
SIMPÓSIO INTERNACIONAL DE ANÁLISE CRÍTICA DO DIREITO
XI SIACRID
03.11 a 05.11
2021
UENP
JACAREZINHO/PR
BRASIL
PANEL UENP Y UNIVERSIDAD DE MURCIA:
CIBERESPACIO: UN NUEVO RETO PARA EL DERECHO INTERNACIONAL
COORDINADOR
Dr. Fernando de Brito Alves (UENP)
04/11/2021 – 10H00
PONENTES
MARÍA JOSÉ CERVELL HORTAL
CATEDRÁTICA DE DERECHO INTERNACIONAL PÚBLICO Y RELACIONES INTERNACIONALES DE LA UNIVERSIDAD DE MURCIA: "CIBERATAQUE Y REACCIÓN: ¿CÓMO, CUÁNDO, DÓNDE?"
JORGE PIERNAS LÓPEZ
. PROFESOR TITULAR DE DERECHO INTERNACIONAL PÚBLICO Y RELACIONES INTERNACIONALES DE LA UNIVERSIDAD DE MURCIA: "EL DERECHO DE LA UNIÓN EUROPEA ANTE LAS CIBERAMENAZAS"
DOROTHY ESTRADA TANCK
PROFESORA CONTRATADA DOCTORA DE DERECHO INTERNACIONAL PÚBLICO Y RELACIONES INTERNACIONALES DE LA UNIVERSIDAD DE MURCIA: "INTELIGENCIA ARTIFICIAL Y DISCRIMINACIÓN A LA LUZ DEL DERECHO INTERNACIONAL PÚBLICO"
IRENE VÁZQUEZ SERRANO
PROFESORA AYUDANTE DOCTORA DE DERECHO INTERNACIONAL PÚBLICO Y RELACIONES INTERNACIONALES DE LA UNIVERSIDAD DE MURCIA: "EL DERECHO INTERNACIONAL DE LA RESPONSABILIDAD Y LAS ACTIVIDADES EN EL CIBERESPACIO"
CIÊNCIA JURÍDICA UENP
CAPES
GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN
Proyecto PID2020-112577RB-I00 financiado por MCIN/ AEI /10.13039/501100011033
Transmissão no canal PPGD UENP do Youtube
WWW.SIACRID.COM.BR

CIBERATAQUES Y REACCIÓN:

¿CÓMO, CUÁNDO, DÓNDE?

María José Cervell Hortal

4 de noviembre de 2021

1. El ciberespacio: ¿limbo jurídico?
2. ¿Cuándo puede hablarse de ciberataque?
3. Otros problemas para definir el concepto
4. Reflexiones finales

¿Se aplica el Derecho Internacional al ciberespacio?

SÍ

Pero ¿CÓMO y A QUÉ?

- ¿Es todo un “ciberataque”?
- La delgada línea entre uso de la fuerza y ataque armado
- Ataque armado en el ciberespacio: el criterio de la “**escala y los efectos**”

DOS CASOS HIPOTÉTICOS

UNIVERSIDAD DE MURCIA

SUPUESTO 1

- Daños serios o muerte de personas
- Daños significativos o destrucción de la propiedad

SUPUESTO 2

- No daños serios o muerte de personas
- No daños significativos o destrucción de la propiedad
- Pero….

LOS PROBLEMAS TRADICIONALES, TAMBIÉN EN EL CIBERESPACIO

UNIVERSIDAD DE MURCIA

1. ¿Quién lanzó el ataque?
   - Atribución
   - Actores no estatales
2. ¿Cuándo? (la inminencia)
3. ¿Cómo responder? (proporcionalidad)

- Ningún ataque ha declarado aún ser víctima de una "ciberagresión"
- Pero cuidado, en su caso, con las posibles repuestas
- Mejor prevenir que curar: la cooperación, indispensable
- Posibles soluciones de futuro

Gracias

María José Cervell Hortal
Catedrática de Derecho Internacional Público y Relaciones Internacionales
Universidad de Murcia

cervell@um.es

El Derecho de la Unión Europea ante las ciberamenazas

Juan Jorge Piernas López

4 noviembre 2021

Las ciberamenazas…un riesgo creciente

UNIVERSIDAD DE MURCIA

- **Ciberataques**: una de las principales amenazas globales (WEF 2020, 5ª; Juncker 2017)….22 300 millones de dispositivos conectados a IoTs para 2024.

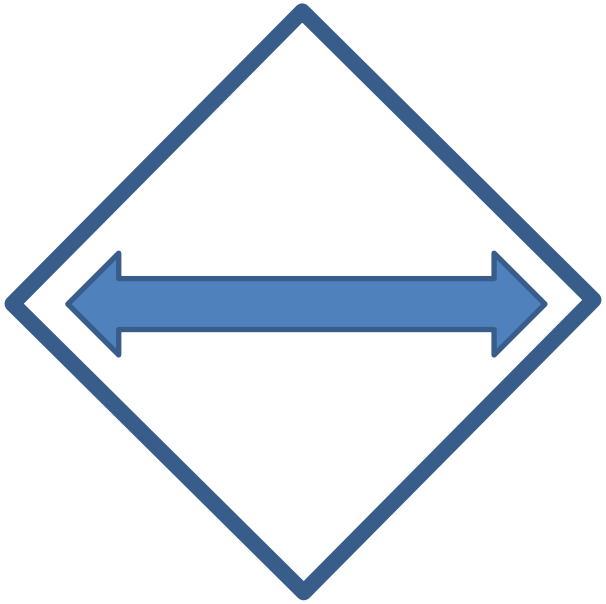
- Los ciberataques han aumentado significativamente durante **la pandemia de COVID-19:** contra **infraestructuras críticas**, centros sanitarios…

- **Participación de actores estatales**, como Rusia, China y Corea del Norte, en actividades informáticas malintencionadas

- **La Unión es un importador neto de productos y servicios de ciberseguridad**, lo que incrementa el riesgo de dependencia tecnológica y vulnerabilidad

Ciberdiplomacia (sanciones *ad extra*)

Lucha contra ciberdelincuencia (*ad intra*)



Cooperación con actores internacionales (ONU, OSCE…)

Ciberdefensa

¿Por qué una ciberdefensa de la UE?

UNIVERSIDAD DE MURCIA

- Discurso de la **Presidenta Comisión sobre** el Estado de la Unión (15.9.2021):

  "no podemos hablar de defensa sin mencionar las cuestiones cibernéticas[…]

  hace falta una política europea de ciberdefensa, con su correspondiente **normativa común** con arreglo a una nueva **Ley Europea de Ciberresiliencia"**

- La **naturaleza transfronteriza** del ciberespacio y de las ciberamenazas hacen evidente la **necesidad de cooperación en la UE….pero**:
  - **Seguridad nacional** (exclusiva de los EEMM Art. 4.2), cuestiones de defensa se rigen por la **unanimidad en el Consejo**…
  - además los EEMM colaboran en el marco de la **OTAN**…especializada en **ciberdefensa…solapamiento o Cooperación? Posible conflicto?**

Medidas concretas de ciberdefensa

UNIVERSIDAD DE MURCIA

- **Inclusión de la ciberdefensa** en el marco de una **"cooperación estructurada permanente"** (CEP) (Art. 42.6 TUE), adoptada en diciembre 2017.

- Inclusión de financiación del **Fondo Europeo de Defensa para ciberdefensa**

- Actualización marco político **ciberdefensa 2018 (ciberespacio como "espacio" o ámbito de operaciones).**

- La ciberdefensa y las cláusulas de solidaridad y defensa mutua de la UE **(artículos 222 TFUE y 42.7 TUE)**

Ciberdefensa y cláusula de solidaridad

UNIVERSIDAD DE MURCIA

Artículo 222 TFUE:

1. La Unión y sus Estados miembros actuarán conjuntamente con espíritu de solidaridad si un Estado miembro es objeto de un **ataque terrorista o víctima de una catástrofe natural o de origen humano**. La Unión movilizará todos los instrumentos de que disponga, incluidos los medios militares puestos a su disposición por los Estados miembros para [...]:

- **¿Se puede invocar la cláusula de solidaridad en caso de ciberataque?**
  - Sí ante un "**ciberataque de especial gravedad**" (ej. Estrategia de ciberseguridad de 2013 y 2017…**estrategia 2020** más cauta **"reflexionar"**)
  - Se podría aplicar ante **actos terroristas (Directiva 40/2013)** y otros que generen una **"catástrofe cibernética"** (ej. Denegación duradera de servicio)
  - **No requiere imputación**, se centra en la respuesta (facilita aplicación)
  - La **respuesta se limita geograficamente al terrritorio del E.M. afectado** y no se prevé (tampoco se prohíbe) la respuesta militar ni el uso de la fuerza.

Ciberdefensa y cláusula de defensa mutua

UNIVERSIDAD DE MURCIA

Artículo 42.7 TUE:

Si un Estado miembro es objeto de **una agresión armada en su territorio**, los demás Estados miembros le deberán ayuda y asistencia con todos los medios a su alcance, de conformidad con el **artículo 51 de la Carta de las Naciones Unidas**. Ello se entiende sin perjuicio del carácter específico de la política de seguridad y defensa de determinados Estados miembros. [...]

- **¿Se puede invocar la cláusula de defensa mutua en caso de ciberataque?**
  - Sí, en caso de **ciberataque** que, por sus efectos, es **equiparable a una "agresión armada"** (ej. pérdida de vidas humanas o grave perturbación en sistemas esenciales para la vida de los ciudadanos de un Estado)
  - También en caso de **ciberataque inminente** (difícil de evaluar en la práctica)
  - Y contra **actores no estatales** (ya se ha hecho…pero Francia reniega)
  - La **respuesta no se limita geograficamente al terrritorio del E.M**. afectado y puede ser militar (es una **respuesta más estatal y menos "UE"**).

¿Y si no se llega al umbral de la legítima defensa *ex* artículo 51 de la Carta?

UNIVERSIDAD DE MURCIA

Resolución aprobada por el Parlamento Europeo el 7.10.2021:

La UE se ve afectada por conflictos híbridos c**on frecuencia no se trata de ataques tan graves en sí mismos como para activar el artículo 5 del Tratado de la OTAN o el artículo 42, apartado 7, del TUE**, pero tienen un **efecto estratégico acumulativo** y no pueden combatirse de forma efectiva con **medidas de retorsión por parte de los Estados miembros perjudicados**;

la Unión debe esforzarse por encontrar una solución que **colme este vacío legal reinterpretando el artículo 42, apartado 7, del TUE y el artículo 222 del TFUE**, de modo que **se reservase el derecho a la defensa colectiva por debajo del umbral de la defensa colectiva y se autorizasen contramedidas colectivas** de los Estados miembros de la Unión con carácter voluntario,

y **trabajar con sus aliados internacionales a fin de adoptar una solución similar a escala internacional**; resalta que este es el único modo eficaz de combatir la parálisis a la hora de reaccionar contra amenazas híbridas, así como un instrumento para incrementar el coste para nuestros adversarios

- **¿Se tratará de una manifestación de autonomía estratégica? …y el artículo 3.5 TUE (estricto respeto y al desarrollo del Derecho internacional)?**

Conclusiones

UNIVERSIDAD DE MURCIA

- Es necesario **acabar** con la **fragmentación del presupuesto y de la información** (creación Unidad Cibernética Conjunta 19.10.2021…voluntaria…insuficiente)

- La Unión debe mirar a sus **políticas más exitosas** (Mercado interior, competencia, comercio…) para buscar el **camino a seguir**.

- La **reforma de los Tratados** en el marco de la **conferencia sobre el futuro de Europa** (conclusiones primavera 2022) podría ser parte de la solución

- ¿Y la **relación verdaderamente complementaria con la OTAN** (ej. retos de las tecnologías cibernéticas e híbridas)? **próxima "brújula estratégica**" (2022)

Muchas gracias

XI Simposio internacional de Análisis crítico del derecho
4 de noviembre de 2021
PANEL UENP-Universidad de Murcia

'Inteligencia artificial y discriminación a la luz del Derecho Internacional Público'

Dorothy Estrada Tanck
Profesora de Derecho Internacional Público y RRII, Universidad de Murcia
Vice-Presidenta del Grupo de Trabajo de NU sobre Discriminación contra las Mujeres y las Niñas

Inteligencia artificial

UNIVERSIDAD DE MURCIA

- La inteligencia artificial sustenta muchos aspectos de la vida moderna:
  - Motores de búsqueda
  - Banca
  - Tecnología biométrica (incluyendo en programas sociales)
  - Reconocimiento de imágenes
  - Traducción automática

- Pero desde el punto de vista ético y jurídico:

Inteligencia artificial: ¿realmente libres de errores y/o de pasiones?

y

¿liberada de cometer actos de discriminación directa o indirecta?

Inteligencia artificial

UNIVERSIDAD DE MURCIA

Inteligencia artificial: postura de sociedad civil, academia y practicantes

UNIVERSIDAD DE MURCIA

- ONGs (e.g. AI in action): Cómo se puede mantener el control humano sobre la IA, a fin de respetar adecuadamente tanto las obligaciones jurídicas como principios éticos

- Stuart Russell, fundador del Centro de Inteligencia Artificial Compatible con el Ser Humano de la Universidad de California en Berkeley: la mayoría de los expertos creen que este siglo se desarrollarían máquinas más inteligentes que los humanos, y pidió tratados internacionales para regular el desarrollo de la tecnología

Inteligencia artificial y efectos

UNIVERSIDAD DE MURCIA

- ***ONU: Prejuicios, racismo y mentiras: enfrentarse a consecuencias no deseadas de IA:***

1) Las consecuencias del mal uso pueden ser devastadoras (Caso hombre negro arrestado Michigan/estudiantes en Reino Unido)

2) El odio, la división y la mentira son buenos para el negocio (redes sociales, polarización, división social)

3) La desigualdad mundial se refleja en Internet (dominio EEUU/China)

4) Los beneficios potenciales son enormes

5) Necesitamos llegar a un acuerdo sobre la regulación internacional de la IA

IA y discriminación en el Derecho Internacional de los Derechos Humanos

UNIVERSIDAD DE MURCIA

- El uso de la IA, con sus características particulares (p. ej., la opacidad, la complejidad, la dependencia de datos, el comportamiento autónomo) puede tener repercusiones negativas para múltiples derechos humanos, en particular, los de la **igualdad y no-discriminación**

- **Discriminación:** toda distinción, exclusión o restricción que tenga por objeto o resultado menoscabar o anular el reconocimiento, goce o ejercicio por una persona, sobre la base de la igualdad, de los derechos humanos y las libertades fundamentales en las esferas política, económica, social, cultural y civil o en cualquier otra esfera.

  - **Discriminación directa** se produce cuando la diferencia de trato está 'explícitamente basada en el sexo y el género'.

  - Sin embargo, un trato idéntico puede ser **indirectamente discriminatorio** si tiene el efecto de perjudicar o anular los derechos de una persona. Esto puede ocurrir cuando 'una ley, una política, un programa o una práctica parecen ser neutrales en lo que respecta a los hombres y a las mujeres, pero tienen un efecto discriminatorio en la práctica para algunas personas porque las desigualdades preexistentes no son abordadas por la medida aparentemente neutral

Postura clásica del DIP:

UNIVERSIDAD DE MURCIA

- IA y Derecho Internacional Público:

- Si se usan en tiempo de paz: Principios y Normas del **Derecho Internacional de los Derechos Humanos:** Principios de universalidad, interdependencia e indivisibilidad, ***igualdad y no-discriminación*** / progresividad y no-regresividad en derechos económicos, sociales y culturales (DESC) / DUDH; Tratados Internacionales de DH; Costumbre

- Si se usan en contexto de conflicto armado: Principios y Normas **del Derecho Internacional Humanitario**

IA y ONU

UNIVERSIDAD DE MURCIA

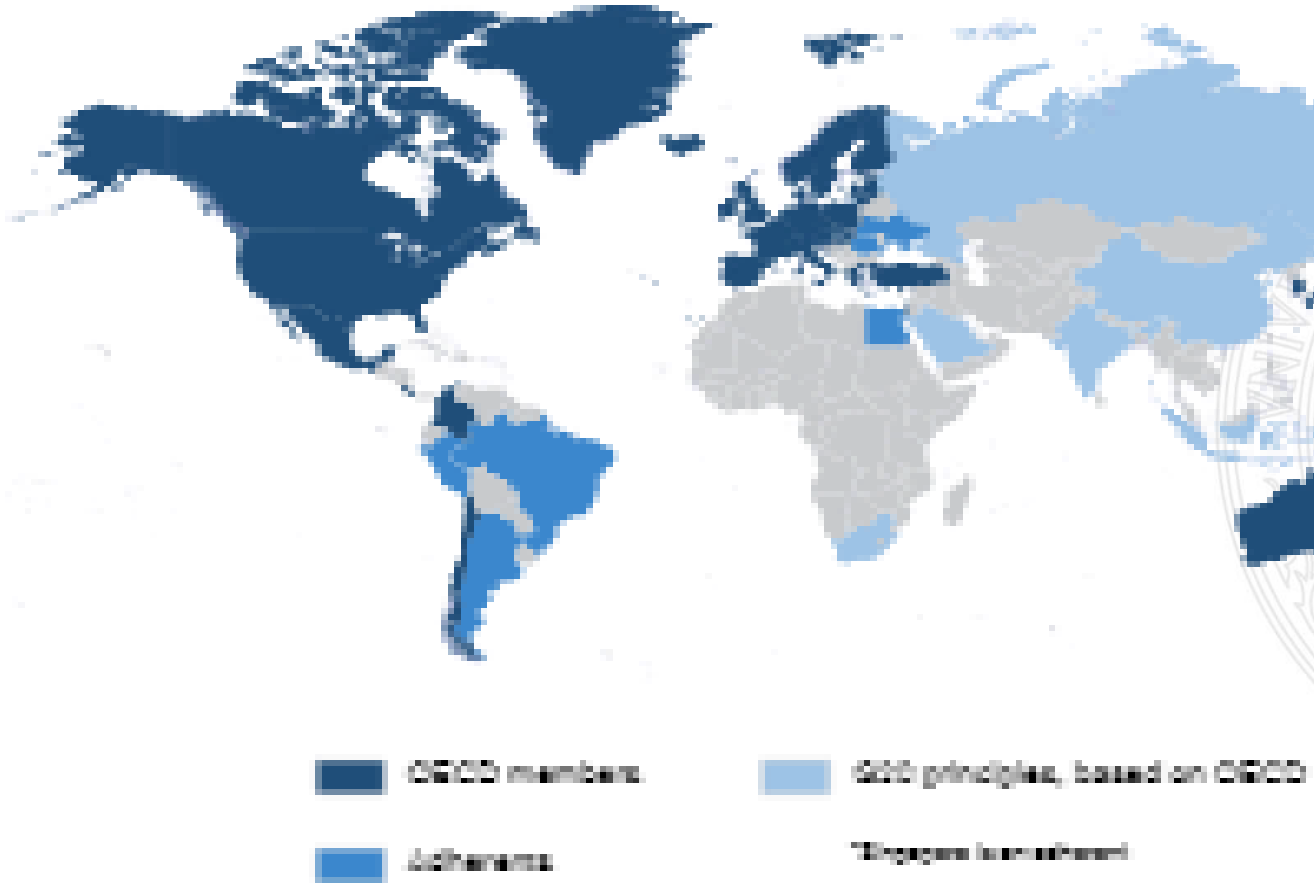
- Consulta de la **UNESCO** sobre la IA comenzó en julio de 2020.

- Los expertos de la **UNESCO** elaboraron un **proyecto de documento jurídico y global** sobre la **ética de la IA**, teniendo en cuenta los amplios impactos de la IA, incluyendo el medio ambiente y las necesidades del Sur Global

Organizaciones internacionales: OCDE

UNIVERSIDAD DE MURCIA

- OCDE: *Principios sobre IA*, adoptados en 2019: inovativos, confiables, basados en los derechos humanos y la democracia



Red Iberoamericana de Protección de Datos lanzó a consulta pública unas Recomendaciones sobre IA para la región.

- RIPD ha elaborado unas "**Recomendaciones generales para el tratamiento de datos en la inteligencia artificial**"

- Estas recomendaciones tienen un enfoque preventivo y parten del supuesto según el cual la mejor forma de proteger los derechos humanos comprometidos en el tratamiento de datos personales es evitando su vulneración.

- La RIPD ha elaborado unas directrices complementarias y más detalladas contenidas en el documento denominado "**Orientaciones específicas para el cumplimiento de los principios y derechos que rigen la protección de los datos personales en los proyectos de Inteligencia Artificial**".

- En el ámbito de la UE:

COMISIÓN
EUROPEA

Bruselas, 21.4.2021
COM(2021) 206 final

2021/0106 (COD)

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

POR EL QUE SE ESTABLECEN NORMAS ARMONIZADAS EN MATERIA DE INTELIGENCIA ARTIFICIAL (LEY DE INTELIGENCIA ARTIFICIAL) Y SE MODIFICAN DETERMINADOS ACTOS LEGISLATIVOS DE LA UNIÓN

PROPUESTA DE REGLAMENTO UE:

UNIVERSIDAD DE MURCIA

- **Art. 3: Sistema de inteligencia artificial (sistema de IA):** *software* que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el Anexo I y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa.

- Enfoques de aprendizaje automático (‘machine learning’);

- Enfoques basados en la lógica y el conocimiento,

- Enfoques estadísticos, estimación bayesiana, métodos de búsqueda y optimización

PROPUESTA DE REGLAMENTO UE:

UNIVERSIDAD DE MURCIA

- Está garantizada su coherencia con la Carta de los Derechos Fundamentales de la Unión Europea y el Derecho derivado de la Unión vigente en materia de protección de datos, protección de los consumidores, **no discriminación e igualdad de género**

- Debe entenderse sin perjuicio del Reglamento General de Protección de Datos y la Directiva sobre protección de datos en el ámbito penal, a los que complementa con un conjunto de normas sobre determinados sistemas de IA de alto riesgo y con restricciones de ciertos usos de sistemas de identificación biométrica remota.

- Complementa el Derecho de la UE vigente en materia de **no discriminación** al establecer requisitos específicos para reducir al mínimo el riesgo de **discriminación algorítmica**, en particular sobre diseño y la calidad de los conjuntos de datos empleados para desarrollar sistemas de IA, los cuales van acompañados de obligaciones referentes a realización de pruebas, gestión de riesgos, la documentación y la vigilancia humana durante todo el ciclo de vida de tales sistemas.

Algunas reflexiones finales…

UNIVERSIDAD DE MURCIA

- *Reto y propuesta*: utilizar los principios y normas del DIDH, especialmente en materia de igualdad y no-discriminación, para abordar la IA

- Interpretación amplia: los mecanismos de IA estarían obligadas a asegurar una visión igualitaria y garantista de los DH en el diseño de algoritmos

- Un paso para lograrlo es conceptual y normativo basado en el Derecho Internacional de los Derechos Humanos

- Y el otro paso es metodológico y procesal: integrar de manera igualitaria (con diversidad de género, racial, religiosa,…) y fomentando una participación civil amplia en la toma de decisiones y el diseño e implementación de mecanismos de IA

- Evitar deshumanización y falta de control humano total y lograr una regulación eficiente y justa

El Derecho Internacional de la responsabilidad y las actividades en el ciberespacio

Dra. Irene Vázquez Serrano

4 de noviembre de 2021

UENP, Jacarezehinhor, Paraná, Brasil

Índice

1. Introducción: una aproximación al concepto de ciberespacio

UNIVERSIDAD DE MURCIA

- ✓ Inteligencia artificial
- ✓ Informática
- ✓ Internet

→ CIBERESPACIO

"un nuevo espacio junto al territorio, el mar, el aire, el espacio ultraterrestre y los espacios polares"

- RAE: "un ámbito virtual creado por los medios informáticos"
- En definitiva, no es un espacio físico sino una red de redes locales conectadas y no accesibles, redes locales no conectadas (casi inexistentes) y redes abiertas.

1. Introducción: una aproximación al concepto de ciberespacio

UNIVERSIDAD DE MURCIA

Un *ámbito global* que **difumina las fronteras entre los diversos Estados** y permite operar en todo él independientemente del sistema o régimen político de cada uno de ellos, con una gama, en fin, extremadamente amplia de actores (desde las personas físicas, pasando por toda una variedad de grupos u organizaciones, hasta los Estados)

2. Las amenazas que genera el ciberespacio

UNIVERSIDAD DE MURCIA

De acuerdo con la ***Estrategia de Seguridad Nacional*** (2017) y la ***Estrategia de Ciberseguridad*** (2919):

- **Cibercrimen** más usual la "extorsión" mediante secuestro de datos, pirateo, fallos de seguridad, accesos no autorizados, robo de archivos… y, especialmente, el **ciberespionaje** (se atacan las vulnerabilidades sistémicas y las instituciones de los Estados con medios militares, ciberataques, manipulaciones informáticas y presiones económicas…)
- **Ciberterrorismo** ciberataques a través de intimidación, coacción y daños con fines políticos o religiosos, convirtiéndose el ciberespacio en un "santuario del terrorismo" debido a la falta de regulación, enmascaramiento de la red y la impunidad
- **Ciberguerra** un conflicto entre Estados tecnológicamente avanzados que usa el ciberespacio como escenario principal y se lleva a cabo con ciberataques, aisladamente o como parte de una guerra u operaciones armadas convencionales (actos estatales y no estatales)

3. Los ciberataques

UNIVERSIDAD DE MURCIA

"Toda operación cibernética, tanto ofensiva como defensiva, de la que puede razonablemente esperarse que cause lesiones o muerte de personas o daño o destrucción de bienes"

Manual de Tallin 2.0, regla 92

"Toda operación cibernética deliberada destinada a vulnerar un sistema crítico para la seguridad nacional, la independencia política o la integridad territorial de un Estado de la que pueda razonablemente esperarse cause lesiones, muertes de personas o daños o estructuras de bienes"

Prof. Gutiérrez Espada, 2021

Tres consideraciones sobre los ciberataques

1. Se llevan a cabo a través de armas cibernéticas, (especialmente, virus informáticos):
   - No son de diseño no estándar
   - No requieren la proximidad física al objetivo para ser efectivas
   - No están identificados (a diferencia de los vehículos y uniformes)
   - No dejan rastros persistentes
   - Son muy fáciles de ocultar (e ideales para la trata)
   - Se pueden programar para que se activen de forma remota en un momento específico o en condiciones específicas (dificulta la detección de la relación de causa y efecto)
   - Son difíciles de distinguir de las tecnologías utilizadas en el ciberespionaje (ambas buscan primero obtener acceso a la guerra)

   Ejemplos:
   - Código dañino, malicioso o malware, la denegación de servicios o denial of service y las intrusiones no autorizadas en sistemas
   - Ataques realizados por un Estado contra buques o infraestructuras de otro Estado

UNIVERSIDAD DE MURCIA

Tres consideraciones sobre los ciberataques

2. **Principales objetivos de los ciberataques: las estructuras críticas** ("instalaciones, redes, sistemas y equipos físicos y de tecnología de la información cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales")

   Consideradas posibles objetivos de grupos terroristas

3. **No todos los ataques cibernéticos pueden ser considerados un acto de guerra.** Debemos estar atentos a
   - la importancia del ataque
   - la interrupción que produce en la vida nacional

Y, si de diera contra una infraestructura crítica, se prevé la invocación de la **legítima defensa** (art. 5 OTAN)

El *Manual de Tallin 2.0* de 2017 regula la aplicación del *ius ad bellum* y el *ius in bello* a las actividades en el ciberespacio

(derecho consuetudinario aplicable a los conflictos en el ciberespacio)

También **el Derecho Internacional** y el **Derecho Internacional de la Responsabilidad** es aplicable al ciberespacio

Un Estado que lleva a cabo una **acción u omisión contraria** a una norma vigente de **Derecho Internacional vigente** (tratado, costumbre, decisión vinculante de un tribunal internacional, acto unilateral de un Estado o resolución obligatoria de una Organización internacional) comete un ***hecho ilícito internacional*** e incurre, por lo tanto, en **responsabilidad internacional.**

Son comportamientos imputables a los Estados

1. Aquellos de sus propios órganos que actúan de forma oficial
2. Aquellos de personas o entidades privadas habilitadas para ejercer funciones públicas (por ej. empresas de seguridad privadas), cuando
   - Las competencias que ejercen sean autorizadas específicamente por el Derecho interno del Estado
   - Sean atribuciones "propias" del poder público
   - Se trate de comportamientos correspondientes con la función pública

3. Aquellos de órganos de otro Estado que que realizan funciones a su disposición

Independientemente de la jerarquía, la división territorial del Estado y la naturaleza de los órganos

¿Qué ocurre con los **comportamientos *ultra vires***, esto es, aquellos que incumplen las órdenes que se han recibido o que se exceden de las competencias otorgadas, de los órganos de un Estado, o de una entidad que ha sido habilitada por él para el ejercicio de las atribuciones propias del poder público o de un órgano de otro Estado que ha puesto a su disposición ?

La CDI

- **Sí,** cuando tal órgano persona o entidad actúan como función pública (actuación oficial)
- **No**, cuando se trata de un comportamiento de un particular, excepto cuando actúa por instrucciones o bajo la dirección y control de ese Estado, que sí le será imputable al Estados

5. El Derecho Internacional de la Responsabidlidad por las actividades en el ciberespacio

UNIVERSIDAD DE MURCIA

En cuanto al control de la actuación de un particular por el Estados,

- *Tesis del control efectivo* (imputables algunos actos)
- *Tesis del control global o general* (imputables todos los actos)

Sin embargo, no hay uniformidad en la doctrina acerca de cuál de estos criterios deba aplicarse ante una actividad cibernética, si bien, mayoritariamente es preferible el ***criterio del control efectivo*** porque de lo contrario el Estado sería responsable por un sinnúmero de actividades

Así lo ha señalado también

- **Resolución 73/27, de 5 de diciembre de 2018, AG de las Naciones Unidas:** "Los Estados no deben recurrir a terceros para cometer actos internacionalmente ilícitos utilizando las TIC"
- **Informe Final de la Comisión Global sobre la Estabilidad en el Ciberespacio (2019):** "Los Estados pueden ser considerados responsables por las ciberoperaciones que ellos llevan a cabo, dirigen o permiten"

5. El Derecho Internacional de la Responsabidlidad por las actividades en el ciberespacio

UNIVERSIDAD DE MURCIA

DIR es aplicable a las actividades en el ciberespacio cuando éstas contradicen normas de Derecho Internacional en vigor.

- **Informe Final de la Comisión Global sobre la Estabilidad en el Ciberespacio** (2019): "los Estados pueden ser considerados responsables por las ciberoperaciones que llevan a cabo".
- **Resolución 73/27** (2018): "un Estado no debe realizar (…) actividades en la esfera de las TIC contrarias a las obligaciones que le incumban en virtud del derecho internacional que dañen intencionalmente infraestructuras fundamentales o dificulten de otro modo la utilización y funcionamiento de infraestructuras fundamentales que presten servicios al público" debiendo fundamentarse "las acusaciones contra los Estados de organizar y llevar a cabo actos ilícitos".
- Y el **Manual de Tallin 2.0**…

5. El Derecho Internacional de la Responsabidlidad por las actividades en el ciberespacio

UNIVERSIDAD DE MURCIA

El **Manual de Tallin 2.0** recoge las normas sobre imputación que la CDI ha establecido en el Proyecto de artículos de responsabilidad de los Estados de 2001. Son imputables al Estado:

1. Las operaciones cibernéticas llevadas a cabo por sus órganos o por personas a las que el Derecho de ese Estado atribuyó el ejercicio de competencias públicas, imputando también al Estado la realización de los hechos en ambos casos (órganos y personas que ejercitaban competencias públicas) cuando se trata de comportamientos *ultra vires* **(regla 15)**

2. Los comportamientos de los órganos de otro Estado que puso a su disposición, incluidos los actos *ultra vires* **(regla 16)**

5. El Derecho Internacional de la Responsabidlidad por las actividades en el ciberespacio

UNIVERSIDAD DE MURCIA

3. En el caso de actores no estatales, las ciberoperaciones de aquellos si siguieron instrucciones estatales o se encuentran bajo la dirección o control del Estado, señalando el criterio del control efectivo **(regla 17)**

> "Como un ejemplo de control efectivo considérese el caso en el que un Estado planea y supervisa una operación de actualizaciones de *software* para implantar nuevas vulnerabilidades en el *software* ampliamente usado por otro Estado en sus ordenadores gubernamentales. El anterior Estado concierta un contrato confidencial para compartir los resultados con la compañía que produce el *software* y entonces dirige el proceso para ponerlo en práctica. En un supuesto así, la conducta de la compañía es imputable al Estado que ejerce el control"

4. Aquellas ciberoperaciones que, si bien en principio no le son imputables, el Estado reconoce y asume como propias **(regla 17)**

5. En cuanto a los actos *ultra vires* llevados a cabo por actores no estatales, éstos no se imputarán con carácter general al Estado, debiendo estar al caso concreto

5. El Derecho Internacional de la Responsabidlidad por las actividades en el ciberespacio

UNIVERSIDAD DE MURCIA

Ahora bien, deberá comprobarse que no se dan ninguna de las 6 **causas de exclusión de la ilicitud (**arts. 20-26 del Proyecto de 2001)

"factores que eliminan la antijuridicidad del hecho de un Estado que (*prima facie* sólo por tanto) no está en conformidad con lo que de él exige una obligación internacional", de forma que "cuando se da uno de los factores recogidos, el hecho del Estado (que aparentemente lo es) no tiene o pierde su carácter ilícito"

El *Manual de Tallin 2.0* recoge (regla 19) las mismas causas de exclusión de ilicitud que el Proyecto de 2001.

6. Conclusiones

UNIVERSIDAD DE MURCIA

1. A pesar de no existir una norma internacional (tratado, documento…) que regule expresamente las actividades en el ciberespacio, lo cierto es **que no existe un vacío jurídico sobre el ciberespacio**.

2. El propio Derecho Internacional vigente y el Derecho de los Estados puede regular y es aplicable a las actividades que se llevan a cabo en el ciberespacio si producen los mismos efectos que las armas convencionales, en concreto, nos referimos a la aplicación de las normas relativas **al uso de la fuerza armada y las normas relativas al uso de la responsabilidad internacional**

3. Ahora bien, **¿no deberían adoptarse normas específicas?** La concertación de un texto internacional con el acuerdo de los Estados al menos sobre los **Principios jurídicos fundamentales del Derecho Internacional en su aplicación al ciberespacio** sería muy útil, que incluyera un Derecho internacional de la responsabilidad respecto a las actividades del ciberespacio

“No dudemos, por tanto, nosotros, ni nos tiemble el pulso en el esfuerzo de contribuir, cada uno desde el lugar que ocupe, a que el Derecho Internacional sepa dar lo mejor de sí mismo en la regulación de estos nuevos desafíos”

Cesáreo GUTIÉRREZ ESPADA

Muito obrigado
pela sua
atenção