¿NOS ENCONTRAMOS ANTE UNA GUERRA CIBERNÉTICA ENTRE LA UNIÓN EUROPEA Y RUSIA?

RESUMEN EJECUTIVO

La relación entre la Unión Europea, en adelante UE y la Federación Rusa, en adelante Rusia, se enfrenta a retos como son los conflictos cibernéticos y la desinformación, agravados por el uso estratégico de recursos energéticos por parte de Rusia. La Unión Europea está respondiendo con medidas de ciberseguridad y regulaciones. La interdependencia energética entre las partes complica la situación. La resiliencia y coordinación interna de los países de la Unión Europea es crucial para ofrecer una respuesta conjunta. Como la atribución de ciberataques es compleja, una escalada parece improbable, ya que ambas partes se benefician económicamente del comercio de energías y recursos.

I. CONTEXTO HISTÓRICO Y GEOPOLÍTICO

Las relaciones entre la UE y Rusia se remontan al final de la Guerra Fría, con la firma del Acuerdo de Asociación y Cooperación en 1994. Sin embargo, las tensiones, agravadas por eventos como la anexión de Crimea en 2014, han caracterizado gran parte de esta relación. El conflicto en Ucrania ha generado sanciones económicas y preocupaciones en el Cáucaso y el Báltico, añadiendo de esta forma capas adicionales de complejidad a la dinámica regional.

II. CIBERSEGURIDAD EN LAS RELACIONES UE-RUSIA

Rusia es una de las naciones más activas en ciberataques y ha llevado a cabo diversas acciones, desde ataques de denegación de servicio hasta la persecución de ciberdisidentes. Su impacto es significativo, representando el 58% de los ciberataques observados por Microsoft en el año 2021, con un 32% de éxito. Ante esta amenaza, la UE ha implementado medidas estrictas de ciberseguridad y fortalecido la cooperación internacional. En 2021, adoptó la Estrategia de Ciberseguridad para la Década Digital, buscando un ciberespacio global basado en el Estado de Derecho y valores democráticos.

La creación de la Agencia de la Unión Europea para la Ciberseguridad (ENISA) refleja su compromiso en mejorar la ciberseguridad y fomentar la colaboración entre los Estados miembros. Sin embargo, tanto la UE como Rusia han sido acusadas mutuamente de llevar a cabo ataques cibernéticos, sumergiendo la esfera digital en una guerra silenciosa donde la información y la infraestructura son objetivos cruciales.

III. ESTRATEGIAS UTILIZADAS POR RUSIA

- **Guerra de información y desinformación:**

La estrategia de desinformación de Rusia, arraigada desde la Guerra Fría, se centra grupos específicos a los que atacar y utiliza medios convencionales, cibernéticos y redes sociales para influir en ciudadanos rusos, minorías en antiguas repúblicas soviéticas y audiencias occidentales. Busca desestabilizar democracias y favorecer partidos afines al Kremlin. Ante ello, la UE responde con un Plan de Acción contra las noticias falsas, estableciendo equipos de alerta rápida, cooperación con la Organización del Tratado del Atlántico Norte, en adelante OTAN, promoción de la alfabetización mediática y regulación de plataformas digitales. Por otra parte, la Ley de Servicios Digitales se centra en regular algoritmos y combatir campañas de desinformación con *bots* y cuentas falsas. En conjunto, la UE está adoptando medidas integrales para contrarrestar la amenaza de desinformación rusa.

- **Guerra cibernética:**

La guerra cibernética entre Rusia y la UE es un conflicto de baja intensidad, pero alto impacto, caracterizado por el uso de medios híbridos y asimétricos. Con graves consecuencias para la seguridad, economía y política de la UE, la cual se está

enfrentando a una serie de amenazas como espionaje, sabotaje, desinformación e influencia electoral por parte de Rusia. Esta serie de ciberataques buscan poner en riesgo la integridad territorial, soberanía y valores democráticos de la UE.

En respuesta, la UE ha impuesto sanciones económicas y diplomáticas a raíz de la invasión de Ucrania por parte de Rusia y ha reforzado su defensa cibernética, cooperando con la OTAN, desarrollando estrategias de resiliencia digital y creando mecanismos de alerta rápida. Además, brinda apoyo a Ucrania con asistencia financiera y humanitaria. En cuanto a Rusia, ha llevado a cabo ciberataques notables, como el ataque a la red eléctrica de Ucrania en 2015 y otros contra instituciones europeas. La amenaza cibernética de Rusia exige una respuesta integral y coordinada por parte de la UE.

- **Recursos energéticos como herramienta política:**

Rusia utiliza sus vastos recursos naturales, especialmente energéticos, como herramienta para ejercer liderazgo en Europa. Aunque la UE ha intentado diversificar su economía, la interdependencia persiste, siendo alrededor del 40% de las exportaciones de gas natural de la UE provenientes de Rusia. A pesar de los esfuerzos posteriores a la invasión de Ucrania, algunos países, como Alemania e Italia, mantienen una fuerte dependencia del gas y petróleo rusos. Proyectos de gasoductos, ahora paralizados, como Nord Stream, Turk Stream y South Stream ilustran esta intensa relación comercial. También, es habitual el comercio con tierras raras y minerales necesarios para la industria de la Unión Europea.

Rusia, afectada por sanciones internacionales, bajos precios de energía y la competencia, es consciente de la importancia de mantener este comercio con la UE debido a la demanda, rentabilidad y seguridad jurídica que ofrece.

- **Injerencia en asuntos internos:**

Rusia ha sido acusada de intervenir en asuntos extranjeros, utilizando diversas tácticas como financiamiento a partidos afines, respaldo a movimientos separatistas y manipulación de procesos electorales. Destacó su injerencia en las elecciones estadounidenses de 2020, favoreciendo a Donald Trump. En conflictos recientes, como Siria y Ucrania, aplicó medidas estratégicas. En Siria, desplegó una narrativa alternativa desde 2011, calificando la revolución contra Asad como lucha antiterrorista, influyendo en políticas occidentales y sembrando confusión. En Ucrania, tras el Euromaidán en 2013, combinó desinformación, acciones cibernéticas y envío de tropas sin identificación para anexar Crimea en 2014. Las campañas de desinformación negaron la implicación rusa y debilitaron la credibilidad ucraniana, las cuales han sido acompañadas de ciberataques.

- **Refuerzo de alianzas estratégicas:**

Un aspecto que Rusia ha reforzado para protegerse respecto a posibles amenazas surgidas a raíz de la invasión de Ucrania es su alineamiento con otros actores internacionales a nivel militar o político que comparten sus mismos intereses sobre soberanía o multipolaridad. Estas alianzas han sido principalmente con países como China, Irán, Venezuela, Corea del Norte, Bielorrusia, India o Armenia. Las cuales se posicionan frente a la influencia ejercida por la OTAN.

IV. CONCLUSIONES

El conflicto cibernético entre la Unión Europea y Rusia, agravado por tensiones históricas y la situación en Ucrania, presenta retos significativos, marcados por tácticas agresivas, ciberataques y desinformación. La UE está respondiendo con medidas proactivas, destacando la importancia de la resiliencia y coordinación interna entre sus miembros. La interdependencia económica entre ambas partes actúa como un elemento de contención, evitando una escalada militar. En este complejo escenario, la necesidad de una respuesta integral y coordinada se vuelve evidente para preservar la integridad territorial y los valores fundamentales de la UE frente a las amenazas cibernéticas de Rusia.

En definitiva, podemos decir que sí que nos encontramos ante una guerra cibernética donde se están produciendo constantes ataques y contraataques en la sombra, donde es muy complicado demostrar realmente el origen y la autoría y siempre con precaución de no ir un paso más allá. Ambos actores internacionales son conscientes de la interdependencia económica que tienen y son conocedores de que un enfrentamiento militar que convierta occidente en un campo de batalla sería devastador para las economías de Rusia y la UE. Las diferentes organizaciones de las que forman parte tanto la UE como Rusia en materia de ciberseguridad y la pertenencia a la Organización para la Seguridad y la Cooperación en Europa (OSCE) deberían de facilitar el acuerdo para el cese de las hostilidades o, al menos, para evitar algún tipo de escalada en el conflicto.