

EL CIBERESPACIO, EL PODER DEL SIGLO XXI

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

Alumno: **Álvaro Franco** Tutor: **Pablo Aguiar**

INTRODUCCIÓN

El **ciberspacio** ha traído consigo un nuevo dominio en el que ejercer el poder y la guerra, en el panorama internacional. Por ello, es relevante indagar en las consecuencias que el ciberespacio representa para la lucha por el **poder** en el panorama internacional y si éste va a ser capaz de desplazar a los viejos campos de batalla.

OBJETIVOS Y METODOLOGÍA

¿Han **cambiado** las relaciones internacionales? ¿Han adquirido más poder los actores más pequeños en detrimento de las **potencias**? ¿Son las **regulaciones** internacionales suficientes?

Para elaborar el análisis, se ha llevado a cabo investigación teórica, además de su aplicación en un caso real.

MARCO TEÓRICO

Teorías de las Relaciones Internacionales

Realismo

1. El sistema internacional cibernético es **anárquico**.
2. El dilema de seguridad se replica, necesidad de **supervivencia**.
3. Carrera de ciberarmas.
4. Existe la **disuasión**.
5. ¿Existe **dependencia** de la tecnología de las grandes potencias? También ellas son las más capaces.

Liberalismo

1. Las **normas** mitigan la anarquía.
2. Existen **actores** relevantes, no solo Estados.
3. Cooperación **público-privada**.
4. El poder se **difunde**.
5. Papel esencial del *soft-power*.

Principales ciberpotencias

Hiperpotencia

Estados Unidos

Superpotencia

China

Gran potencia

Rusia

Potencias

Reino Unido, Australia, Países Bajos, Corea del Sur, Vietnam, Francia

Potencias emergentes

Irán, Corea del Norte e Israel



El poder en el sistema internacional cibernético

La atribución

Encontrar el **culpable** de los hechos es más fácil para los países más poderosos, hecho que aumenta su capacidad de respuesta y, por tanto, de **disuasión**.

Soft-power

Es poco probable que las reglas cambien, el poder sigue perteneciendo a los grandes. Sin embargo, se espera que el poder, cada vez más, se ejerza desde la influencia, la agenda, el activismo, la diplomacia o el *shaming*, es decir, el *soft power*.

La regulación del ciberespacio

- **Escasa** regulación efectiva para reclamar responsabilidad internacional.
- La regulación aplicable **no es específica** del ciberespacio, pero se tiene en consideración informes de **Grupos de Expertos**.
- ¿Se atarían las manos las potencias aprobando regulaciones en su **propio perjuicio**?

CASO STUXNET, 2009



EEUU e Israel sabotean una planta de enriquecimiento de uranio en Natanz, Irán, retrasando sus planes de proyección como **potencia nuclear** en la región.

Stuxnet, el primer ataque físico-virtual, inutiliza alrededor de 1000 equipos de la planta.

El cambio de *statu quo* era una **amenaza** para Israel, por lo que, mediante el ataque, los gobiernos de EEUU e Israel lograron **ralentizar** el programa nuclear iraní, alterando el **balance de poder** en medio oriente y el sistema internacional.



DESAFÍOS Y TENDENCIAS

- El ciberespacio será cada vez más **importante**.
- Es necesario **regularlo** eficazmente a través del multilateralismo.
- Garantizar la **libertad** de acceso a internet y la protección de datos.
- Conviene invertir en ciberestructura y **defensa**.

CONCLUSIONES

1. El ciberespacio es actualmente el **principal** campo de batalla.
2. Éste **no** ha alterado las relaciones de poder en el sistema, perpetúa a los más grandes.
3. Las regulaciones son **escasas** e **ineficientes** y hasta que no se avance en ellas, los perjudicados son los que menos poder poseen.
4. Es necesario sistematizar el problema de la **atribución**.

UAB

Universitat Autònoma de Barcelona