22/05/2022

ECONOMIST&JURIST

Cristina Cajigos
Key Account Manager en Grupo Paradell

¿Cómo afecta el conflicto ruso a la ciberseguridad de tu empresa?

Rusia es una superpotencia económica y cibernética. Las **empresas de cibercrimen rusas** están profesionalizadas y la única condición que les impone el Kremlin es que operen fuera del territorio ruso. A partir de aquí, no tienen restricción alguna. Por tanto, disponen de una gran capacidad para realizar ataques de gran alcance y gravemente destructivos.

Es importante que diferenciemos entre una guerra digital establecida por un gobierno, que dispone de un equipo de *hackers* y que tienen como objetivo el pentágono, infraestructuras críticas y esenciales, etc.; de los **ciberataques**, dirigidos por **ciberdelincuentes** cuyo único objetivo es la recompensa económica.

Se han dado muchos ciberataques a infraestructuras críticas: energía, agua, hospitales etc., pero para que podamos definirlo como **guerra digital**, además, se deben consultar las más de 95 reglas del Manual de Tallinn que establecen en qué momento un ataque se puede considerar violación del Derecho Internacional y cuándo y cómo los Estados pueden responder a ellos.

"Para que podamos definirlo como guerra digital, además, se deben consultar las más de 95 reglas del Manual de Tallinn" (Foto: E&J)

Ucrania, además del ataque bélico, ha sufrido **ciberataques en Kiev** que han paralizado su inf ...