# La guerra cibernética que se vive detrás de la guerra en Ucrania

Rusia ha intentado 'hackear' a más de 40 países aliados de Ucrania desde el inicio de la guerra

David Gómez Correa

Edición Textual

Septiembre 6 del 2022

**Palabras clave:** Guerra Ucrania, Rusia, ciberataques, Microsoft, ciberseguridad.

El presente informe enunciativo busca abordar la noticia escrita por Rodrigo Alonso titulada: “Rusia ha intentado 'hackear' a más de 40 países aliados de Ucrania desde el inicio de la guerra”, publicada por el diario ABC el 23 de agosto del 2022. La noticia presenta como tema los ciberataques lanzados por Rusia, analizando principalmente la poca efectividad por parte de estos. Así, en primer lugar, se explicará la importancia del ciberespacio en la guerra de Ucrania; en segundo lugar, se expondrá los principales blancos rusos y la mesura tomada por el país, para finalizar con una síntesis de lo descrito.

El ciberespacio en la guerra de Ucrania ha jugado un papel muy importante durante los cuatro meses que han transcurrido. Menciona la empresa Microsoft en su informe que se han lanzado ataques contra, al menos, 128 infraestructuras de 42 países. Dichas actividades no solo se concentran en su principal objetivo, Estados Unidos, sino que además incluyen países bálticos como Dinamarca, Noruega, Finlandia, Suecia y Turquía.

Igualmente, añade la empresa Microsoft que durante los últimos cuatro meses han aumentado los intentos de ‘hackeo’ contra varios países de la OTAN. Menciona Alonso (2022) que: “la mayoría de los ciberataques rusos contra países extranjeros aliados de Ucrania han estado dirigidos, precisamente, contra sitios gubernamentales.” (2022, párr. 3).

No obstantes, el éxito de los intentos rusos se limita a un 29%, de acuerdo con las cifras que maneja Microsoft. La empresa pone en valor la preparación de Ucrania, que preventivamente migro gran parte de datos y sistemas a la nube, en servidores extranjeros. También, anexa Alonso (2022), que en buena medida se debe a la lección aprendida por Ucrania, que en los últimos años ha funcionado como sujeto de pruebas de amenazas cibernéticas de todo tipo (párr. 6).

Sumada a la baja tasa de efectividad, los golpes realizados no han sido especialmente severos. Esta situación ha sorprendido a muchas empresas de ciberseguridad; porque, las vulnerabilidades presentes tanto en empresas, como en instituciones gubernamentales, sigue siendo grande. Agrega Alfonso (2022) que: “además, se sabe que países como Estados Unidos han estado lanzando ciberataques contra Moscú.” (2022, párr. 9), situación que aumenta el desconcierto por parte de las empresas. En opinión de Albors, eso se debe al interés del país ruso de no escalar el conflicto hasta cotas más altas.

En síntesis, los ataques lanzados por Rusia han sido poco efectivos, en gran parte, por las medidas tomadas Ucrania y, por el interés ruso de no escalar el conflicto. Se puede afirmar que el informe cumplió su cometido, pues planteo el contexto de la ciberguerra en Ucrania y los aspectos mas relevantes que subyacen sobre esta. Para finalizar, es importante preguntarnos si la falta de efectividad de Rusia se debe a las mejoras en la ciberseguridad o son tácticas premeditadas.

**Referencia:**

Alonso, R. (2022, 23 junio). Rusia ha intentado ‘hackear’ a más de 40 países aliados de Ucrania desde el inicio de la guerra. *ABC*. <https://www.abc.es/tecnologia/redes/abci-rusia-intentado-hackear-mas-40-paises-aliados-ucrania-desde-inicio-guerra-202206231128_noticia.html?ref=https%3A%2F%2Fwww.abc.es%2Ftecnologia%2Fredes%2Fabci-rusia-intentado-hackear-mas-40-paises-aliados-ucrania-desde-inicio-guerra-202206231128_noticia.html>