VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

*Los marcos legales y normativos a nivel nacional e internacional del ecosistema **CIBER***

Claudio Peguero

Embajador
Asesor en Asuntos Ciberneticos
Ministerio de Relaciones Exteriores
República Dominicana

Ciberdelitos

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

Sistemas informáticos utilizados como **medio**

Pornografía infantil, amenazas, robo o suplantación de identidad, acoso sexual, difamación, estafas, phishing, *noticias falsas*

Sistemas informáticos como **fin** u objetivo del delito

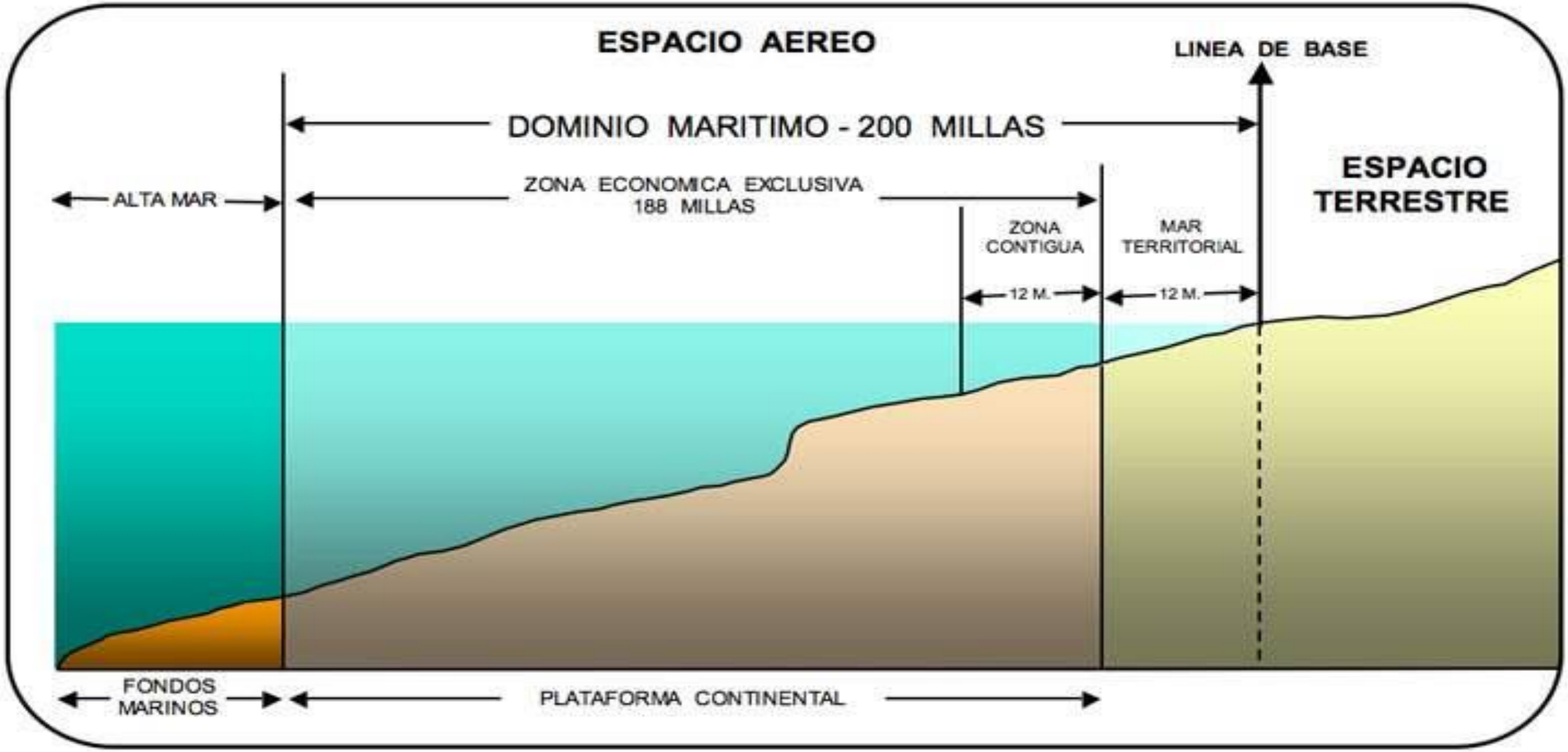
Virus, gusanos, malware, espionaje industrial, pirateria de software, hacking, sabotaje, acceso ilicito

Evidencia Digital / Electrónica

"Evidencia: es cualquier elemento, tanto físico como lógico, de valor probativo sobre algún aspecto relevante en un caso"

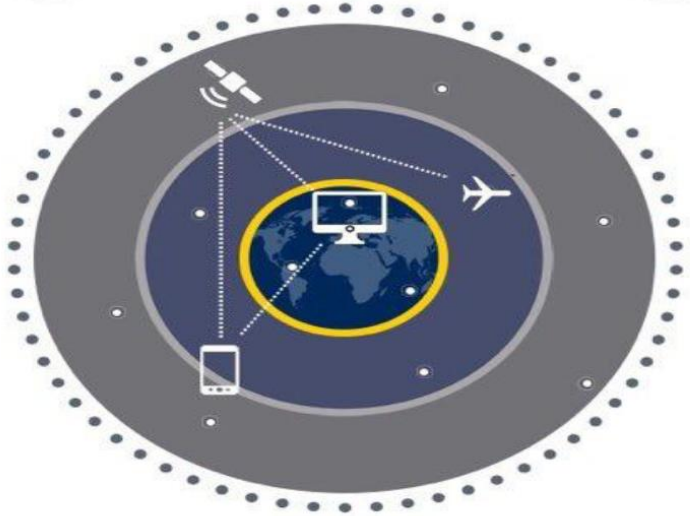
(K. Mandia, 2003)

Jurisdicción tradicional



Jurisdicción en el Ciberespacio

CIBERESPACIO



ESPACIO MARÍTIMO

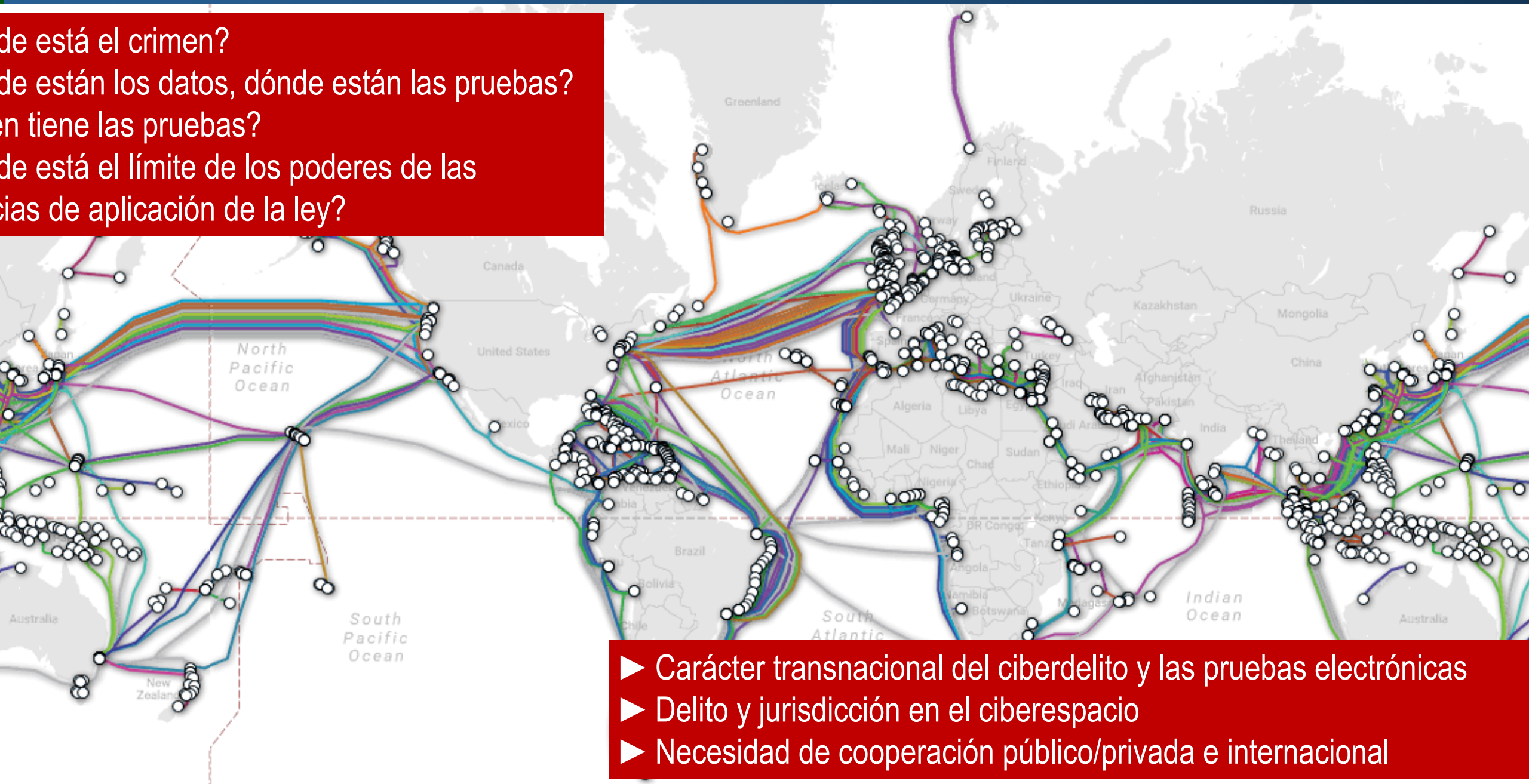
ESPACIO AÉREO Y ULTRATERRESTRE

PRINCIPALES CARACTERÍSTICAS

- Apertura geográfica y funcional
- Ausencia de soberanía y jurisdicción por parte de los Estados
- Facilidad de acceso
- Dificultad de atribución de las acciones que en ellos tienen lugar

Cibercrimen y pruebas electrónicas: el problema de la territorialidad y la jurisdicción

de está el crimen?
de están los datos, dónde están las pruebas?
en tiene las pruebas?
de está el límite de los poderes de las
cias de aplicación de la ley?



- ► Carácter transnacional del ciberdelito y las pruebas electrónicas
- ► Delito y jurisdicción en el ciberespacio
- ► Necesidad de cooperación público/privada e internacional

CONVENIO DEL CONSEJO DE EUROPA SOBRE CIBERDELINCUENCIA (CONVENIO DE BUDAPEST)

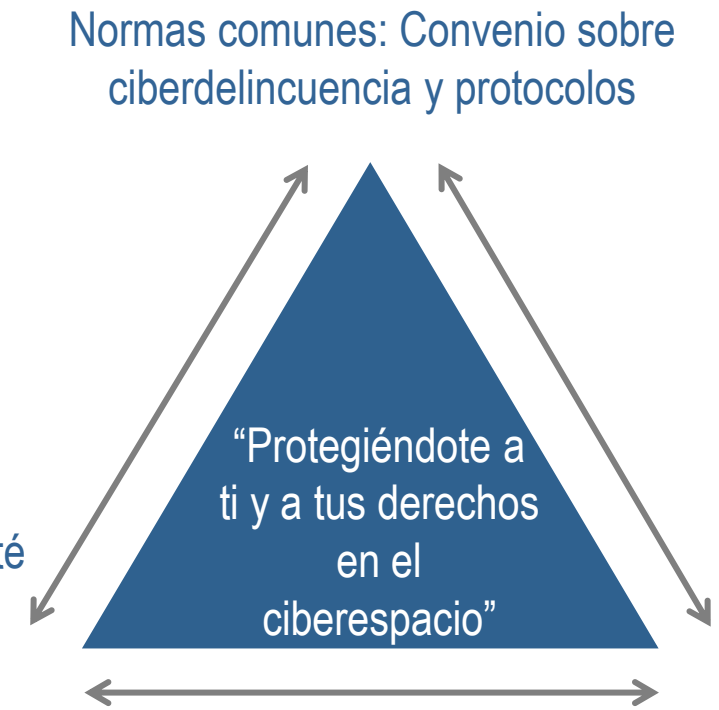
Convenio sobre la Ciberdelincuencia

Las Partes del Convenio (2001), en su legislación penal, deben adoptar:

- Delitos específicos contra y por medio de sistemas informáticos
- Poderes procesales con salvaguardias para investigar la ciberdelincuencia y obtener pruebas electrónicas en relación con cualquier delito
- Cooperación internacional en materia de ciberdelincuencia y pruebas electrónicas

1. Protocolo adicional sobre la ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos (2003)
2. Protocolo relativo al refuerzo de la cooperación y de la divulgación de pruebas electrónicas (2022)

El mecanismo del Convenio



CONVENIO SOBRE CIBERCRIMINALIDAD (ETS 185)

Elaborado por el Consejo de Europa con la participación de Canadá, Japón, África del Sur y los Estados Unidos

Abierto para la firma en Budapest en Noviembre 2001

En vigencia desde Julio 2004

Protocolo adicional relativo a actos de naturaleza racista y xenófoba cometidos a través de sistemas informáticos (ETS 189)

Abierto para la firma en Enero 2003

En vigencia desde Marzo 2006

ESTRUCTURA DEL CONVENIO

Capítulo I – Terminología

Capítulo II - Medidas que deben ser adoptadas a nivel nacional

- Sección 1 – Derecho penal material (delitos que deben penalizarse)
- Sección 2 – Derecho procesal
- Sección 3 – Jurisdicción

Capítulo III - Cooperación internacional

- Sección 1 – Principios generales
- Sección 2 – Disposiciones específicas

Capítulo IV – Cláusulas finales

SUPERVISIÓN DEL TRATADO

EL COMITÉ PARA EL CONVENIO SOBRE CIBERCRIMINALIDAD (T-CY) CONSULTA DE LAS PARTES (SOBRE EL ART. 46)

- Eficacia del Convenio
- Papel de los funcionarios de servicios policiales
- Cooperación del sector encargado del cumplimiento de la ley y el sector privado
- Operación de la red 24/7
- Ampliación o enmienda del Convenio

APLICACIÓN – SITUACIÓN ACTUAL

CONVENIO SOBRE LA CIBERCRIMINALIDAD (ETS 185)

- Entró en vigor en julio de 2004.
- 68 ratificaciones
- Firmado asimismo por Canadá, Estados Unidos (ratificacion), Japón y Sudáfrica
- Enmiendas legislativas y procesos de ratificacion en marcha en muchos otros paises.
- Republica Dominicana ratificó en 2013.
- El convenio sirve como un marco global.

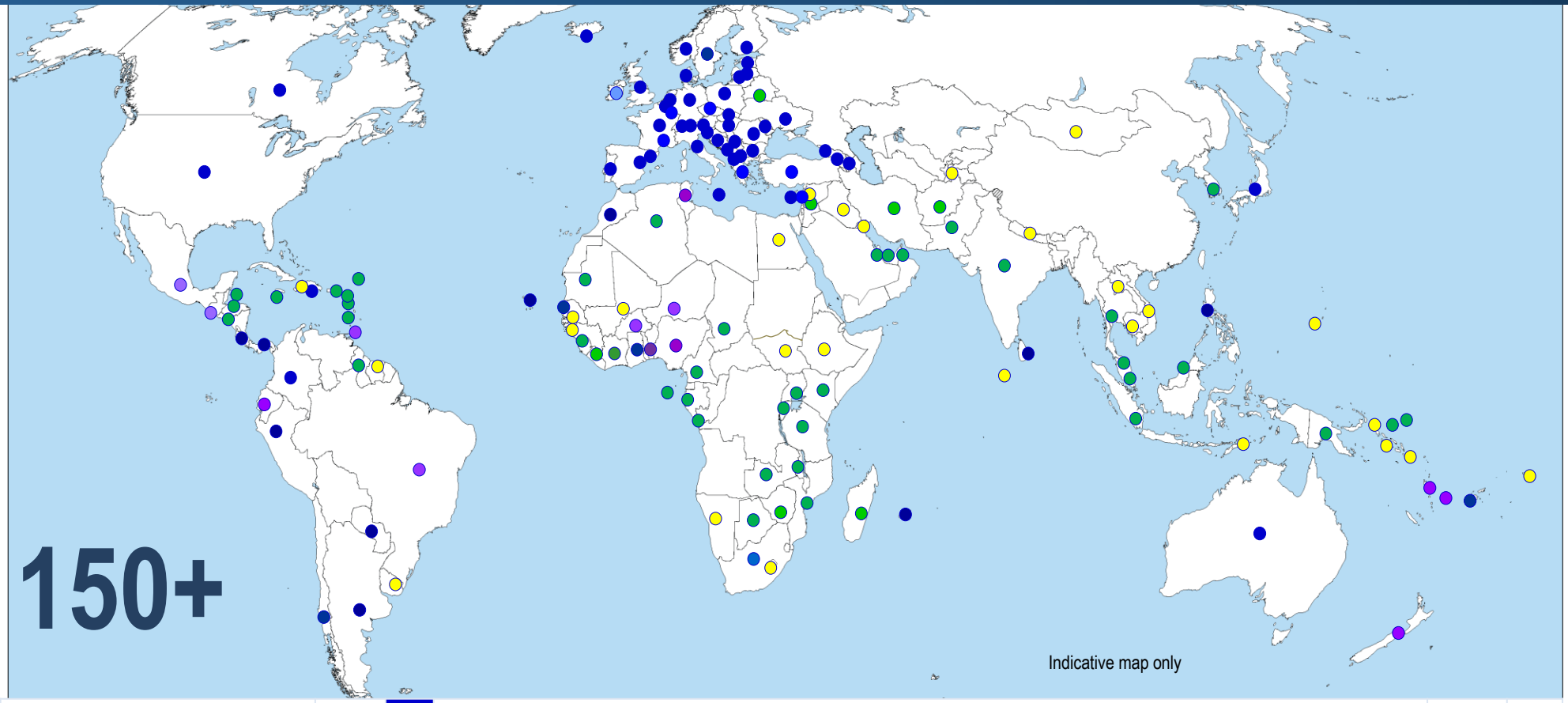
EL CONVENIO COMO MARCO PARA LA COOPERACIÓN INTERNACIONAL

- El Convenio (Capitulo III) es crecientemente utilizado como base legal para la cooperacion international
- Contribuye a la creacion de puntos de contacto adicionales 24/7
- Accesion al Convenio necesaria para hacer uso de las herramientas para cooperacion internacional

ADHESIÓN AL CONVENIO – BENEFICIOS PARA REPÚBLICA DOMINICANA

- Enfoque nacional coherente de la legislación sobre ciber-criminalidad
- Instrumentos para la recopilación de pruebas electrónicas
- Instrumentos para la investigación del blanqueo de dinero por Internet, el ciberterrorismo y otros delitos graves
- Armonización y compatibilidad de las disposiciones de derecho penal relativas a la cibercriminalidad con las de otros países
- Base jurídica e institucional para el cumplimiento de la legislación a nivel internacional y la cooperación judicial con otras partes en el Convenio
- Participación en las consultas de las partes en el Convenio
- El tratado como plataforma que facilita la cooperación público-privada

Alcance del Convenio de Budapest



Ratificaciones:	68				
Firmas:	2		Otros Estados con leyes sustantivas bastante alineadas con la convención:	45+	
Invitaciones a acceder:	12		Estados que han utilizado la convención como marco de desarrollo legislativo:	30+	
=	**82**		**=**	**75+**	

Segundo Protocolo adicional relativo a la cooperación reforzada y a la divulgación de pruebas electrónicas: nuevas herramientas de cooperación

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

La ciberdelincuencia: una amenaza para

- Los derechos humanos
- La democracia
- El Estado de Derecho

Obligaciones positivas:

- Asegurar los medios para proteger los derechos de las personas, incluso contra la delincuencia

Problema:

- Proliferación de la ciberdelincuencia
- Hoy en día, todos los delitos implican pruebas electrónicas
- Las pruebas están en algún lugar en jurisdicciones extranjeras, múltiples, cambiantes o desconocidas
- No se dispone de medios eficaces para obtener la divulgación de pruebas electrónicas
- Menos del 0,1% de los casos de ciberdelincuencia acaban en juicios y condenas

- ¿Se hace justicia a las víctimas?

2º Protocolo Adicional ayuda a afrontar estos desafíos

Argumento: ¿Por qué un 2° Protocolo Adicional al Convenio de Budapest?

- ¿Cómo obtener datos de abonados de manera eficiente?
- ¿Cómo cooperar directamente con un proveedor de servicios ubicado en el territorio de otra Parte?
- ¿Cómo obtener datos WHOIS (información de registro de dominio) de los registradores?
- ¿Cómo obtener datos almacenados, incluidos datos de contenido, en caso de emergencia?
- ¿Cómo hacer la asistencia mutua más eficaz?
- ¿Cómo reconciliar medidas eficaces y efectivas con requisitos relativos al estado de derecho y a la protección de datos personales?

2° Protocolo Adicional al Convenio sobre la Ciberdelincuencia: proceso de negociación

Protocolo:

- Preparado por la Plenaria de Redacción (PDP, por su sigla en inglés) y los Grupos de Redacción (PDG, por su sigla en inglés) del Protocolo creados por el Comité del Convenio sobre la Ciberdelincuencia, septiembre de 2017 – mayo de 2021
- 91 reuniones de los PDP, PDG y subgrupos de PDG
- 75 estados y varias organizaciones internacionales participaron con más de 620 expertos
- Especialistas en protección de datos también tomaron parte en las negociaciones
- 6 reuniones de consulta dedicadas a varias partes interesadas

= Un texto cuidadosamente calibrado, diseñado a ser compatible con el acervo del Consejo de Europa y, al mismo tiempo, a satisfacer los requisitos de todas las otras Partes del Convenio de Budapest

2º Protocolo Adicional al Convenio sobre la Ciberdelincuencia: contenido

Preámbulo

Capítulo I: Disposiciones comunes

Artículo 1 Finalidad

Artículo 2 Ámbito de aplicación

Artículo 3 Definiciones

Artículo 4 Idioma

Capítulo II: Medidas de cooperación reforzada

Artículo 5 Principios generales aplicables al Capitulo II

Artículo 6 ***Solicitud de información sobre el registro de nombres de dominio***

Artículo 7 ***Divulgación de la información de los abonados***

Artículo 8 ***Dar efecto a las ordenes de otra parte para la producción acelerada de información sobre los abonados y datos de tráfico***

Artículo 9 ***Divulgación acelerada de datos informáticos almacenados en caso de emergencia***

Artículo 10 ***Asistencia mutua en caso de emergencia***

Artículo 11 Videoconferencia

Artículo 12 Equipos conjuntos de investigación e investigaciones conjuntas

Capítulo III – Condiciones y salvaguardias

Artículo 13 Condiciones y salvaguardias

Artículo 14 Protección de datos personales

Capítulo IV: Disposiciones finales

Artículo 15 Efectos del presente Protocolo

Artículo 16 Firma y entrada en vigor

Artículo 17 Cláusula federal

Artículo 18 Aplicación teritorial

Artículo 19 Reservas y declaraciones

Artículo 20 Situación y retirada de las reservas

Artículo 21 Enmiendas

Artículo 22 Solución de controversias

Artículo 23 Consultas de las Partes y evaluación de la aplicación

Artículo 24 Denuncia

Artículo 25 Notificación

2° Protocolo Adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la divulgación de pruebas electrónicas (CETS 224)

Firmas (*al 28 de septiembre 2023*)**:**

1. Andorra
2. Austria
3. Bélgica
4. Bulgaria
5. Chile
6. Colombia
7. Costa Rica
8. Estonia
9. Finlandia
10. Islandia
11. Italia
12. Japón
13. Lituania
14. Luxemburgo
15. Montenegro
16. Moroco
17. Países Bajos
18. Macedonia del Norte
19. Portugal
20. Rumanía
21. Serbia
22. España
23. Suecia
24. EE.UU
25. Croacia
26. Moldova
27. Slovenia
28. Sri Lanka
29. Ucrania
30. Reino Unido
31. Grecia
32. Francia
33. Alemania
34. **Rep. Dominicana**
35. Argentina
36. Albania
37. Islas Mauricio
38. Canadá
39. Malta

Siguientes pasos:

- ► Firma por otras Partes
- ► Ratificación (5 para entrar en vigor)
- ► Desarrollo de capacidades

Ratificaciones:

1. Serbia 9/Feb/2023
2. Japón 10/Ago/2023

Experiencia de la Republica Dominicana en el Marco Legal y Normativo Contra el CIBERDELITO

- 2003 - Primera investigación “delito informático”

Experiencia de la Republica Dominicana en el Marco Legal y Normativo Contra el CIBERDELITO

- 2003 - Primera investigación “delito informático”
- 2004 - Redacción proyecto de ley utilizando el marco del Convenio de Budapest

Experiencia de la Republica Dominicana en el Marco Legal y Normativo Contra el CIBERDELITO

- 2003 - Primera investigación “delito informático”
- 2004 - Redacción proyecto de ley utilizando el marco del Convenio de Budapest
- 2007 - Promulgación **Ley 53-07 contra Crímenes y Delitos de Alta Tecnología**

Experiencia de la Republica Dominicana en el Marco Legal y Normativo Contra el CIBERDELITO

- 2003 - Primera investigación “delito informático”
- 2004 - Redacción proyecto de ley utilizando el marco del Convenio de Budapest
- 2007 - Promulgación **Ley 53-07 contra Crímenes y Delitos de Alta Tecnología**
- 2008 - Solicitud al Consejo de Europa de invitación a acceder al Convenio

Experiencia de la Republica Dominicana en el Marco Legal y Normativo Contra el CIBERDELITO

- 2003 - Primera investigación “delito informático”
- 2004 - Redacción proyecto de ley utilizando el marco del Convenio de Budapest
- 2007 - Promulgación **Ley 53-07 contra Crímenes y Delitos de Alta Tecnología**
- 2008 - Solicitud al Consejo de Europa de invitación a acceder al Convenio
- 2013 - Ratificación **Convenio de Budapest** por el Congreso Nacional,

  convirtiéndose en el *primer país del hemisferio (no firmante en 2001) en adherirse*.

Experiencia de la Republica Dominicana en el Marco Legal y Normativo Contra el CIBERDELITO

- 2003 - Primera investigación “delito informático”
- 2004 - Redacción proyecto de ley utilizando el marco del Convenio de Budapest
- 2007 - Promulgación **Ley 53-07 contra Crímenes y Delitos de Alta Tecnología**
- 2008 - Solicitud al Consejo de Europa de invitación a acceder al Convenio
- 2013 - Ratificación **Convenio de Budapest** por el Congreso Nacional,
  convirtiéndose en el *primer país del hemisferio (no firmante en 2001) en adherirse*.
- 2018 – Establecimiento de la Estrategia Nacional de Ciberseguridad mediante el Decreto 230-18
  con un plan complementario contra los ciberdelitos.
  - Creación **Centro Nacional de Ciberseguridad** y CSIRT-RD

Experiencia de la Republica Dominicana en el Marco Legal y Normativo Contra el CIBERDELITO

- 2003 - Primera investigación “delito informático”
- 2004 - Redacción proyecto de ley utilizando el marco del Convenio de Budapest
- 2007 - Promulgación **Ley 53-07 contra Crímenes y Delitos de Alta Tecnología**
- 2008 - Solicitud al Consejo de Europa de invitación a acceder al Convenio
- 2013 - Ratificación **Convenio de Budapest** por el Congreso Nacional,
  convirtiéndose en el *primer país del hemisferio (no firmante en 2001) en adherirse*.
- 2018 – Establecimiento de la Estrategia Nacional de Ciberseguridad mediante el Decreto 230-18
  con un plan complementario contra los ciberdelitos.
  - Creación **Centro Nacional de Ciberseguridad** y CSIRT-RD
- 2019 – Inicio actualización Ley 53-07 contra **Ciberdelitos**
  – Inicio redacción proyecto de ley de **Protección de Datos Personales**
  – Inicio redacción proyecto de ley de **Ciberseguridad**

Experiencia de la Republica Dominicana en el Marco Legal y Normativo Contra el CIBERDELITO

- 2003 - Primera investigación “delito informático”
- 2004 - Redacción proyecto de ley utilizando el marco del Convenio de Budapest
- 2007 - Promulgación **Ley 53-07 contra Crímenes y Delitos de Alta Tecnología**
- 2008 - Solicitud al Consejo de Europa de invitación a acceder al Convenio
- 2013 - Ratificación **Convenio de Budapest** por el Congreso Nacional,
  convirtiéndose en el *primer país del hemisferio (no firmante en 2001) en adherirse*.
- 2018 – Establecimiento de la Estrategia Nacional de Ciberseguridad mediante el Decreto 230-18
  con un plan complementario contra los ciberdelitos.
  - Creación **Centro Nacional de Ciberseguridad** y CSIRT-RD
- 2019 – Inicio actualización Ley 53-07 contra **Ciberdelitos**
  – Inicio redacción proyecto de ley de **Protección de Datos Personales**
  – Inicio redacción proyecto de ley de **Ciberseguridad**
- 2020 – República Dominicana electa Vice-Presidente por GRULAC del Comité Ad-Hoc para elaborar
  una nueva convención internacional contra los ciberdelitos de la Organización de las Naciones Unidas (ONU)
  - 2da. versión de la Estrategia Nacional de Ciberseguridad 2030

Experiencia de la Republica Dominicana en el Marco Legal y Normativo Contra el CIBERDELITO

- 2022 - Presidente del Grupo de Trabajo Ciber-Amercias de INTERPOL
  - Vicepresidente del Grupo de Trabajo de Medidas de Fomento de la Confianza de la OEA
  - Designación de un Ciber-Embajador (primero en LAC, 2do en el hemisferio después de EE.UU.)

Experiencia de la Republica Dominicana en el Marco Legal y Normativo Contra el CIBERDELITO

- 2022 - Presidente del Grupo de Trabajo Ciber-Amercias de INTERPOL
  - Vicepresidente del Grupo de Trabajo de Medidas de Fomento de la Confianza de la OEA
  - Designación de un Ciber-Embajador (primero en LAC, 2do en el hemisferio después de EE.UU.)

- 2023 – Firma del 2do. Protocolo adicional del Convenio de Budapest.
  – Remisión al Congreso Nacional proyecto de modificación Ley 53-07 contra **Ciberdelitos**
  – Remisión al Congreso Nacional proyecto de ley de **Protección de Datos Personales**
  – Remisión al Congreso Nacional proyecto de ley de **Ciberseguridad**

Experiencia de la Republica Dominicana en el Marco Legal y Normativo Contra el CIBERDELITO

- 2022 - Presidente del Grupo de Trabajo Ciber-Amercias de INTERPOL
  - Vicepresidente del Grupo de Trabajo de Medidas de Fomento de la Confianza de la OEA
  - Designación de un Ciber-Embajador (primero en LAC, 2do en el hemisferio después de EE.UU.)

- 2023 – Firma del 2do. Protocolo adicional del Convenio de Budapest.
  – Remisión al Congreso Nacional proyecto de modificación Ley 53-07 contra **Ciberdelitos**
  – Remisión al Congreso Nacional proyecto de ley de **Protección de Datos Personales**
  – Remisión al Congreso Nacional proyecto de ley de **Ciberseguridad**

Y SEGUIMOS!!

Proceso de la ONU sobre Ciberdelitos y Ciberseguridad

El Comité Ad-Hoc *"encargado de elaborar una nueva convención internacional contra el uso criminal de las tecnologías de información y comunicación"*

UNODC
United Nations Office on Drugs and Crime

VII CONGRESO DE INFORMÁTICA FORENSE Y CIBERSEGURIDAD
IFC 2023
Informática Forense & Ciberseguridad
26 al 29 de Octubre del 2023, Punta Cana, Rep Dom

El proceso de la ONU sobre Ciberdelitos y Ciberseguridad

- **Grupo Intergubernamental de Expertos (IEG) en Cibercrimen** creado en 2010 mediante resolución 65/230 de la Asamblea General adoptada en el 12vo. Congreso de Prevención del Delito y Justicia Criminal en Salvador de Bahía, Brasil (RD participa activamente desde 2017).

- **Grupo de Trabajo de Composición Abierta (OEWG) sobre Ciberseguridad** creado en 2019 mediante resolución 73/27 de la Asamblea General.

- **Comité Ad Hoc para Elaborar una Convención Internacional Comprensiva Contra el Uso de las Tecnologías de Información y Comunicación para Propósitos Criminales** creado mediante resolución 74/247 de la Asamblea General en 2019.

Resolución AG 65/230

12vo Congreso de las Naciones Unidas en Prevencion del Delitos y Justicia Criminal Salvador de Bahia, Brasil, 12-19 Abril 2010

Grupo Intergubernamental de Expertos de Composición Abierta para realizar un estudio exhaustivo del problema del delito cibernético

- Primera sesión, Viena, 17-21 Enero 2011
- Segunda sesión, Viena, 25-28 Febrero 2013
- Tercera sesión, Viena, 10-13 Abril 2017
- Cuarta sesión, Viena, 3-5 Abril 2018
- Quinta sesión, Viena, 27-29 Marzo 2019
- Sexta sesión, Viena, 27-29 Julio 2020
- Septima sesión, Viena, 6-8 Abril 2021

Resolución AG 74/247

27 Diciembre 2019

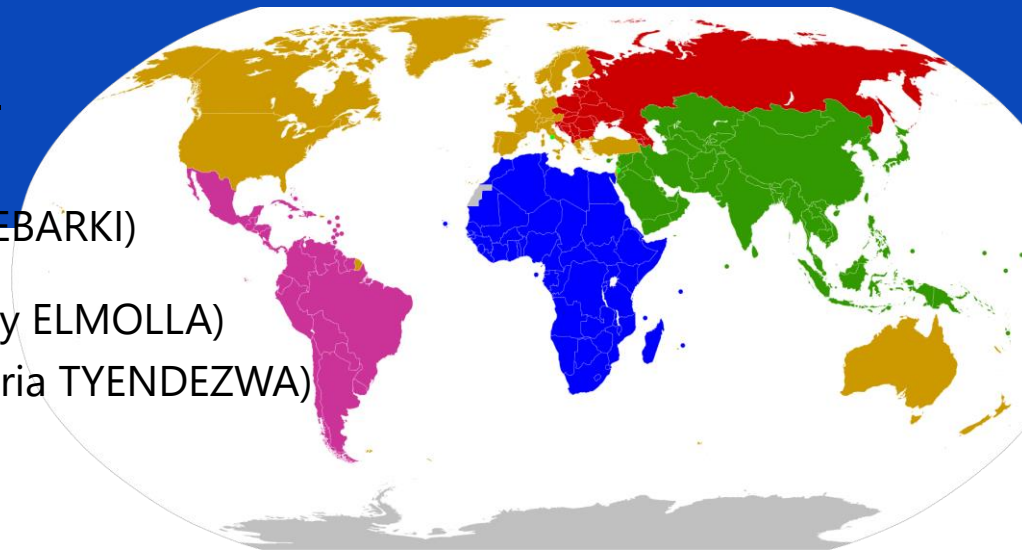
Estableció un "**Comité intergubernamental Ad Hoc de expertos de composición abierta para elaborar una convención internacional comprensiva sobre la lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos**"

- Sesión organizacional, NY, 10-12 May 2021
- Primera sesión, NY, 28 Feb-11 Mar 2022
- Segunda sesión, Viena 30 May - 10 Jun 2022
- Tercera sesión, NY 29 Ago - 9 Sept 2022
- Cuarta sesión, Viena 9 – 20 Ene 2023
- Quinta sesión, Viena 11– 21 Abr 2023
- Sexta sesión, NY 21 Ago – 1 Sept 2023
- Sesión final, NY, 29 Ene – 9 Feb 2024

Roadmap AHC

1ra Sesión	Nueva York, 28 Feb – 11 Marzo 2022	Objetivos, alcance y estructura de la convención. Modalidades de trabajo AHC.
Consulta intersesional	Viena, 24-25 Marzo 2022	
2da Sesión	Viena, 30 Mayo – 10 Junio 2022	Primera lectura de las provisiones sobre criminalización, provisiones generales, medidas procesales y cumplimiento de la ley.
Consulta intersesional	Viena, 13-14 Junio 2022	
3ra Sesión	Nueva York, 29 Ago – 9 Sept 2022	Primera lectura de las provisiones sobre cooperación internacional, asistencia técnica, medidas preventivas y mecanismo de implementación, provisiones finales y preámbulo.
Consulta intersesional	Viena, 31 Oct – 11 Nov 2022 (2 días)	
4ta Sesión	Viena, 9 – 20 Enero 2023	Segunda lectura de las provisiones sobre criminalización, provisiones generales, medidas procesales y cumplimiento de la ley.
Consulta intersesional	Viena, 6-10 Marzo 2023 (2 días)	
5ta Sesión	Viena 11 – 21 Abril 2023	Segunda lectura de las provisiones sobre cooperación internacional, asistencia técnica, medidas preventivas y mecanismo de implementación, provisiones finales y preámbulo.
Consulta intersesional	Viena, 12-23 Junio 2023 (2 días)	
6ta Sesión	Nueva York 21 Ago – 1 Sept 2023	Tercera lectura del borrador del texto completo de la convención
Sesión final	Nueva York, 29 Ene – 9 Feb 2024	Finalización y aprobación del texto de la convención; discusión y aprobación de un borrador de resolución que deberá llevar el texto de la convención anexo, para consideración y adopción por la Asamblea General en su 78va sesión en

Representación regional: *Oficiales del Buró*



Presidente - Grupo de África: **Argelia** (Emb. Faouzia BOUMAIZA MEBARKI)

Vice-Presidente - Grupo de África: **Egipto** (Emb. Mohamed Hamdy ELMOLLA)
Vice-Presidente - Grupo de África: **Nigeria** (Terlumun George-Maria TYENDEZWA)

Vice-Presidente - Grupo Asia-Pacifico: **China** (WU Haiwen)
Vice-Presidente - Grupo Asia-Pacifico: **Japon** (Chitaru SHIMIZU)

Vice-Presidente - Grupo Europa del Este: **Estonia** (Markko KÜNNAPU)
Vice-Presidente - Grupo Europa del Este : **Polonia** (Emb. Dominika KROIS)
Vice-Presidente - Grupo Europa del Este : **Federacion Rusa** (Dmitry BUKIN)

Vice-Presidente - ***GRULAC***: ***República Dominicana*** (Claudio PEGUERO CASTILLO)
Vice-Presidente - ***GRULAC*** : **Nicaragua** (Emb. Sabra Amari MURILLO CENTENO)
Vice-Presidente - ***GRULAC*** : **Brasil** (Eric SOGOCIO)

Vice-Presidente - Grupo Europa Occidental y Otros Estados: **Australia** (Emil STOJANOVSKI)
Vice-Presidente - Grupo Europa Occidental y Otros Estados : **Portugal** (Emb. ALMEIDA RIBEIRO)
Vice-Presidente - Grupo Europa Occidental y Otros Estados : **Estados Unidos** (James WALSH)

- **Relator** - Grupo Asia-Pacifico : **Indonesia** (Arsi Dwinugra FIRDAUSY)

Gracias!

¿Preguntas?

Claudio Peguero

Embajador

Asesor en Asuntos Ciberneticos

Ministerio de Relaciones Exteriores

República Dominicana

cmpeguero@mirex.gob.do

@cmpeguero

https://linktr.ee/cpeguero