Amenazas Híbridas y Derecho Internacional

Reconocimientos

Cátedra Gobernanza y Regulación en la Era Digital. Proyecto 101127331 *GovReDig.*
Financiado por la UE. Las opiniones no reflejan necesariamente los de la Unión Europea o los de la Agencia Ejecutiva Europea de Educación y Cultura (EACEA). Ni la Unión Europea, ni la EACEA pueden ser considerados responsables de ellos

Fernando Val Garijo

UNED

GovReDig

Financiado por la Unión Europea

Introducción

- **Las amenazas híbridas** son una mezcla de tácticas convencionales y no convencionales usadas por Estados y Actores No Estatales:
- **Algunos de los elementos de las amenazas híbridas son, entre otros:**

1. Ciberataques
2. Coerción económica
3. Campañas de Desinformación
4. Intervención en asuntos internos (procesos electorales)
5. Uso de la fuerza…

- **Presentan retos al Derecho internacional**

Sectores de Derecho Internacional afectados por las Amenazas Híbridas

- **Responsabilidad internacional**. Atribución, Respuestas, Reparación
- **Derecho internacional y uso de la fuerza**. Legítima Defensa y Seguridad Colectiva
- **Derecho Internacional Humanitario**. Si la amenaza híbrida desemboca en conflicto armado
- **Soberanía y No intervención en Asuntos Internos**
- **Derecho Internacional de los DDHH (*)**. Protección de individuos

Responsabilidad Internacional

- **Todo Hecho Internacionalmente Ilícito de un Estado conlleva responsabilidad internacional**

- **Hecho Internacionalmente Ilícito (HII). 2 elementos.**

  - **Atribución:** la conducta (acto u omisión) es atribuible al Estado conforme al Derecho internacional

  - **Violación:** la conducta constituye una violación de una obligación jurídico internacional del Estado

- **Daño o pérdida resultante**, elemento no esencial

Responsabilidad Internacional
El Problema de la Atribución

- **Problemas de atribución:** 1) anonimato de los autores; 2) múltiples autores y orígenes; 3) velocidad de los ciberataques; 4) atribución a máquina, ser humano, o Estado

- A veces se puede determinar el **origen**, pero no lo suficiente para atribuir una conducta a un Estado. **¿Actores No Estatales?**

- **Principio de Diligencia Debida**: Los Estados no deben permitir que su territorio o ciber infraestructuras bajo su control sean usadas para vulnerar derechos de otros Estados.

- Reglas emergentes: **Control efectivo v. Control global o general**

Responsabilidad Internacional Respuestas al HII

- **Contramedidas.** Basadas en la auto-tutela
- **Retorsiones.** Actos inamistosos pero lícitos adoptados por el Estado víctima contra el Estado responsable. Ruptura de relaciones diplomáticas, retirada de programas voluntarios de ayuda, embargos comerciales...
- **Represalias** que no impliquen el uso de la fuerza, en respuesta a un HII anterior. El Estado víctima vulnera alguna obligación internacional, pero no emerge la responsabilidad internacional. Reversibles en lo posible. Cuestión clave: **Proporcionalidad:** daño sufrido, gravedad del HII, derechos afectados. Evaluación por aproximación. **Límites:** prohibición del uso de la fuerza, derechos humanos fundamentales, obligaciones humanitarias... Ciber-represalias son posibles.

Responsabilidad Internacional Contramedidas Urgentes

- En algunas circunstancias, el Estado puede adoptar **contramedidas (represalias) sin notificación previa al Estado responsable.**

- **Ejemplo 1: Ataque DDoS** del Estado A contra el Estado B. El Estado B puede intentar intervenir los servidores usados en el ataque DDoS. La notificación previa es contraproducente. Si los servidores están localizados en los Estados A, C & D, las contramedidas solo pueden dirigirse contra los servidores en A, salvo que C y D consientan.
- **Ejemplo 2:** El Estado A infecta al Estado B con un **malware** que afecta la infraestructura industrial. Para eliminar el malware, el Estado B puede intentar infectar equipos IT en el Estado A para obtener información sobre origen y tipos de malware.