, antes que nada, un entendimiento fino y penetrante que perciba la verdad con un juicio atinado.
>
> *De la guerra*, KARL VON CLAUSEWITZ

A principios de mayo de 2022 tuvo lugar uno de los episodios más significativos de la guerra de Ucrania: el fallido intento de cruzar el río Donets por parte del ejército ruso. Desde el 4 hasta el 13 de mayo las tropas rusas intentaron cruzar el río en tres puntos, en las proximidades de las localidades de Dronivka, Serebrianka y Bilohorivka, con un resultado absolutamente desastroso: los puentes fueron detectados y la artillería ucraniana se apresuró a destruirlos, impidiendo la retirada de los contingentes que habían podido cruzar, que quedaron aislados y fueron metódicamente masacrados. En total, Rusia perdió más de setenta carros de combate y vehículos blindados, además de los cinco puentes que se llegaron a tender.

Figura 1. Restos de vehículos rusos destruidos tras los intentos de cruce del río Donets en mayo de 2022
Fuente: Fuerzas Armadas de Ucrania.

Hace pocos años habría sido difícil conocer con exactitud lo ocurrido. Si la «niebla de la guerra» de la que hablaba Clausewitz ya ponía las cosas difíciles a los presentes en el campo de batalla, quienes seguimos la guerra desde miles de kilómetros de distancia

solo podíamos esperar a que alguno de los bandos contase lo sucedido y que los corresponsales de guerra pudieran acudir a la zona. Y las noticias se limitarían a lo que esos corresponsales pudieran ver (y les dejaran ver), mezclado con la propaganda de cada uno de los bandos. Pero esta guerra es distinta: las primeras noticias de que algo serio estaba pasando en la zona empezaron a difundirse la noche del 4 al 5 de mayo, y muy poco después las imágenes de los BMP destrozados y los T-72 reventados o hundidos en el río recorrían las redes sociales cuando aún humeaban, confirmando casi en tiempo real la magnitud de la ya conocida como «batalla del río Donets» y la gravedad de la derrota rusa.

Y es que las nuevas tecnologías pueden ser un vehículo para la difusión de bulos y falsedades, como pudimos comprobar con especial intensidad durante la pandemia de la COVID-19, pero también son un medio excelente para disipar un poco esa niebla y conocer al menos una parte de la verdad.

Difundiendo noticias (y niebla): las redes sociales

En los últimos años el desarrollo de las redes sociales (entre las que se encuentran no solo las conocidas Twitter, Facebook, Instagram, etcétera, sino también los canales de WhatsApp, Telegram y otros programas de mensajería) ha permitido que las noticias, verdaderas o falsas, se distribuyan con una rapidez y un alcance sin precedentes. Desde un terremoto en Asia hasta el enésimo tiroteo en una escuela de EE. UU., desde las elecciones en algún país sudamericano hasta la aparición de un mamut congelado en Siberia, a menudo nos enteramos de las noticias en las redes antes que en los medios de comunicación; de hecho, muchas veces los medios también conocen las noticias gracias a las redes. Imágenes, tuits y vídeos transmitidos en tiempo real, a menudo por quienes están viviendo el suceso en primera persona, han hecho que nuestra época sea la más informada de la historia.

O no, porque junto a esas noticias también circulan otras erróneas o, directamente, falsas: las llamadas *fake news,* los bulos de toda la vida, forman también parte de ese inmenso flujo de datos, oscureciendo y a veces hasta ocultando la verdad. Y más aún en tiempos de guerra: la niebla de Clausewitz hoy no está formada solo por el polvo de

las cargas de caballería y el humo de los mosquetes, sino también por esa desinformación deliberada, que se usa como un arma más.

Hay algunas medidas que pueden ayudar a evitar los bulos y a que nos quedemos solo con la información solvente. Evidentemente, los canales de Telegram que llevan repitiendo día tras día desde el 24 de febrero que las tropas ucranianas dan la espalda a sus dirigentes nazis, judíos o nazi-judíos[1] y se rinden a millares, que el colapso de la resistencia se va a producir ya, ahora sí, de verdad de la buena, y que las tropas rusas van a estar desfilando por las calles de Kiev de un momento a otro no parecen una fuente demasiado fiable. Tampoco las fuentes oficiales de uno y otro bando, con su lógico interés en ocultar las malas noticias y exagerar las buenas o, si no las hay, incluso inventarlas.

Contenidos descaradamente partidistas, errores en el uso del lenguaje que revelan que el usuario está hablando de un tema que desconoce por completo, un historial previo de propagación de bulos… son pistas que nos alertan de que no debemos fiarnos de lo que nos están contando. Y, por el contrario, elegir fuentes solventes y de prestigio, recibir siempre las noticias con un sano escepticismo, analizar con cuidado las afirmaciones (especialmente las que coincidan con nuestras esperanzas y deseos, porque en esos casos será más fácil que nos dejemos engañar inconscientemente)… son algunas de las precauciones «de toda la vida» que pueden protegernos un poco de los bulos, y que siguen siendo válidas en el mundo de las redes sociales.

Pero las nuevas tecnologías nos ofrecen otras herramientas, mucho más poderosas, para conocer la verdad e incluso desenmascarar a los embusteros: las conocidas bajo el acrónimo OSINT.

OSINT: conviértase en analista sin moverse de su casa

Se denomina OSINT, *open source inteligence* o inteligencia de fuentes abiertas, a un conjunto de técnicas y herramientas que permite obtener información a partir de fuentes de carácter público.

[1] No es broma. El 1 de mayo Serguéi Lavrov, ministro de Asuntos Exteriores de Rusia, declaró en la televisión italiana: «¿Y qué si Zelenski es judío? El hecho no niega los elementos nazis en Ucrania [...]. Cuando preguntan "¿Qué clase de nazificación es esta si somos judíos?", bueno, creo que Hitler también tenía orígenes judíos, así que no significa nada».

Evidentemente, los ciudadanos de a pie no disponemos de satélites espías, redes de agentes de campo o equipos de interceptación de comunicaciones para adquirir información, pero resulta que las nuevas tecnologías han hecho que muchos datos interesantes estén ya circulando libremente y al alcance de todos, y recopilando y analizando esos datos puede obtenerse un volumen de información sorprendente.

Lo que se publica en redes sociales, como Twitter, Instagram, Facebook, etcétera, es fácilmente accesible con solo abrirse una cuenta en ellas (o, a veces, ni siquiera eso). Servicios de cartografía, como Google Maps, Google Earth, Apple Maps, etcétera, permiten localizar rápidamente cualquier lugar, consultar fotografías del mismo o incluso, en algunos casos, ver cómo ha cambiado a lo largo del tiempo. Los buscadores, como todos sabemos, nos permiten encontrar cientos de resultados tecleando una palabra o una frase, pero también pueden identificar un vehículo, un lugar o un uniforme a partir de una fotografía, reconocer y traducir carteles y textos en otros idiomas…

Otros servicios son menos conocidos, pero también extremadamente útiles. Los programas robot de archive.org visitan diariamente millones de páginas web y almacenan una captura, de modo que se puede comprobar, por ejemplo, si algún medio ha publicado una noticia que no debía y la ha suprimido a las pocas horas, como ha ocurrido varias veces en esta guerra. La captura también puede ser manual: al visitar una web podemos pedir a archive.org que almacene una copia para cotejarla con otras versiones anteriores o posteriores. Actualmente archive.org dispone de la friolera de 625.000 millones de páginas web almacenadas, lo que da una idea de la enorme cantidad de información disponible a través del servicio[2].

Pero hay más: muchos de los satélites de observación de la Tierra también son de libre acceso[3], de modo que a través de sistemas como FIRMS (Fire Information for Resource Management System, de la NASA) o EFFIS (European Forest Fire Information System, de la Unión Europea) podemos acceder a mapas que nos muestran prácticamente en tiempo real los incendios forestales… y los provocados por los combates, obviamente.

[2] Dicho sea de paso, archive.org también mantiene una extensísima biblioteca de, literalmente, millones de libros, artículos, vídeos, imágenes, obras musicales, archivos sonoros y hasta programas informáticos, de dominio público o cuyos derechos de autor han caducado, disponibles para su libre descarga o accesibles mediante un sistema de préstamo gratuito.
[3] Especialmente los de EE. UU., cuya legislación suele regirse por el principio de que los datos obtenidos mediante el uso de medios y fondos públicos son, salvo causa justificada, también públicos y de libre acceso.

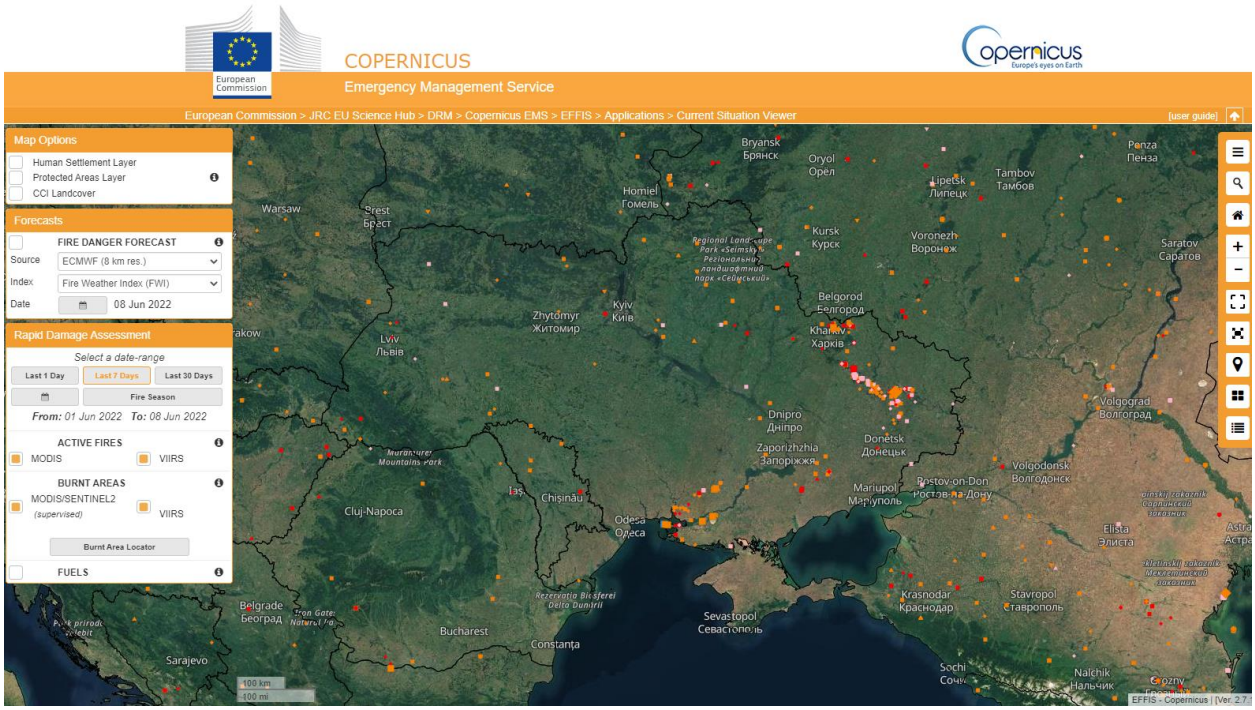

Figura 2. Mapa EFFIS de los incendios detectados en Ucrania del 1 al 8 de junio de 2022
Se aprecia fácilmente que los combates se han concentrado en los oblast de Lugansk, al este, y Járkov, al sur.
Fuente: Copernicus EMS, Comisión Europea.

La lista es muy larga, y más aún si añadimos herramientas especializadas como TheHarvester, Sherlock, Maltego..., pero creo que con lo que hemos visto nos podemos hacer una idea de la cantidad de información que se puede recopilar sin violar ninguna ley ni apuntarnos al CNI. Veamos ahora cómo se está utilizando esa información con algunos ejemplos.

La geolocalización: situándonos en el mapa

A finales de marzo de 2022 empezó a circular por las redes una imagen especialmente evocadora: en primer plano se veían los restos de un carro de combate T-72, y tras él un campo de escombros y ruinas en el que destacaba, en el centro, un pedestal con un viejo tanque T-34, que también había sido alcanzado por un proyectil.

La fotografía no incluía ninguna localización, pero unas búsquedas en internet permitían dar rápidamente con el lugar: se trataba de Trostianets, en el *oblast* de Sumi. Concretamente es la plaza del 40 Ejército, situada frente a la estación del ferrocarril; el

T-34 es el monumento a la batalla de Kursk de 1943. La foto se tomó desde la esquina de la plaza con la carretera de Vulytsya a Blahovishchenske.

En este caso bastó con consultar en una web dedicada a los T-34 cuáles se conservan aún en Ucrania, ver las fotos, dar con una localización probable y cotejarla y confirmarla mediante Google Maps y Street View. Otros son más difíciles, pero casi siempre es posible encontrar un edificio reconocible, un parche de vegetación con una forma característica, una línea eléctrica, un meandro del río…

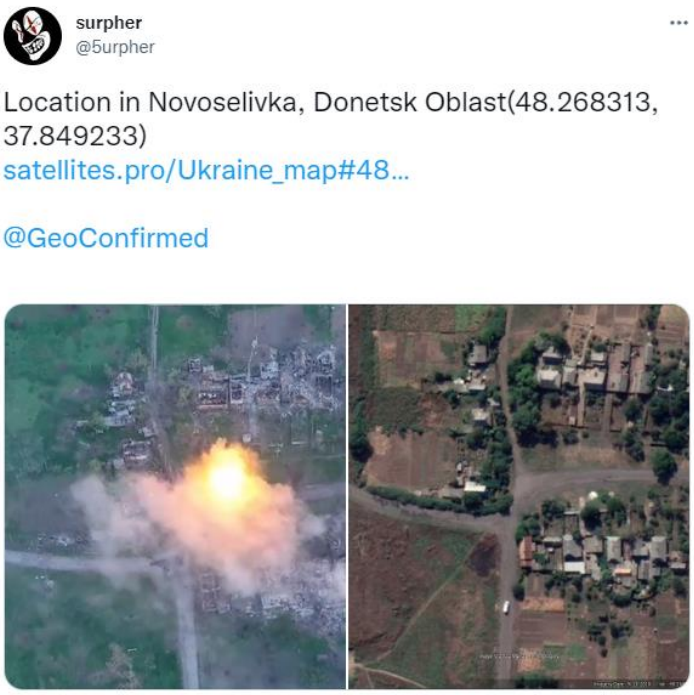

Figura 3. Geolocalizando con toda precisión el escenario de unos combates
Fuente: Twitter.

La geolocalización, que es el nombre que recibe esta técnica, permite desde localizar el lugar de un accidente o identificar el hotel donde pasan las vacaciones unos amigos hasta pasar un rato entretenido con juegos como *GeoGuessr* o *Geocaching*. Pero también permite, por supuesto, localizar el lugar de un combate, comprobar que la foto de un tanque destruido ha sido realmente tomada en Ucrania y no en Siria o Irak, ver si la imagen de una población conquistada o liberada ha sido de verdad tomada allí…

Gracias a la geolocalización podemos seguir el progreso de los avances y retrocesos con mucha más fiabilidad que si tuviéramos que confiar solo en los comunicados de uno

y otro bando. Pero claro, no solo nosotros: a lo largo de la invasión hemos visto cómo en varias ocasiones la geolocalización de un taller de reparación de carros de combate, una columna de vehículos o una patrulla de soldados ha permitido anticipar los movimientos del enemigo y preparar una respuesta, o incluso lanzar un ataque devastador con cohetes o artillería contra la posición. Poco a poco los combatientes han ido aprendiendo la lección y limitando la transmisión de imágenes en tiempo real, pero los vídeos grabados con teléfonos móviles (como los del llamado «Batallón TikTok» checheno) o el descuido de algunos medios de comunicación siguen dando algún que otro disgusto: el 20 de mayo, por ejemplo, el periodista ruso Sasha Kots, ansioso por dar por fin alguna buena noticia, publicó unas imágenes de un 2S4 Tyulpan, un poderoso mortero autopropulsado de 240 milímetros, disparando desde una posición semioculta por unos edificios; pocas horas después, y tras haber geolocalizado el lugar, la artillería ucraniana destruía el vehículo. Y seguro que no será el último caso en esta «guerra de los *smartphones*».

Contando bajas

Cuando escribo estas líneas, Rusia asegura haber destruido ya todos los vehículos blindados de Ucrania, el 117 % de su artillería, el 123 % de sus helicópteros, el 154 % de sus aviones y alrededor del 1100 % de sus drones[4]. En cuanto a las cifras de material ruso destruido que aporta Ucrania, detectar exageraciones es más difícil, dado que el inventario de Rusia es mucho mayor, pero cabe suponer que también estarán bastante hinchadas.

[4] Tomando como fuente, por un lado, los comunicados del Ministerio de Defensa ruso sobre material destruido al enemigo y, por otro, las cifras del *Military Balance* de 2022 respecto al material del que disponía Ucrania antes de la invasión. Las cifras rusas resultan aún más disparatadas si tenemos en cuenta que una parte de esos medios equipan a tropas situadas muy lejos de las líneas de combate, están en mantenimiento o reparación en talleres de retaguardia...

Figura 4. Parte de bajas ucranianas publicado por el Ministerio de Defensa ruso el 6 de junio
La mayoría de las cifras indican cantidades mayores que el total de unidades que poseía Ucrania
Fuente: Ministerio de Defensa ruso

Pero la OSINT proporciona herramientas para hacernos una idea más realista de las pérdidas que están sufriendo los contendientes. Es lo que hacen, por ejemplo, Stijn Mitzer, Joost Oliemans y sus colaboradores en la página web Oryx: cuentan las pérdidas de material, pero solo aquellas con confirmación gráfica mediante fotografías o vídeo. En su listado[5], Oryx relaciona uno por uno cada vehículo o equipo destruido o capturado con un enlace a las imágenes que permiten verificar su estado.

Por supuesto, el sistema de Oryx no es perfecto. Para empezar, es obvio que, al depender de las imágenes, no contabiliza el material cuya destrucción no cuente con confirmación gráfica, por lo que la lista tiende a quedarse corta. También puede ocurrir que se cuente como ruso material ucraniano o viceversa (recordemos que ambos bandos usan muchos equipos parecidos o idénticos), que se anote varias veces el mismo material (por usar imágenes tomadas desde distintos ángulos o en épocas diferentes) o que incluso se listen vehículos y armas destruidos en otros conflictos. Sin embargo, los autores toman toda clase de precauciones, estudiando cuidadosamente las imágenes

[5] ORYX. «Attack on Europe: Documenting Russian equipment losses during the 2022 Russian invasion of Ukraine». 24 de febrero de 2022. Disponible en: https://www.oryxspioenkop.com/2022/02/attack-on-europe-documenting-equipment.html

para determinar el modelo concreto que aparece en ellas, el esquema de pintura y las marcas tácticas que muestra, qué otros vehículos o armas aparecen asociados… La geolocalización es aquí, de nuevo, clave, junto con la colaboración de numerosos internautas que vigilan para evitar errores y duplicidades.

Figura 5. El cada vez más largo listado de carros de combate perdidos por Rusia cuya destrucción o captura ha podido ser verificada con imágenes
Fuente: Oryx.

Más difícil resulta contar las bajas humanas, pero los miembros de un grupo llamado Inform Napalm encontraron una curiosa manera de estimarlas haciendo uso, nuevamente, de fuentes públicas. El 3 de marzo de 2022 las Fuerzas Armadas rusas otorgaron a todos los caídos durante la primera semana de la invasión la Orden al Coraje, una medalla acompañada de un certificado conmemorativo, fechado y numerado. Y, como es natural, en las redes aparecieron muchos obituarios en los que los afligidos parientes mostraban con orgullo la medalla y el certificado. Así que los miembros de Inform Napalm rastrearon internet buscando imágenes de los certificados expedidos con esa fecha, anotando los números de serie. El más bajo que encontraron era el 78.487 y el más alto, el 83.281, por lo que una simple resta permite comprobar que durante la primera semana de guerra murieron al menos 4.794 soldados rusos[6]. Con esa misma fecha el Ministerio de Defensa ruso admitía tan solo 498 fallecidos.

[6] INFORM NAPALM. «Medal count: OSINT analysis of real Russian losses for the first week of hostilities in Ukraine». 25 de marzo de 2022. Disponible en: https://informnapalm.org/en/medal-count-osint-analysis-of-real-russian-losses-for-the-first-week-of-hostilities-in-ukraine/

Antes se pilla a un mentiroso…

Lo cual nos lleva a otra utilidad de las herramientas OSINT: la detección de bulos, engaños o incluso simples errores.

Y de quienes los difunden. Existen herramientas que permiten comprobar quién lanza un bulo, quiénes lo replican… Los resultados son a menudo sorprendentes (o quizá no tanto). Por ejemplo, es bastante habitual que los bulos no partan de una sola cuenta, sino de muchas a la vez. Puede tratarse de personas reales que se coordinan, pero es más habitual que se trate de *bots,* programas informáticos diseñados para parecerse a personas, cuya actuación simultánea, en cualquier caso, permite multiplicar el alcance de los mensajes. La redifusión de los mensajes (mediante retuits, nuevas publicaciones, nuevos envíos de la misma publicación, etcétera) también está automatizada, con intervalos calculados para esparcirlos al máximo.

Otra característica de estas redes de difusión de bulos, denominadas *troll farms,* es que lo hacen con asiduidad y en relación con los temas más insospechados. Se han identificado redes que han ido apoyando a los partidos de ideologías extremas en diversos procesos electorales, que difundieron mensajes sobre presuntos excesos de las Fuerzas de Seguridad en el referéndum ilegal de autodeterminación de Cataluña, que luego se dedicaron a negar la existencia de la COVID o la eficacia de las vacunas, y que ahora nos cuentan que los soldados ucranianos son nazis, que sus Fuerzas Armadas están en realidad dirigidas por oficiales occidentales disfrazados y que se están rindiendo en masa ante los libertadores rusos. Más allá de la difusión de mensajes concretos, el objetivo de estas redes parece ser únicamente el de crear confusión, polarizar a los electores y la opinión pública y fomentar la desconfianza en los dirigentes occidentales y los regímenes democráticos.

Pero, aunque nos topemos con ellas muy a menudo, la detección e identificación de estas redes requiere programas especializados de rastreo y recopilación de datos, y en este escrito nos estamos limitando a las herramientas más básicas, al alcance de cualquiera. Y es que para detectar bulos también pueden servir nuestra ya conocida geolocalización o incluso eso tan difuso, pero a veces tan útil, que se suele denominar «inteligencia colectiva».

Puede que personalmente seamos un desastre a la hora de calcular o estimar algo a ojo, pero hay experimentos que demuestran que una estimación colectiva, es decir, la formada por un buen número de estimaciones individuales, suele ser bastante más correcta que cada una de esas estimaciones individuales. Desde el número de peces en un acuario hasta la extensión territorial de un país, desde la edad de un árbol hasta el estilo arquitectónico de un edificio, la suma de muchas opiniones suele ser bastante más acertada que las opiniones personales aisladas.

Esto se debe, por un lado, a que con un número suficientemente alto de personas los errores de unos y otros tienden a compensarse, pero también a que suele producirse un cierto efecto de llamada: una pregunta sobre una determinada materia llamará más la atención a los interesados en esa materia, cuyas respuestas serán por regla general mejor informadas y, por tanto, más precisas que las de los legos.

A la hora de analizar la información sobre la guerra ocurre lo mismo: son muchos los ojos que la observan, y aunque entre ellos hay desde simples curiosos hasta los inevitables fanáticos de uno u otro bando, podemos tener la seguridad de que muchos de esos observadores serán profesionales o, como mínimo, aficionados a los temas militares, las armas y materiales, la historia, la geografía…, lo que proporciona una cierta calidad a su análisis colectivo.

Así, a la mayoría de los mortales nos puede resultar difícil distinguir un T-72 de un T-80, y no hablemos ya de identificar una variante concreta, pero hay quienes son capaces de hacerlo de un solo vistazo. Y podemos estar seguros de que muchos de ellos analizarán los comunicados, los vídeos, las fotos y, en fin, todo ese material que al fin y al cabo les interesa y atrae.

Este análisis más o menos informal ha permitido descubrir que algunas veces se nos han presentado imágenes de vehículos capturados o destruidos que en realidad son el mismo. Fotografías tomadas desde diferentes ángulos o en diferentes épocas del año (de modo que la vegetación del entorno parezca distinta), vídeos grabados inmediatamente después de la captura y tras la reparación, puesta a punto y repintado, imágenes de vehículos que luego han sido volados con explosivos y vueltos a fotografiar, el inevitable Photoshop… Hemos visto de todo.

Incluyendo casos de lo más chusco: hemos podido ver, por ejemplo, un vídeo de un carro de combate ruso arrastrando a un carro ucraniano capturado; el vídeo original mostraba justo lo contrario, pero los propagandistas del Kremlin lo reprodujeron marcha atrás. Restos de varios drones capturados que mostraban las mismas marcas y hasta el mismo número de serie, lo que demostraría que se trataba de los fragmentos de uno solo ordenados de distinto modo; imágenes de otro dron supuestamente capturado intacto, pero que en realidad estaba formado por fragmentos de dos modelos distintos chapuceramente unidos; restos de carros, aviones o helicópteros presentados como enemigos, pero que en realidad corresponden a modelos que usa solo el bando que asegura haberlos destruido…

Por supuesto, no faltan las fotos de soldados en lugares que, debidamente geolocalizados, resultan no ser los que ellos dicen (de hecho, lo más habitual es que estén bastante más hacia la retaguardia). Y también se nos ha colado alguna otra foto de material destruido en Chechenia o Siria, épicos avances que fueron grabados durante maniobras militares en tiempos de paz y una abundante cantidad de vídeos de fuego antiaéreo que en realidad son capturas de videojuegos. Incluso un impresionante vídeo en el que se veía al crucero Movska siendo alcanzado por los misiles Neptune ucranianos resultó ser la secuencia del hundimiento en 2013 de la vieja fragata Trondheim durante unas maniobras con fuego real de la Armada noruega.

Pero a las pocas horas, a veces a los pocos minutos, todos ellos han sido refutados.

Figura 6. El 16 de mayo fuentes prorrusas difundieron imágenes de supuestos soldados ucranianos caídos en un intento de recuperar la Isla de las Serpientes, pero el único rasgo identificable de sus uniformes, la hebilla del cinturón, mostraba que se trataba de infantes de Marina rusos
Fuente: Twitter.

Descubrir el rastro de la manipulación digital de unas imágenes, identificar la nacionalidad de un soldado caído al ver la hebilla de su cinturón, reconocer a qué modelo pertenecen los restos de un helicóptero viendo unas cuantas piezas rotas o saber qué arma (y de qué bando) ha destruido un tanque observando los restos del misil que lo alcanzó son cosas que no están a mi alcance ni al de la mayoría de las personas. Pero sí al de más de un profesional de la edición digital, un aficionado a los uniformes, un fanático de la aviación o un experto en armas anticarro. Y de ellos siempre va a haber unos cuantos mirando las imágenes con todo detenimiento y contribuyendo a la veracidad de ese análisis colectivo.

Un caso práctico: la batalla del río Donets

Pero la mejor manera de ver cómo se conjugan todas estas herramientas es con un caso práctico: hablemos del incidente con el que empezábamos este artículo, la batalla del río Donets.

Las primeras pistas de que pasaba algo las proporcionaron, cómo no, los satélites de vigilancia contra incendios: desde la noche del 4 al 5 de mayo se multiplicaron los fuegos en la zona, coincidiendo con los tres ejes de los tres ataques rusos sucesivos: el 5 se concentraban en Serebrianka, el 6 en Dronivka y el 7 en Bilohorivka. Luego los fuegos se retiraron de nuevo al norte del río, ocupando casi toda la zona boscosa el día 6 y los siguientes.

Las imágenes publicadas en las redes sociales, rápidamente geolocalizadas, y las imágenes de satélite permitían comprobar lo que había pasado: el 5 los rusos cruzaron el Donets a la altura de Serebrianka, consiguiendo hacer llegar un gran contingente hasta la orilla sur. El contingente se desplegó rápidamente, pero no lo suficiente: fue duramente batido por los ucranianos, especialmente por la artillería, que además destruyó el puente, impidiéndoles la retirada.

El día 6 se produjo un nuevo intento, esta vez más al oeste, en Dronivka. Las imágenes, muy fáciles de identificar, ya que los rusos aprovecharon una zona por la que pasa una línea de alta tensión y que por tanto permanece despejada de vegetación, formando una especie de camino entre los densos bosques, muestran que los puentes fueron destruidos casi inmediatamente, y solo pudieron cruzar el río algunas unidades anfibias

de vanguardia que, también atacadas por los ucranianos, tuvieron que retirarse o fueron destruidas.

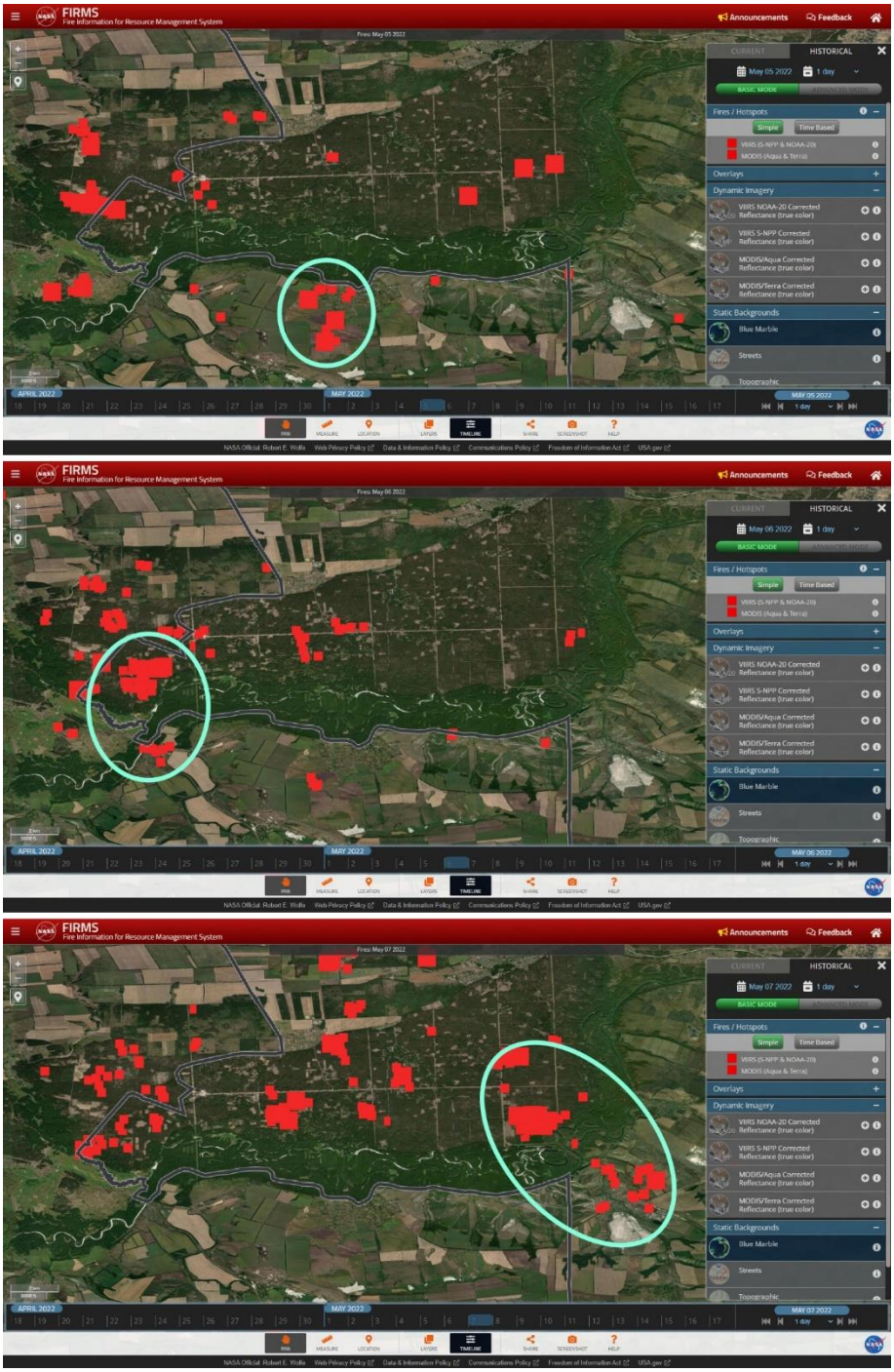

Figura 7. Imágenes del sistema FIRMS de los días álgidos de la batalla
Las áreas con mayor cantidad de incendios, marcadas con óvalos, se corresponden con los combates en los intentos de cruce del Donets en Serebrianka (5 de mayo), Dronivka (6 de mayo) y Bilohorivka (7 de mayo). Fuente: NASA/FIRMS y elaboración propia.

Y el 7, en fin, los rusos volvieron a cruzar el río, esta vez por Bilohorivka, con un resultado similar al del primer día: los ucranianos destruyeron los puentes dejando aisladas a las tropas que habían conseguido cruzar, que fueron nuevamente aniquiladas.

Figura 8. Geolocalización del lugar de intento de cruce del río en las cercanías de Dronivka
Las torres del tendido eléctrico (flechas rojas) y el propio tendido (flechas amarillas) son clave en su identificación
Fuente: Fuerzas Armadas de Ucrania, Google Maps y elaboración propia.

El 8 y el 9 aún se registra algún fuego al sur del río, quizá indicativo de que todavía quedaban unidades rusas combatiendo, pero al día siguiente ya no hay ninguno: los fuegos se trasladan después al norte del Donets, siendo ya seguramente una mezcla de bombardeos artilleros ucranianos e incendios forestales provocados por los rusos para cubrir su retirada de la zona.

Como decíamos al principio, hace pocos años habríamos conocido una batalla así tarde, seguramente de forma fragmentaria, y probablemente al gusto de quien nos la contara. Y ahora, sin embargo, hemos podido vivirla prácticamente en directo, con múltiples fuentes corroborándose unas a otras y dejando poco margen a tergiversaciones o engaños. No solo hemos sabido cuándo y cómo se movían las tropas y dónde se producían los combates, sino que hemos podido hasta contar uno por uno los vehículos destruidos, abandonados o hundidos en el río, haciéndonos una idea exacta de la magnitud de la batalla.

Y es que la niebla sigue, y quizá más espesa que nunca. Pero ahora tenemos herramientas que pueden ayudar a despejarla...

*Fernando Frías Sánchez**
@FerFrias