

Soberanía en el ciberespacio y la problemática de la aplicación del Derecho Internacional

NISS, OSCAR RAMÓN
Maestría en Derecho Internacional
oscarniss@gmail.com

? Tema - Pregunta

La ONU reconoce que el Derecho Internacional Público (DIP) rige en el ciberespacio, pero persiste una brecha entre ese consenso y su aplicación práctica.

¿En qué medida y bajo qué condiciones el DIP se aplica al ciberespacio, y qué mecanismos técnicos y normativos pueden reducir esa brecha?

Casos analizados

-  **Estonia 2007:** denegación de servicio
-  **Stuxnet 2010:** daño físico en Irán
-  **EE. UU. 2016:** injerencia electoral
-  **NotPetya 2017:** malware contra Ucrania
-  **AWS y Azure 2025:** caídas de la nube

🎯 Objetivo/s

General: precisar los supuestos normativos y los criterios operativos del DIP para dirimir controversias sobre la delimitación funcional y el ejercicio de competencias soberanas en el ciberespacio.

 **Conceptualizar** el ciberespacio y sus componentes técnicos.

 **Revisar** resoluciones ONU, CIJ y posiciones estatales.

 **Contrastar** casos para precisar umbrales de ilícitos.

 **Evaluar** configuraciones técnico-jurídicas nacionales.

💬 Discusión

El DIP es aplicable, pero su eficacia depende de criterios operativos sobre atribución, umbrales de efectos, debida diligencia y responsabilidad.

La dificultad no es la falta de normas sino la atribución: los autores pueden ocultar su identidad (falsa bandera).

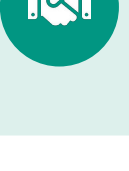
La respuesta predominante fue política (sanciones, atribuciones públicas) y no judicial.

Modelos domésticos (11 países)

-  **Soberanía cerrada:** China, Rusia, Corea del Norte.
-  **Intermedios:** Argentina, Brasil, España, Estonia.
-  **Mercado abierto:** EE. UU., Reino Unido.

📊 Principales resultados

Cuatro conclusiones

-  **DIP aplicable** con criterios operativos claros.
-  **Capacidades** técnicas e institucionales nacionales.
-  **No replicar** regímenes de dominios clásicos.
-  **Práctica y opinio juris** para consolidar costumbre.

Propuesta: Puertas de Enlace Soberanas

-  **IXP nacionales** como puntos de soberanía operativa.
-  **Enrutamiento** y residencia de datos.
-  **Perímetros declarados** para servicios esenciales.
-  **Salvaguardas** de derechos humanos.



Territorialización funcional

Delimitar dónde residen las funciones esenciales, sin perder interoperabilidad.



Control de derechos

Auditorías externas, transparencia de bloqueos y revisión judicial.

Método

Teórico-normativo y socio-jurídico: fuentes ONU (GGE, OEWG), estudio de casos y método comparado.

Marco teórico

Principios de la Carta de la ONU (art. 2), Manual de Tallin 2.0 y jurisprudencia de la CIJ por analogía.

Referencias bibliográficas

NATO CCDCOE (2017). Tallinn Manual 2.0. CICR (2019). DIH y ciberoperaciones durante conflictos armados.