Universitat Autònoma de Barcelona

FACULTAD DE CIENCIAS POLÍTICAS Y SOCIOLOGÍA

GRADO EN CIENCIA POLÍTICA Y GESTIÓN PÚBLICA

RESUMEN EJECUTIVO

El ciberespacio, el poder del siglo XXI

Análisis del impacto de la ciberseguridad en las dinámicas de poder del sistema internacional

ESTUDIANTE: Álvaro Franco, 1604400

TUTOR: Pablo Aguiar Molina

Barcelona, mayo 2024

Al sistema internacional se ha incorporado, durante las últimas décadas, una dimensión antes desconocida. La configuración del sistema, el poder, las guerras o las capacidades materiales de los actores internacionales se han adaptado a los nuevos tiempos y, consecuentemente, a las nuevas tecnologías. Internet, un espacio digital tan amable y útil para la vida cotidiana del ciudadano es, ahora, un nuevo espacio de interacción donde tanto cooperación como conflicto aparecen.

Aunque las armas convencionales no se han abandonado, Internet puede llegar a ser una nueva arma que abre oportunidades para amenazar y comprometer nuestros datos, la integridad funcional y seguridad, incluso, de estados y empresas.

El espacio cibernético, implica, consecuentemente, la existencia de una herramienta de doble filo. Una nueva amenaza presupone una nueva necesidad de seguridad y de ello, tanto los Estados como otros actores no estatales son conscientes, por este motivo es que crece constantemente la inversión en ciberseguridad. No obstante, la ECIIA (Confederación Europea de Institutos de Auditoría Interna) elabora cada año un informe que explora los principales riesgos internacionales para ayudar a las organizaciones a identificar soluciones a los mismos. Sus informes, año tras año, incluyen la ciberseguridad como uno de sus "*Hot topics*", incluso, en primera posición.

Así pues, el objetivo del trabajo es contribuir al debate entorno si el sistema internacional cibernético, es decir, el conjunto de actores internacionales y sus relaciones en materia de ciberseguridad, ha alterado la configuración del poder imperante hasta el nacimiento de internet. Mientras que unos argumentan que el poder se ha difundido entre los diferentes actores del sistema, sustrayéndoselo a las grandes potencias, otros argumentan que nada de esto ha ocurrido y que la balanza de poder no ha sido modificada.

Las teorías de las Relaciones Internacionales, realismo y liberalismo, pueden ser útiles para resolver esta cuestión. En primer lugar, el realismo tiene mucha aplicabilidad al dilema de la ciberseguridad, pues la anarquía también está presente en el sistema internacional cibernético, y los estados buscan su seguridad en él a través de ciberataques y ciberdefensas. Sin embargo, surge aquí el primer objeto de debate, pues las ciberpotencias son aquellas que más dependencia tienen de la tecnología y por tanto las más vulnerables; aunque también son estas las que más invierten en defensa de su espacio cibernético y las que más capacidad de ataque tienen, por lo que la disuasión es un elemento a tener en cuenta. En segundo lugar, el liberalismo entiende que la anarquía del sistema internacional cibernético se puede mitigar mediante la cooperación internacional en materia de normas e instituciones que garanticen la seguridad. Además, los Estados no representan los únicos actores dentro del sistema, pues los individuos, empresas, organizaciones internacionales, etc., juegan un papel fundamental en él.

Con lo anterior, es necesario comprender quienes son las principales potencias del sistema, a las que es útil ubicar en una escala, por niveles. Primero, Estados Unidos es el país tecnológicamente más potente, al que le sigue de cerca, en segundo lugar, China. Tercero, se encuentra a Rusia, que posee seguramente a los mejores hackers. Por debajo se ubican ya muchos países como Reino Unido, Australia, Países Bajos, Corea del Sur, Vietnam o Francia. Por último, Irán, Corea del Norte e Israel terminan la lista.

Estas potencias proyectan su poder en el sistema internacional cibernético a través de diferentes dinámicas, que juegan un papel esencial. La primera de estas dinámicas es el problema de atribución, pues al realizarse la mayoría de los ciberataques desde el anonimato, es difícil identificar los perpetradores de las mismas, por lo que las represalias también se complican. En segundo lugar, el poder es entendido también en el ciberespacio en su expresión blanda, el conocido *softpower*. Esta proyección del poder se basa en la influencia, la formulación de agenda o la persuasión, mecanismos utilizados por numerosos estados para ampliar sus capacidades, a través del ciberespacio. Por último, es necesario entender que todavía el ciberespacio escasea de regulaciones plenamente efectivas, pues son aquellos que pueden formularlas los menos interesados en ello porque representaría atarse las manos a la espalda.

Para llevar todo esto a la práctica, hago uso del famoso caso Stuxnet, el cual fue un virus informático que neutralizó la central nuclear de Natanz, en Irán. Los artífices (no oficialmente) de tal suceso, Estados Unidos e Israel, en medio de un conflicto geopolítico contra Irán por su emergencia como potencia nuclear en Oriente Medio, deciden, según la teoría neorrealista, frustrar sus ambiciones nucleares para responder al interés de seguridad de Israel, el único faro de influencia de EEUU en la región.

En conclusión, el ciberespacio cada vez será más relevante para los actores internacionales, pues es el dominio en el cual ejercer el poder es más rentable. Sin embargo, las dinámicas del ejercicio del poder, así como la balanza y el equilibrio, seguirán inalteradas. Esto se debe a que las grandes potencias van a seguir acumulando más poder, haciendo uso de sus capacidades tecnológicas para blindarse y atacar a quien perturbe su cometido, disuadiendo a los pequeños actores, que tampoco están protegidos por regulaciones efectivas, de participar en esta pugna.