



# Cuando el ciberfrente decide la guerra: lecciones desde Ucrania

Desde el inicio de la invasión rusa, los especialistas del **Departamento de Ciberseguridad del Servicio de Seguridad de Ucrania** (SSU) han neutralizado más de 14.000 ciberataques contra organismos del gobierno central y la infraestructura crítica. “La guerra en Ucrania ha demostrado que la agresión basada en el ciberespacio es un componente esencial de la doctrina militar rusa. Esta amenaza sólo se expandirá en el futuro. Tanto para Ucrania como para sus socios”, advertía en 2024, en **Revista SIC**, el general **Oleksandr Potii**, en nuestro Especial anual de Ciberamenazas.

Este **24 de febrero** se cumplirán cuatro años del mensaje televisado de **Vladimir Putin**, con el que anunció una “operación militar especial” con la que comenzó la invasión de Ucrania. Una guerra que ha transformado el



## Ucrania se ha convertido en el cortafuegos de Europa y en el epicentro donde se redefine el concepto de ciberguerra

equilibrio geopolítico global y que ha llevado al límite el uso de tecnologías emergentes: desde la inteligencia de datos hasta la inteligencia artificial, pasando por los drones y la automatización del combate y la ciberguerra en una lógica de conflicto continuo, sin fronteras claras entre la paz y la guerra. En este contexto también ha tomado forma de modo muy explícito la **guerra híbrida**, aprovechando zonas grises para inclinar la balanza estratégica.

Con el deseo, más urgente que nunca, de que la paz llegue a Ucrania en 2026, siempre con una oración por los muertos, heridos y el sufrimiento indescribible que vive el país, resulta pertinente leer –en detalle y con la profundidad que requiere– los últimos cuatro **‘Especiales de Ciberamenazas’** de Revista SIC (nº153, 158, 163 y 168). En ellos se cuenta con la visión, ‘desde el frente’, de dos referentes como **Victor Zhora**, entonces CDTO y ahora vicepresidente del **Servicio Estatal de Comunicaciones Especiales y Protección de la Información** (SSSCIP), el primer año, y el ya citado general Potii, presidente del organismo, estos tres últimos.

Es especialmente ilustrativo, en este número de SIC, cómo éste anticipa que Ucrania se prepara, más que nunca, “para las ciberamenazas impulsadas por la IA”, subrayando que, aunque, tras no lograr sus objetivos estos cuatro años, “el volumen de ataques, ya sean drones, misiles o ciberataques, por parte de Rusia, no hace más que aumentar”. Advierte, además, que se ve cómo “el uso de IA reduce significativamente la barrera para la creación de

nuevas ciberamenazas”. Una visión, desde el cibercampo de batalla, que hemos tenido el privilegio de publicar, año tras año y en la que destacó como en **2022**, los ataques se centraron en destruir infraestructuras informáticas y exfiltrar bases de datos; en **2023**, en la destrucción sistemática de infraestructuras, incluidos proveedores de Internet, ministerios y agencias; y en **2024**, las acciones se orientaron a “todo lo relacionado con el teatro de operaciones”, buscando mantener “una **presencia persistente y encubierta** en sistemas clave para la guerra y la política”.

Ya en 2023, Zhora, por su parte, advertía de la necesidad de “crear un sistema de defensa colectiva en el ciberespacio, a medida que aumentan las ciberamenazas, el mundo debe estar preparado para afrontarlas antes de que sea demasiado tarde”.

Occidente intenta hacer los deberes, con mayor o menor acierto. Prueba de ello es que en diciembre **Consejo de Europa** sancionó a **12 personas y dos entidades rusas**, –alcanzando ya las 57 y 19, respectivamente– entre ellas miembros del la unidad **29155 del GRU**, el grupo de ciberamenazas **Cadet Blizzard**, el **Movimiento Rusófilo Internacional** y el **142.º Batallón de Guerra Electrónica Separada**, vinculado a interferencias y fallos de señal GPS sufridos en países de la UE.

Leí recientemente que Ucrania es el cortafuegos de Europa y pocos dudan de que lo que allí ocurra tendrá consecuencias directas sobre nuestras vidas. De hecho, ya ha cambiado el concepto mismo de ciberguerra. El futuro dirá si hemos hecho lo suficiente para preservar en el ciberespacio la paz que buscamos en el mundo físico.

Decía la madre Teresa que la “paz empieza por una sonrisa”; ojalá llegue este año a Ucrania.

Y en esta guerra no quiero olvidar a los **criptógrafos**, siempre en la sombra, asegurando las comunicaciones. Bajo el título *“Criptógrafos que salvaron el mundo y ‘casi’ nadie recuerda”* tendré el privilegio de impartir una conferencia en el track de **Criptored**, durante **RootedCON 2026**, en paralelo a la primera gran exposición dedicada a **Enigma** y a la historia de la criptografía, que acogerá el congreso el próximo **5 de marzo**.



**José Manuel Vera**  
Redactor  
**Revista SIC**