**Propuesta de una Convención Internacional contra la Delincuencia Cibernética y Terrorismo**

**Abraham D. Sofaer
Seymour E. Goodman
, Mariano Florentino Cuéllar
Ekaterina A. Drozdova
David Elliott D.
Gregory D. Grove
Stephen J. Lukasik
Tonya L. Putnam
George D. Wilson**

**08 2000**

Conjuntamente patrocinado por:
The Hoover Institution
El Consorcio para la Investigación en Seguridad y Política (CRISP) Información
El Centro para la Seguridad y Cooperación Internacional (CISAC),
la Universidad de Stanford

Las opiniones expresadas aquí son responsabilidad de los autores y no representan necesariamente la posición de la Hoover Institution, CISAC, fresco, sus partidarios, el Gobierno de los EE.UU. (o cualquier departamento o agencia del mismo) o la Universidad de Stanford.

**Resumen Ejecutivo**

La infraestructura de la información es cada vez más atacados por los delincuentes cibernéticos. El número, costo y sofisticación de los ataques están aumentando a un ritmo alarmante. Daño total anual mundial de los ataques ahora se mide en miles de millones de dólares. Los ataques amenazan la dependencia sustancial y creciente del comercio, los gobiernos y al público sobre la infraestructura de la información para hacer negocios, llevar mensajes, y procesar la información. Ataques más importantes son transnacionales por su diseño, con las víctimas de todo el mundo.

Las medidas hasta ahora adoptadas por los sectores público y privado no han proporcionado un nivel adecuado de seguridad. Mientras que los nuevos métodos de ataque han sido predichos con exactitud por los expertos y algunos ataques a gran escala han sido detectados en las primeras etapas, los esfuerzos para prevenir o dificultar han fracasado, con consecuencias cada vez más perjudiciales. La información necesaria para combatir los ataques no ha sido compartida a tiempo. Las investigaciones han sido lentos y difíciles de coordinar. Algunos ataques son parte de los Estados que carecen de leyes adecuadas que rigen la conducta destructiva deliberada. Este tipo de cooperación internacional, como ocurre es voluntaria e inadecuada. Algunos mejora significativa de la capacidad defensiva parece esencial. La ciberdelincuencia es esencialmente transnacional, ya menudo implican afirmaciones jurisdiccionales de varios Estados. Acuerdos sobre competencia y reconocimiento se deben desarrollar para evitar reclamaciones conflictivas.

La necesidad y métodos para efectuar la cooperación internacional en la lucha contra el delito cibernético y el terrorismo fueron el tema de una conferencia patrocinada por la Institución Hoover, el Consorcio para la Investigación en Seguridad y Política (CRISP) Información y el Centro para la Seguridad y Cooperación Internacional (CISAC) en la Universidad de Stanford en 6 a 7 diciembre 1999 (la "Conferencia de Stanford"). Los miembros del gobierno, la industria, las organizaciones no gubernamentales y el sector académico de muchas naciones conocieron en Stanford para discutir el problema cada vez mayor. Un claro consenso de que es necesaria una mayor cooperación internacional y un acuerdo considerable de que un tratado multilateral centrado en el abuso de los sistemas cibernéticos podría ayudar a crear el marco de cooperación necesario. (Una síntesis de los trabajos de la Conferencia de Stanford y la discusión será publicado por la prensa de Hoover.) Esta monografía resume y presenta el Proyecto de Convención Internacional Stanford para mejorar la seguridad de la delincuencia en el ciberespacio y el terrorismo (el "Proyecto de Stanford" o el "Proyecto") y Comentario sobre el proyecto. El proyecto reconoce y se basa en el proyecto de Convención sobre el Delito Cibernético propuesto por el Consejo de Europa (el "COE Proyecto").

¿Por qué una Convención Multilateral

· La ciberdelincuencia es transnacional, y requiere una respuesta transnacional.

· Los ciberdelincuentes explotan las debilidades en las leyes y prácticas de aplicación de los Estados, la exposición de todos los demás Estados a los peligros que se encuentran más allá de su capacidad de manera unilateral o bilateral de responder.

· La velocidad y la complejidad técnica de las actividades cibernéticas requiere predispuestos, los procedimientos de cooperación acordados en la investigación y responder a las amenazas y ataques.

· Un convenio multilateral se asegurará de que todos los Estados Partes:

- Adoptar leyes que hacen actividades cibernéticas peligrosos criminales;

- Hacer cumplir esas leyes o extraditar a los criminales para el procesamiento de otros Estados;

- Cooperar en la investigación de las actividades delictivas y para aportar pruebas utilizables para procesamientos y

- Participar en la formulación y convenir en adoptar y aplicar las normas y prácticas que mejoren la seguridad y la seguridad.

· Un organismo internacional creado en virtud del proyecto de Convención servirá de foro para el debate internacional, la respuesta permanente a la evolución tecnológica y la asistencia técnica a los Estados en desarrollo.

***Delitos tipificados***

El Proyecto de Stanford está diseñado para fomentar el reconocimiento universal de los delitos básicos en el ciberespacio y el acuerdo universal a cooperar en la investigación, extraditar y enjuiciar a los perpetradores. (El proyecto excluye específicamente la conducta del Estado, frente a sólo un comportamiento de personas o grupos.) El artículo 3 describe la conducta que cubre, entre ellas: interferir con la función de un sistema cibernético, la culpa, la manipulación de los sistemas de autenticación, lo que interfiere con los datos, el tráfico de herramientas cibernéticas ilegales, utilizando sistemas informáticos de otros delitos especificados en otros tratados y la orientación infraestructuras críticas. Los Estados Partes se comprometen a castigar a todas las formas de conducta especificadas. El artículo 3 se redactó con el objetivo de asegurar un acuerdo rápido entre las naciones a adoptar definiciones comunes de delitos y compromisos, a pesar de tener diferentes capacidades de la red y los intereses políticos. Por lo tanto, los delitos relacionados con las cuestiones más controvertidas, como la protección de la propiedad intelectual y la regulación de contenido político, ético o religioso, se omiten. Implementación de los delitos tratados se efectuará en el derecho interno de los signatarios, de conformidad con el artículo 2.

***Cooperación Internacional en Investigación y Persecución***

Los participantes en la Conferencia de Stanford debatieron técnica, jurídica, política y diplomática preocupaciones, y muchas de estas disciplinas dispares de acuerdo en que la necesidad más importante en la lucha contra el crimen cibernético y el terrorismo es el desarrollo de relaciones de cooperación, personales entre los agentes de la ley del gobierno y expertos técnicos de todo el mundo. Los éxitos han fluido de las redes informales existentes de expertos, que colaboran para resolver los incidentes transfronterizos que se produzcan. Incluso los mayores éxitos podrían resultar de la armonización de las leyes, el establecimiento de normas técnicas, los mecanismos de respuesta a emergencias internacionales de cooperación, y el intercambio de inteligencia.

El Proyecto de Stanford requiere la cooperación del Estado Parte en la investigación a través de la asistencia jurídica mutua y las disposiciones de aplicación de la ley se especifican en los artículos 6 y 11.Estados Partes están obligados a intercambiar información, ayudar en la recopilación y preservación de pruebas, detener presuntos delincuentes, procesar o extraditar a ellos, y para aplicar las normas internacionales acordadas que se ocupan de la seguridad y el orden público.

***Jurisdicción y extradición***

El artículo 5 del proyecto confirma la jurisdicción prescriptiva y la ejecución en los Estados donde se cometen delitos, donde los presuntos delincuentes son ciudadanos, residan o estén presentes, o cuando la conducta de los delincuentes tiene efectos sustanciales. Se establece prioridad en la jurisdicción, descansando primero en que el delincuente está físicamente presente cuando se produce el delito, en segundo lugar donde se sufrió daños considerables, y la tercera en el Estado de la nacionalidad dominante del delincuente. El artículo 7 del proyecto requiere que todos los Estados en los que un delincuente alegado está presente ya sea para enjuiciar o extraditar.

***La Agencia Internacional de la***

El artículo 12 del Proyecto de Stanford propone una Agencia internacional para la Protección de la Infraestructura de la Información (AIIP). El AIIP está destinado a servir como una estructura formal en la que los grupos interesados ​​cooperarán a través de expertos en países de todo el mundo en el desarrollo de normas y prácticas relativas a la seguridad cibernética.

La estructura de la representación AIIP se inspira en los tratados constitutivos de la Organización de Aviación Civil Internacional (OACI) y la Unión Internacional de Telecomunicaciones (UIT). Todos los Estados Partes están representados en la Asamblea AIIP, que adopte objetivos y políticas acordes con la Convención, aprobar las normas y prácticas de cooperación, y aprobar los programas de asistencia técnica, entre otras responsabilidades. El Consejo AIIP, elegido por la Asamblea, permitiría, entre otras funciones, nombrar comités para estudiar los problemas particulares y recomendar medidas para la Asamblea. El proyecto prevé también una Secretaría para realizar tareas administrativas. El AIIP sería aprovechar y complementar, no intente modificar o sustituir, las actividades del sector privado.

***Privacidad y Derechos Humanos***

El artículo 13 del Proyecto de Stanford permite a los Estados Partes a establecer y mantener sus propias normas para la privacidad y los derechos humanos. La notificación consular y otras protecciones de procedimiento se proporcionan para todas las personas detenidas en virtud del Proyecto. Además, el artículo 13 establece un comité permanente de la AIIP para estudiar y recomendar al Consejo medidas para proteger la privacidad y otros derechos humanos.

***Comentario***

Un comentario importante precede al Proyecto. El comentario explica el consenso emergente en contra de ciertas actividades, ciber destructivos, y las ventajas y desventajas de utilizar un enfoque multilateral para abordar este problema. El comentario explica por qué algunas disposiciones se incluyen en el proyecto, y por qué se omiten algunas cuestiones, tales como la infracción de derechos de autor y de los delitos relacionados con el contenido del habla,. En él se compara el proyecto de Stanford con el Proyecto de COE, y analiza el papel que se espera y la influencia del sector privado en el desarrollo de normas, y el otro trabajo de la AIIP propuesto.

**Introducción**

Los métodos de ataque de la infraestructura de información son ni misteriosa ni difícil de prever, en la Conferencia de Stanford, Thomas Longstaff del Computer Emergency Response Team Carnegie-Mellon ("CERT") prevé que, a finales de 1999 o principios de 2000, una nueva y muy dañina distribuye forma de ataque de denegación de servicio podría ser frecuente. Él basó sus predicciones sobre las observaciones de los intercambios de hackers públicas que las estrategias de ataque compartidos y software para implementar esas estrategias. Longstaff predijo con precisión el método utilizado por los hackers en los posteriores, en todo el mundo, los ataques de febrero 2000 en la CNN, eBay, Yahoo!, Amazon.com, las empresas de inversión en línea y otros. A pesar de ser capaz de anticiparse a los ataques de este tipo, los agentes del orden fueron incapaces de prevenir, y personal de seguridad empleado por los sistemas informáticos específicos fueron incapaces de defenderse de ellos. Estas fallas inquietantes provienen de serias debilidades en las capacidades de los Estados para proteger los sistemas informáticos valiosos de los ataques que ponen en peligro rápida escalada. Como se dijo Longstaff, métodos eficaces para proteger contra ataques de denegación de servicio pueden ser mejor abordados por la cooperación regional, nacional e internacional.

La forma abierta y desafiante en el que los atacantes operan actualmente refleja la debilidad de la capacidad jurídica, a la defensiva, y de investigación del sistema actual. Algunos atacantes están atrapados después de largas y costosas investigaciones, pero la mayoría quedan impunes. Las incapacidades se derivan en última instancia de que la infraestructura de la información es de carácter transnacional. Los atacantes deliberadamente manera sus esfuerzos para aprovechar la ausencia de normas acordadas internacionalmente de la conducta y la cooperación. Por ejemplo, un atacante puede evitar el enjuiciamiento o complicar en gran medida las investigaciones, simplemente mediante el inicio de paquetes de ataque de países con leyes inadecuadas, y el encaminamiento a través de países con diferentes leyes y prácticas, y no existen estructuras de cooperación.

La falta de una respuesta internacional adecuada a estos puntos débiles es sorprendente, teniendo en cuenta el impacto financiero enorme y creciente de los ataques cibernéticos y delitos. Incluso si son exagerados algunas estimaciones de daños, el problema ha crecido sin duda costoso para las empresas, gobiernos y consumidores de todo el mundo. Se requiere una acción multilateral para fomentar la seguridad en la estructura técnica y social subyacente. La historia ha demostrado que cuando las naciones están de acuerdo en una amenaza maliciosa común, ya sea la piratería en alta mar hace siglos o el terrorismo de la aviación del siglo 20, un régimen cooperativo, tratado mediada puede contribuir sustancialmente a solucionar el problema.

El reto de la lucha contra la delincuencia cibernética en sus dimensiones más importantes requiere una amplia gama de respuestas, incluyendo tanto la cooperación voluntaria y jurídicamente obligatorio.Existe un consenso en torno a muchas formas de conducta que deben ser tratados como delitos cibernéticos. Las posiciones comunes se están desarrollando o se pueden diseñar para facilitar la cooperación en la investigación, la conservación de las pruebas, y la extradición. La cooperación también es fundamental en el desarrollo e implementación de soluciones y estándares para mejorar la capacidad de los Estados y los usuarios con eficacia para proteger los equipos y sistemas contra ataques futuros tecnológicos.

La naturaleza y la cultura de la demanda mundial cibernética que estas respuestas sean moda para maximizar la participación y el control del sector privado, así como para asegurar que la privacidad y otros derechos humanos no se vean perjudicados. Ciertos elementos de un programa eficaz contra la delincuencia cibernética requerirá control o aprobación del estado, sin embargo. Además, para desarrollar y asegurar la adopción universal de las normas tecnológicas y políticas para defenderse, juzgar y prevenir el crimen cibernético y el terrorismo requerirá un foro internacional con la autoridad y la capacidad necesaria. Esto se puede lograr mediante la creación de una Agencia internacional para la Protección de la Infraestructura de la Información (AIIP), un organismo diseñado para reflejar las necesidades y la naturaleza del mundo cibernético en gran medida autorregulado en particular y el modelo de la Organización de Aviación Civil Internacional (OACI) y la Unión Internacional de Union (ITU).

Si bien se ha producido el crecimiento y la confianza en las infraestructuras de información reciente en la ausencia de participación de los gobiernos importantes, la idea de que las actividades de voluntariado solo pueden crear una seguridad adecuada para actividades cibernéticas que ahora involucran a 300 millones de personas en Internet solo es simplemente insostenible. A nivel nacional, el crimen cibernético es probable que sea aún más frecuente y costosa de lo que se ha tenido gobiernos abandonaron la zona unpoliced. Las leyes aprobadas hasta el momento en que hacen los ciberataques penal han proporcionado al menos un vehículo por el cual para arrestar - y por lo tanto se detengan, castigar y disuadir - ciberdelincuentes. La gran mayoría de los usuarios - comercial, educativo, personal - Derecho a favor sobre la anarquía, cuando se trata de ataques cibernéticos diseñados para robar, engañar y destruir. Lo mismo ocurre en el ámbito internacional, donde sólo a través de la acción del gobierno se pueden pasar leyes establecen normas universales de conducta, autorizando la cooperación de investigación, la extradición y la adopción de métodos tecnológicamente avanzados para detectar, bloquear, rastrear y disuadir las conductas prohibidas.

Liderazgo multilateral no debe significar la subordinación de la dirección privada y la influencia sobre la tecnología cibernética y las operaciones. La revolución cibernética ha sido excepcionalmente exitoso y rápido, ya que está dirigida y controlada en gran medida por el sector privado. Gobierno, sin embargo, jugó un papel fundamental en el apoyo y dar autoridad legal para las instituciones privadas. Esta distribución del poder y la responsabilidad puede continuar, y de hecho ser mejorado, por el continuo apoyo y la autoridad del AIIP. Los gobiernos no pueden esperar responsablemente el sector privado para resolver el problema de la seguridad cibernética. Sector empresarial, en la infraestructura de información han dejado claro que el sector privado no puede esperar para llevar a cabo las funciones tradicionalmente desempeñadas por la policía. Sin embargo, un mayor papel del gobierno no tiene que ser uno que requiere significativamente mayores poderes nacionales o medidas más intrusivas, más bien, es la necesidad de la cooperación internacional para crear normas y prácticas comunes. Estos objetivos pueden lograrse sin conferir poderes inadecuados o innecesarios a los gobiernos para regular y para inmiscuirse en los sistemas informáticos, y al mismo tiempo preservar el control del sector privado de este sector exclusivamente productivo y dinámico.

**Comentario sobre el Proyecto de Convención**

La defensa de la cooperación internacional en la lucha contra el delito cibernético es abrumadora. El debate en curso es sobre la forma y el alcance dicha cooperación debe tomar, y el grado en que los Estados Unidos y otros Estados tecnológicamente avanzados deben confiar en los esfuerzos multilaterales para mejorar la seguridad cibernética.

Propuestas para la cooperación internacional de carácter voluntario se han avanzado y se están aplicando. Los principales elementos de estas propuestas - para capacitar a los funcionarios encargados de hacer cumplir la ley para comprender y hacer frente a los delitos cibernéticos, y establecer equipos de respuesta de emergencia alrededor del reloj - son ampliamente compatibles. Además, el Grupo de los Ocho (G-8) y los grupos privados como la Alianza Internet han publicado directrices destinadas a hacer más eficaz la cooperación voluntaria. Si bien estos grupos reconocen que la cooperación internacional es esencial, todavía tienen que aceptar la idea de que un tratado internacional debe negociar el establecimiento de normas y obligaciones legalmente establecidos.

Apoyo a la voluntaria, a diferencia jurídicamente obligatorias, las medidas internacionales se apoya en varios argumentos. Delito cibernético más, se argumenta, es el crimen convencional (por ejemplo, fraude, tráfico de drogas, lavado de dinero, la explotación sexual de menores de edad), en la que la tecnología cibernética pasa a ser utilizado. Los tratados existentes y los acuerdos internacionales, incluyendo las referentes a la extradición y la asistencia legal, son potencialmente aplicables en estos casos. Asegurar un acuerdo internacional sobre la redacción de nuevos delitos cibernéticos, será difícil, por otra parte, y existen grandes diferencias entre los Estados en relación con la regulación adecuada de contenido, el ámbito concreto de la investigación transnacional y las bases sobre las que el seguimiento de la información y los mensajes deben ser objeto de incautación y escrutinio. Por otra parte, existe una gran disparidad entre los Estados - incluso los tecnológicamente avanzados - en cuanto al alcance de la privacidad y otros derechos que poseen los individuos bajo las leyes nacionales que, o bien operar para limitar un acuerdo internacional o estar en peligro por una. Finalmente, el Internet, muchos creen, ha sido un poderoso vehículo para el crecimiento económico y la mejora de la comunicación, en gran parte debido a que es controlada por el sector privado, en lugar de los gobiernos, y este crecimiento y la creatividad puede ser afectado adversamente por los requisitos legales internacionales y la regulación .

Por estas razones, a Drew C. Arena, entonces Asesor Principal del Procurador General Adjunto, Departamento de Justicia de EE.UU., comentó en la Conferencia de Stanford que el logro de un consenso sobre "las medidas concretas" que se deben tomar en la negociación de un tratado multilateral sería "muy difícil "en el momento actual para justificar el esfuerzo. Universidad de Chicago Escuela de Derecho Profesor Jack L. Goldsmith ha argumentado que, en ausencia de un régimen internacional adecuado, los Estados Unidos deberían recurrir a medidas unilaterales en la lucha contra la delincuencia cibernética transnacional. Sin embargo, él, en principio, a favor de la búsqueda de un régimen de este tipo.

Los argumentos en contra de la creación de un régimen jurídico internacional para hacer frente a la seguridad cibernética son convincentes, pero en base a las dificultades y peligros que se pueden evitar.El argumento a favor de un acuerdo multilateral para combatir el delito cibernético y el terrorismo es fuerte, y la necesidad de emprender el esfuerzo de negociar una vez está más claro con el aumento de los costos de esa actividad. Si bien puede ser cierto que la mayoría de los delitos en los que participan los equipos y las redes son convencionales y potencialmente cubiertos por convenios internacionales, no se trata de los delitos contra las que se necesita un nuevo tratado. Los acuerdos internacionales existentes no ofrecen ayuda para hacer frente a los delitos relacionados directamente con la infraestructura de la información, incluidos los ataques de virus que utilizan (como "Melissa" y "Te Amo"), negaciones de servicio, y otras conductas destructivas. Por otra parte, la necesidad de un acuerdo internacional para hacer frente a la delincuencia cibernética se basa no sólo en el hecho de que tales actos incluyen nuevos tipos de conducta, sino también en la necesidad de nuevos métodos con los que los delitos cibernéticos tendrán que ser investigados y procesados ​​para proporcionar una protección efectiva . Para lograr un acuerdo multilateral sobre la formulación precisa de los delitos cibernéticos que, de hecho, ser complicado, pero ese esfuerzo no tiene que llevarse a cabo. Existe un amplio consenso con respecto a una determinada conducta que implica la infraestructura de la información que debe ponerse a criminales, y un tratado fácilmente podría redactarse que describe esa conducta y requiere que todos los Estados Partes a hacer tal conducta criminal a través de una fórmula que decidan utilizar.

Las diferencias que existen entre los Estados en relación con varias cuestiones clave en el desarrollo de un tratado deben tenerse en cuenta y podrán limitar y dar forma a los acuerdos que se encuentran actualmente factible. Pero las diferencias sobre asuntos tales como la regulación del contenido, el alcance extraterritorial de la investigación, las normas de la prueba, y la protección de la privacidad y otros derechos, se pueden resolver, en gran medida a través de una voluntad de iniciar este esfuerzo, centrándose en medidas que puedan llegar a un acuerdo universal. Las grandes diferencias que existen entre los Estados con respecto a lo que se puede hacer unilateralmente demuestran, de hecho, la necesidad de tratar de obtener acordados, acuerdos multilaterales, en lugar de establecer una base para hacer ningún esfuerzo para hacerlo.

La noción de que Estados Unidos debe actuar unilateralmente cuando sea necesario para proteger sus intereses es el sonido principio. Profesor Goldsmith parece reconocer, sin embargo, que las actividades unilaterales deben ser jurídicamente defendible, y recurrir a ellos deben estar en los mejores intereses de la nación. Su suposición de que se necesitarán muchos años para negociar y aplicar una convención multilateral puede llegar a estar mal, a la luz de la necesidad cada vez más evidente y cada vez mayor impulso a ese acuerdo. Además, incluso antes de que un tratado multilateral se ha completado, los Estados Unidos pueden ser capaces de llegar a acuerdos menos integrales con otros Estados para mejorar la protección legal. La conducta unilateral que ofende a otros Estados, y los lleva a rechazar o retrasar la negociación de un tratado conveniente, perjudique los intereses de Estados Unidos.

Las preocupaciones expresadas por el sector privado sobre el establecimiento de normas y obligaciones jurídicamente obligatorias proceden del temor de que las consideraciones de orden público afectarán negativamente (y en gran medida la carga), las empresas de Internet y la libertad de expresión. El control gubernamental de la infraestructura de información bien podría tener efectos perjudiciales, y la regulación internacional podría ser especialmente perjudicial si se permite que los objetivos políticos y los requisitos burocráticos para interferir con el régimen actual de Internet, dominada privada. Los gobiernos nacionales - incluyendo el gobierno de los EE.UU. - han buscado o impuesto restricciones potencialmente perjudiciales para los usuarios de Internet, incluidas las limitaciones sobre el uso y la venta de encriptación avanzada, exige el poder de perturbar, oír, y el tráfico de Internet registrar y sugerencias que las entidades privadas asumir responsabilidades cuasi-fiscales en las investigaciones criminales. Estas políticas y sugerencias han, sin embargo, injustificadamente evocado sospecha de todos los esfuerzos para establecer obligaciones jurídicamente obligatorios. Si, como creemos, los esfuerzos voluntarios no proporcionar la seguridad adecuada, las obligaciones jurídicas de cooperar pueden concebir que sean coherentes con la continua creatividad y control privados. Un régimen internacional puede ser formado para satisfacer toda la gama de necesidades de seguridad cibernética, de manera que garantice el control continuado del sector privado de la tecnología y las prácticas de Internet. Los Estados Unidos son parte en diversos regímenes internacionales que abarcan la creación de medidas basadas en el consenso, no obligatorias elaboradas por los expertos del sector público y privado, en la que un tratado de seguridad cibernética podría dibujar en el suministro de un sistema integral y permanente para la cooperación internacional.

El caso fuerte para un carácter obligatorio, el régimen internacional ha dado lugar a varios acontecimientos importantes. Se están proponiendo disposiciones del Tratado para cerrar lagunas en los compromisos multilaterales existentes en el ámbito específico de la aviación civil. Este enfoque puede ser factible en otras áreas, sobre todo para proteger las infraestructuras críticas contra ataques criminales y terroristas, y parece poco probable que cause controversia.

El Consejo de Europa (COE) ha adoptado un enfoque más integral, publicando recientemente un proyecto de tratado sobre la delincuencia cibernética. Esta propuesta incluye las definiciones de actividades cibernéticas que se deben realizar penal de todos los Estados Partes, así como otras características y formas de cooperación. El proyecto del COE asume, con razón, que existe un consenso sustancial con respecto a las actividades cibernéticas que deben ser considerados criminales, y que los beneficios sustanciales se pueden derivar de un acuerdo multilateral de las normas comunes, la cooperación de investigación y extradición.

Nos comprometemos en esta monografía para demostrar las ventajas y la viabilidad de un régimen aún más exhaustivo, y propone un proyecto de convención internacional (el Proyecto de Stanford) y discutir sus elementos principales. El Proyecto de Stanford coincide en gran medida con el proyecto de Convenio del Consejo de Europa sobre la Delincuencia Cibernética, pero difiere en algunos aspectos.Lo más significativo es el Proyecto de Stanford establecería un organismo internacional, basado en los lineamientos de éxito, agencias especializadas de las Naciones Unidas, para preparar y promulgar - sobre la base del asesoramiento de expertos no políticos - las normas y métodos recomendados (SARPS) para mejorar la eficacia de las medidas de protección y de investigación.

1. Cubierta Conducta . La base de restos de cooperación internacional, fundamentalmente, en la combinación de una necesidad demostrable de acuerdo internacional para combatir la conducta cyber perjudiciales, y la existencia de un consenso internacional sobre qué conducta debe ser considerada criminal. Una revisión de la ley estatutaria vigente y los acuerdos internacionales propuestos refleja un consenso generalizado sobre enjuiciamiento criminal como la conducta cubierta en el Stanford Proyecto: ataques dirigidos a interferir o dañar las operaciones de computadora, las intrusiones intencionales y no autorizados; interferencia con las medidas de seguridad informática, la alteración maliciosa de contenido; intencional y materialmente facilitar la comisión de conductas prohibidas, utilizando un sistema cibernético para cometer violaciónes de cualquiera de las varias convenciones antiterroristas ampliamente adoptadas, y el uso de un sistema cibernético para atacar las infraestructuras críticas. La mayoría de estas formas de conducta están cubiertos en el proyecto la propuesta del Consejo de Europa, a pesar de que el proyecto trata de clasificar los delitos cibernéticos en un número de categorías específicas: acceso ilegal; intercepción ilegal, la interferencia de datos, la interferencia del sistema, y la posesión o la transferencia de "dispositivos ilegales "en circunstancias específicas. El esfuerzo COE generalizar puede haber creado la cobertura en algunas cuestiones que es indeseable amplio. El texto introductorio del artículo 3 del Proyecto - específicamente el concepto de "autoridad legalmente reconocida" - tiene la intención de incorporar el concepto de auto-defensa. Los esfuerzos de los gobiernos, empresas e individuos para defenderse de los ataques a veces pueden requerir medidas que, si se adopta sin autorización o justificación, sería criminal, tales como alteraciones de código, o interferir con el funcionamiento de los ordenadores utilizados por los atacantes. A veces, estos esfuerzos pueden afectar a terceros inocentes, pero sin embargo, puede ser razonable. Los complejos problemas que están determinados a surgir en la aplicación de los principios establecidos del derecho a esta nueva área de actividad tecnológica se resolverán con el tiempo, sobre la base de la experiencia.

El Proyecto de Stanford reconoce y trata de lidiar con el hecho de que los Estados tienen normas diferentes en los estatutos que cubren la conducta que prohíbe. En lugar de tratar de enumerar específicos, definidos en común "delitos", como en la mayoría de los tratados de extradición, el Stanford Proyecto se refiere a los tipos de conducta y compromisos protege de todos los Estados Parte para hacer cumplir cualquier ley contra toda forma de conducta cubierto, o de adoptar nuevas leyes necesarias para crear autoridad para enjuiciar o extraditar a dicha conducta. Este enfoque supera el problema de tratar de desarrollar objetivos precisos, acordaron definiciones de los delitos, y por lo tanto el requisito de que todos los Estados Partes que adopten formulaciones particulares como delitos nacionales.

Además de exigir la ejecución penal en contra de la conducta dirigida específicamente a la infraestructura de la información, el Proyecto de Stanford requiere acción criminal en contra del uso de las computadoras en la comisión de delitos en virtud de ciertos tratados multilaterales, ampliamente adoptados. Éstos incluyen crímenes claramente definidas contra aeronaves, buques, los diplomáticos y los atentados terroristas. Las computadoras pueden mejorar en gran medida el daño potencial causado por los delitos, y pueden hacerlas especialmente difíciles de investigar. Por lo tanto, dado que la mayoría de los Estados son partes en estos tratados multilaterales, deben estar dispuestos a imponer penas más estrictas para el uso de las capacidades cibernéticas en la comisión de los delitos específicos. (El COE Proyecto actualmente no incluye esas disposiciones.) Otras formas, ampliamente reconocidos de conducta criminal también pueden ser más agravados por el uso de las computadoras, tales como falsificación, fraude, robo, y la conversión. Estos crímenes no están incluidos en el Proyecto de Stanford, sin embargo, ya que son, en general, ya comprendidos en los tratados de extradición, a los Estados Partes desean medida dicha cobertura. La dimensión cibernética de tales actividades, por otra parte, por lo general implicaría conductas contempladas en el Proyecto de Stanford, con independencia de los crímenes de esa conducta haya facilitado. (El Proyecto COE incluye la cobertura de la falsificación "informáticos" y el fraude, pero sus definiciones de estos delitos parece probable que cause incertidumbre.)

Otros tipos de conducta, cuando se refieren a la infraestructura de la información, se han prohibido en algunos Estados, incluyendo violaciónes de derechos de autor, y la explotación sexual de menores.Estos delitos están cubiertos por el Proyecto de COE, junto con el uso de ordenadores para cometer fraude. Este tipo de conducta no están cubiertos en el Proyecto de Stanford, ya que su inclusión puede ser controvertido. De hecho, el consenso suficiente para la inclusión de algunos de estos delitos - puede existir - en especial el uso de las computadoras con fines de explotación sexual de menores, la cobertura del Proyecto de Stanford podría ampliarse para incluir tales delitos. (El COE Proyecto incluye los delitos relacionados con la pornografía infantil, así como "autor y derechos conexos delitos", pero si el alcance de la cobertura debe ser colindantes con los tratados de la zona - como el Convenio de Berna y otros tratados de derechos de autor administrado por la Organización Mundial de la Organización de la Propiedad - se ha dejado sin resolver).

El Proyecto de Stanford también incluye una cobertura muy limitada de delitos "contenido", para evitar las grandes diferencias que existen entre los Estados en materia de restricciones a la libertad de expresión y la actividad política. Ningún tipo de expresión, o de la publicación, se requiere ser tratado como criminal bajo el Proyecto de Stanford, y si, por ejemplo, Alemania decidiera prohibir la publicación en Internet de *Mein Kampf* , tendría que hacerlo de forma unilateral y no podía esperar para recibir asistencia en la aplicación en el marco del Proyecto de Stanford. La única excepción a este principio en el Proyecto de Stanford es la cobertura limitada de conducta descrita como la "distribución de dispositivos o programas destinados a la finalidad de cometer" otro tipo de conducta criminal hecha por el Proyecto de Stanford. El Proyecto de ello hace criminal el esfuerzo consciente y deliberado para causar ataques ilegales a través de dicha distribución, pero no en las discusiones sobre la vulnerabilidad informática diseñada para evaluar la exposición a ataques a través de Internet u otra expresión protegida. Los Estados Partes que deseen fomentar la discusión abierta de los ataques informáticos y vulnerabilidades podrían designar sitios "puerto seguro" en el que la discusión sería considerado legal. (El Proyecto COE prohibiría a una amplia gama de conducta que implique la transferencia o posesión de "dispositivos ilegales", definidas para incluir ciertos programas de computadora.)

Una última cuestión sobre delitos es si una convención de la ciberdelincuencia debe abarcar únicamente los delitos que prevén penas que excedan cierta pena mínima de prisión. Los tratados de extradición generalmente contienen esa limitación, por lo general que el delito por el cual se pide la extradición sea punible con un año de prisión o más. Esta norma tiene por objeto excluir delitos menores de la cobertura. Dadas las complicaciones y el esfuerzo requeridos para satisfacer las solicitudes de extradición, esta consideración es al menos tan importante en una convención de la ciberdelincuencia como en cualquier otro. Al contar con este requisito, por otra parte, estaría en realidad exige a los Estados Partes para cubrir las conductas prohibidas con posibles penas de al menos un año en la cárcel. Por tanto, el Proyecto de Stanford incluye sólo delitos por los que se proporciona una posible pena de prisión de al menos un año. (El COE Proyecto incluye un artículo específico sobre este tema, el cual está diseñado para asegurar graves sanciones penales y civiles.)

2. Jurisdicción . El Proyecto de Stanford anticipa que la conducta abarca tendrá efectos potencialmente conferir jurisdicción en varios Estados Partes por el mismo delito. Proporciona un conjunto de prioridades que las Partes acuerden seguir en la realización de sus funciones y la consecución de sus derechos, en la medida de lo posible, dada la dificultad de prever todas las contingencias posibles. El Estado Parte debe establecer jurisdicción para juzgar a los delincuentes que cometen delitos en su territorio, que sean nacionales, o que son residentes apátridas en su territorio y cuya extradición desde su territorio se negó. Todo Estado Parte podrá establecer su jurisdicción para tratar de delincuentes que tratan de dañarlo o sus nacionales, o para obligarla a realizar o abstenerse de realizar un acto, o cuyo delito tenga efectos importantes en su territorio. (El Proyecto COE proporciona una cobertura similar, pero no resuelve los aspectos de este problema de una manera definitiva.)

El problema de la jurisdicción de varios Estados sobre la delincuencia es por ahora un lugar común en el derecho internacional. Fraude transnacional, por ejemplo, ha llevado a las decisiones de los tribunales nacionales asumiendo competencia sobre la base de cualquier relación significativa con la conducta en cuestión. Entre ellos están los Estados en los que se planeó un fraude, donde se inició un esfuerzo para defraudar, donde los individuos trabajaban en la aplicación del fraude, en oa través del cual se hicieron las comunicaciones que son intrínsecos al fraude, donde se encontraban las víctimas, y en el que fraude tuvo efectos materiales que se destina. El reconocimiento generalizado del fraude como la actividad criminal lleva Unidos facilidad para encontrar jurisdicción sobre dicha actividad, a pesar de la importante relación particular, los fraudes pueden tener a otros Estados. Ellos tienden a asumir que el fraude castigo será apoyado por otros Estados afectados, en vez de oposición como una violación de su soberanía.

La ciberdelincuencia es esencialmente transnacional, ya menudo implican afirmaciones jurisdiccionales de varios Estados. Para evitar el conflicto de esas afirmaciones de jurisdicción podría causar la ejecución en virtud del Proyecto de Stanford se limita a las actividades cibernéticas que son universalmente condenadas. El Proyecto de Stanford no accede a la jurisdicción de un Estado simplemente porque alguien dentro de su territorio es capaz de acceder a un sitio web en otro Estado, para atribuir la competencia, alguien en el control de la página web debe causar deliberadamente uno de los delitos previstos, con efectos en el Estado tratar de hacer valer su jurisdicción. Parece probable, por tanto, que los Estados, en general, aceptar todas las demandas jurisdiccionales razonablemente basadas aprobados en el Proyecto.

3. Cooperación en Ejecución Penal . El Proyecto de Stanford incluye compromisos de los Estados Partes a participar en toda la gama de actividades de cooperación que se encuentran en los acuerdos internacionales ampliamente adoptados. Debajo de ella, los Estados Partes están de acuerdo de extraditar o juzgar a presuntos razonablemente haber participado en alguna forma de la conducta o delitos cubiertos. Cuando sea necesario y en una base probatoria adecuada, podrían arrestar y detener a los presuntos delincuentes durante un corto período de espera de una solicitud de extradición. También estarían de acuerdo en cooperar en aprovechar, conservar, desarrollar y proporcionar pruebas en forma utilizable para el enjuiciamiento de los delincuentes en los tribunales de los demás Estados Partes.Ellos coordinarán estas actividades a través de las Autoridades Centrales designadas "," como en los Tratados de Asistencia Legal Mutua, por lo que cada Estado Parte sabría a quién dirigir peticiones y tendrían una agencia o persona identificada encargada de resolver estas solicitudes de manera oportuna y manera apropiada.

El Proyecto de COE es particularmente impresionante para obligar la respuesta rápida a los ataques cibernéticos y demandas de cooperación, sobre la base 24-hour/7-day-per-week y el Stanford Proyecto incorpora un compromiso similar. El Proyecto de COE también normas detalladas relativas a la incautación de datos, órdenes de fabricación, presentación acelerada, y la revelación. A disposición (artículo 28) en relación con "la interceptación" se contempla, pero en discusión. Estas reglas son actualmente útiles, pero pueden llegar a ser problemática con la disponibilidad de nuevas tecnologías o métodos.El Proyecto de Stanford, por esta razón, ofrece un compromiso de cooperación en cada uno de esos temas que no se abordan con detalle.

Los principios básicos de la cooperación son claras. Cuando se trata de la aplicación, sin embargo, existen muchos problemas, y muchos más están seguros de que surjan, para los que no han sido aún desarrollado respuestas. ¿Cuál es, por ejemplo, debería ser el alcance del poder de un Estado de forma unilateral para buscar información en un Estado extranjero? Un Estado no puede saber si su esfuerzo de electrónica para obtener información acerca de un crimen a entrar y tener un efecto significativo en otro Estado o Estados, no podía evitar esa incertidumbre, aún si no lo intentó. Algunos de tolerancia de los efectos extraterritoriales que parece, por lo tanto, ser imprescindible en todo viable, acuerdo multilateral cyber-relacionado. Tanto el Proyecto de Stanford y el Proyecto de convocatoria del Consejo de Europa para la cooperación más amplia posible, la prestación del primero de una acción unilateral es más estrictamente definidas en algunos aspectos, pero este último todavía no está acordado por los miembros del COE.

Otra área de incertidumbre actual es lo que los derechos de un proveedor de servicios de Internet (ISP) debe tener para preservar y proporcionar información de los delitos cibernéticos. En caso de tal derecho sea exigible por la ley, por otra parte, y si es así por qué medios? Estos son temas delicados, ya que los Estados no han establecido derechos de los ISP y otros participantes de Internet, como las impuestas en contextos similares. ¿Qué deben los Estados deben hacer para mejorar las perspectivas de conservar las pruebas que podrían ser útiles en la investigación de un ataque, en particular, se debe exigir a un Estado a confiscar esa información?

Este tipo de cuestiones relacionadas con la investigación transnacional del delito cibernético y el terrorismo plantean varias cuestiones. La primera tecnología inquietudes: ¿qué es posible y / o deseable para ayudar a los Estados Partes en la obtención de la cooperación que va más allá de las medidas convencionales actualmente asumidas en los tratados de extradición y asistencia judicial recíproca medidas tecnológicas? La rápida evolución de las capacidades tecnológicas y de hacerla inútil para tratar de acabar definitivamente en un proyecto de convenio con este aspecto de la delincuencia cibernética y el problema de terrorismo. En cambio, el proyecto propone principios generales de apoyo a ciertos objetivos tecnológicos existentes y establecería un organismo internacional a través del cual los Estados Partes cooperarán en la consideración y proponer el uso de determinadas medidas tecnológicas para mejorar los esfuerzos de cooperación.

Además de la dimensión tecnológica son algunas cuestiones de principio relativas al derecho de los Estados Partes para defenderse o para investigar delitos cibernéticos. ¿Puede un Estado Parte, por ejemplo, iniciar deliberadamente acciones de investigación o las contramedidas correspondientes del orden público que podrían suponer el envío de transmisiones en los sistemas informáticos situados en otros territorios soberanos? Basándose en la experiencia hasta la fecha, de rápida propagación virus informáticos y otros ataques cibernéticos exigen actuar con diligencia para localizar a los atacantes, y es difícil, si no imposible conocer de antemano todos los lugares a través de la cual o de cualquier parte de cualquier transmisión cibernética podría viajar. Por lo tanto, el Proyecto de Stanford aprueba en principio las medidas unilaterales en los que son electrónicos y razonable. El Proyecto de Stanford ofrece, además, que cualquier actividad de aplicación de la ley que afecta a sabiendas a cabo otro Estado Parte, incluyendo cualquier intento de buscar medidas de cooperación de una entidad situada en otro Estado Parte, debe darse a conocer a la Autoridad Central de ese Estado lo antes factible. Además, el Proyecto de Stanford exigiría a todas las entidades, incluidos los ISP, para cumplir con alguna norma o procedimiento desarrollado por el AIIP bajo el Proyecto de Stanford y aceptado por el Estado Parte en el que se encuentren, y que obligar a todos los Estados Partes apliquen los estas normas y procedimientos. Disposiciones sobre la base de estos principios parece probable que obtener el apoyo generalizado y serían preferibles a las acciones unilaterales que algunos Estados podrían considerar objetable (o incluso penal).

El Proyecto de Stanford incluye una disposición que autoriza la incautación y el decomiso de los equipos utilizados en la comisión de delitos, sin perjuicio de las garantías procesales. Unidos podría utilizar la información contenida en dicho equipo, o disponer de los equipos si lo consideran conveniente, de conformidad con la legislación nacional. Los fondos provenientes de decomisos han proporcionado recursos en otras áreas para su uso en la mejora de las capacidades de las fuerzas del orden. La incautación y / o decomiso de equipos cyber utilizado en la comisión de delitos cubiertos es compatible con el derecho universalmente reconocido a los gobiernos a aprovechar los instrumentos del delito.

4. Estructura de Cooperación Tecnológica . Una respuesta eficaz a la delincuencia transnacional cyber requiere un alto nivel de cooperación tecnológica con respecto a prácticamente todas las funciones que se espera que realizan los Estados Partes. Los ciberdelincuentes explotan las posibilidades tecnológicas disponibles, incluyendo la capacidad de ocultar su identidad, para ocultar el origen de los ataques y otras acciones mediante la realización a través de los sitios intermedios, y para encontrar y explotar las debilidades en toda la infraestructura de la información en todo el mundo. Los retos de tratar con estas capacidades se ven agravados, además, por los cambios dinámicos en la tecnología, el continuo desarrollo de nuevos métodos para la comisión de delitos cibernéticos, la corriente generalizada intercambio de información e ideas acerca de las vulnerabilidades de sistemas informáticos, y una cultura entre los usuarios del ciberespacio que es escéptico, cuando no abiertamente hostiles a la participación del gobierno.

En este contexto, es poco realista esperar que el crimen cibernético se controlará de manera significativa o disuadido a través de medidas unilaterales o voluntaria o puramente defensiva. Medidas defensivas siempre tienen sentido, y resultarán eficaces para algunas entidades, algunas de las veces. Pero la presión de operar abiertamente en los negocios, la educación, la investigación, el entretenimiento y las actividades personales lleva a los usuarios a desarrollar o elegir accesible (y por lo tanto más vulnerables) tecnología. Los gobiernos han parecido especialmente incapaces de defender sus sitios y sistemas, y han sido blanco frecuente de ataques. Por otra parte, los objetivos que se persiguen a través de la cooperación, y simplemente no está disponible para los Estados que actúan de forma unilateral, requiere un alto nivel de coordinación tecnológica. Tomemos, por ejemplo, la necesidad de anticipar, congelar, y rastrear los paquetes de información que se utilizan en el crimen cibernético. Estas medidas, una vez elaborados, deberán ser aprobadas y aplicadas por todos los participantes en la infraestructura de la información, de una manera compatible con la tecnología o criminales encontrar y utilizar las brechas en la cobertura. Del mismo modo, para que los Estados lleven a cabo inspecciones e incautaciones, de proveer para la extradición, y el desarrollo de pruebas de que se puede utilizar en los tribunales de todos los Estados a cooperar, se requerirá la adopción de normas uniformes y mutuamente aceptables y soluciones tecnológicas, en la que todos los Estados puedan confiar .

Las presiones para encontrar soluciones multilaterales a los problemas de infraestructura de la información son, de hecho, probablemente sea tan grande que las soluciones se desarrollarán sin los procesos formales, abiertas y responsables asociados a las instituciones internacionales establecidas. La historia de cómo los actores públicos y privados desarrollan y aseguran el apoyo del gobierno de EE.UU. para un sistema de protección del dominio ilustra tanto la necesidad y la inevitabilidad de soluciones multilaterales a por lo menos algunos de los temas clave, así como el proceso ad hoc y relativamente no democrático que puede ocurrir en ausencia de establecidas, mecanismos públicamente.

El proceso por el cual las normas y prácticas efectivas se establecen para la cooperación internacional en la lucha contra el delito cibernético y el terrorismo será probablemente el aspecto más importante de cualquier acuerdo multilateral. Orientación considerable puede ser adquirida en el diseño de una estructura de fijación de dichos niveles de otras áreas en las que tienen lugar las actividades normativas transnacionales, como la seguridad aérea, la seguridad marítima, las telecomunicaciones y la banca. En general, el establecimiento de normas y la cooperación en estas áreas se logra mediante la creación de un organismo internacional asignado objetivos claramente articulados y ampliamente compartida, con los recursos técnicos y materiales para lograr esos objetivos, el equipo de profesionales y no políticos, la dependencia sustancial en el sector privado (sobre todo en los técnicos especialistas altamente cualificados), y la participación política continua y el control final de los representantes de los Estados participantes.

La historia y la estructura de la Organización de Aviación Civil Internacional (OACI) son instructivas a este respecto. OACI se rige por una Asamblea, integrada por representantes de todos los Estados Partes (185), que se reúne al menos una vez cada tres años, establece las políticas básicas en consonancia con los tratados que rigen, considera y recomienda revisiones del Tratado, aprueba el presupuesto, que financia a través de un reparto entre los Estados miembros, y elige a los delegados en el Consejo por períodos de tres años. Actualmente el Consejo tiene 33 miembros, incluyendo representantes de los Estados de mayor importancia en el transporte aéreo, de los Estados que conforman las mayores contribuciones a la aviación internacional, o elegidos para asegurar la representación de todas las áreas geográficas. El Consejo aplica las decisiones de la Asamblea, se prepara el presupuesto, administra las finanzas de la OACI, nombra al Secretario General y establece una Secretaría, y está facultado para adoptar las normas y métodos recomendados (SARPS), que se incorporan en el Convenio de la OACI a través de los anexos. El Consejo se pronunciará por mayoría de votos en el desempeño de sus funciones, en particular en la adopción de SARPS, que sólo se adopten después de un desarrollo exhaustivo y "seguimiento técnico, evaluación y apoyo." Si bien puede delegar la autoridad con respecto a cualquier asunto en particular a un comité de sus miembros, las decisiones de cada comisión pueden ser apeladas ante el Consejo por cualquier Estado contratante interesado.

Los temas tratados en los SARPS reflejan la autoridad del Consejo para adoptar las medidas necesarias para mantener la seguridad y eficiencia del transporte aéreo internacional. En el desempeño de estas funciones, el Consejo cuenta con la asistencia de la Comisión de Navegación Aérea, un cuerpo de quince personas con "cualificación y experiencia adecuadas", nombrados por el Consejo entre los candidatos de los Estados miembros. Este órgano de expertos se encarga de estudiar y recomendar SARPS nuevos o enmendados, estableciendo subgrupos técnicos y garantizar que el Consejo reúne y difunde a todos los Estados miembros la información necesaria y útil para el progreso de la navegación aérea.

La asistencia técnica es un aspecto importante de la labor de la OACI. Estados miembros de los pilotos de licencia, de conformidad con las normas de la OACI. Normalización de los equipos y procedimientos es un objetivo y la actividad principal, en toda la gama de cuestiones técnicas, como la navegación, la meteorología, los gráficos, la medición, la operación de aeronaves, servicios de tránsito aéreo, búsqueda y rescate, investigación de accidentes y la seguridad. Los países en desarrollo cuentan con la asistencia activa a través de una variedad de programas, financiados por la OACI, el Programa de Desarrollo de las Naciones Unidas (PNUD) y otras fuentes. Unos 80 miembros del personal están implicados en cerca de 120 proyectos de asistencia cada año, con un presupuesto total de $ 55 millones. Ofrecen capacitación, asesoramiento técnico y ayuda en la compra de equipo necesario.

Un segundo organismo internacional que realiza funciones análogas a las que se refieren a la seguridad cibernética es la Unión Internacional de Telecomunicaciones (UIT). La UIT es la organización intergubernamental más antigua de la existencia, de haber sido formado en 1865 para aplicar el Convenio Telegraph. Se expandió sus actividades a la radio en 1906, y actualmente se ocupa de las cuestiones relacionadas con todas las formas de "telecomunicaciones", incluyendo el teléfono, la televisión, y el télex. Opera a lo largo de las mismas líneas que la OACI, con una fuerte dependencia de conocimientos y la participación del sector privado. En declaraciones recientes, la UIT ha expresado su intención de involucrarse más con los problemas de infraestructura de la información.

El acuerdo de los regímenes de la OACI y la UIT se basa cuestiones tecnológicas que se diferencian unos de otros, y de las comunicaciones por Internet, de manera significativa. Pero las necesidades que llevaron a la creación de éstos, y de otros mecanismos de regulación, de manera similar, son en gran parte similar a las que afectan al mundo cibernético. Los principales factores subyacentes a la creación de estos organismos multilaterales han sido la seguridad y la eficiencia - las mismas consideraciones apoyo a una solución multilateral al problema del delito cibernético y el terrorismo. Además, estas entidades multilaterales están diseñadas para: (1) permitir a todos los Estados Partes para aprender de y se involucren en las soluciones multilaterales de los problemas relacionados con las tecnologías transnacionales; (2) permiten a los Estados tecnológicamente avanzados para proteger sus intereses, (3) asegurar que las soluciones se basan en el mejor conocimiento científico posible, desarrollado con la aportación de expertos, y (4) se benefician de la participación y la experiencia de los intereses privados (tanto comerciales como sin fines de lucro).

El Proyecto de Stanford aprovecha la OACI y los patrones de la UIT en la creación de una institución internacional propuesta, denominada "Agencia para la Protección de la Infraestructura de la Información" o "AIIP," para poner en práctica los objetivos de los Estados Partes con respecto a la protección de la infraestructura de información de las actividades de ciber criminales y terroristas . No solo conjunto de soluciones técnicas resolverán los problemas que existen en la actualidad, por no hablar de los que se desarrollarán como las posibilidades tecnológicas se expanden. Por tanto, el AIIP está diseñado para desempeñar un papel permanente en la formulación y revisión de las normas, y la propuesta de revisión del tratado para mejorar la seguridad, la eficiencia y la cooperación efectiva a la luz de continuar los avances tecnológicos y políticos. Correctamente diseñado y estructurado, este tipo de agencia debe contribuir sustancialmente a la seguridad cibernética.

El Proyecto de Stanford requeriría Estados Partes para establecer la AIIP, con las siguientes, componentes clave: un conjunto que tiene funciones similares a las ejercidas por los órganos plenarios que operan en la OACI, la UIT y otros organismos especializados; un Consejo que implementa la las políticas establecidas por la Asamblea, a través de comités de expertos, con representación del sector privado fuerte y un Secretario General y la Secretaría para poner en práctica las instrucciones de la Asamblea y el Consejo y realizar tareas administrativas. El Consejo formulará y la Asamblea adoptaría las normas y prácticas (SARP) recomendadas para avanzar en los objetivos del Proyecto de Stanford y el AIIP también proponer enmiendas y acuerdos internacionales adicionales para la aplicación de soluciones a los problemas que requieren una nueva autoridad de los Estados. Algunos de los organismos especializados de las Naciones Unidas tienen un historial impresionante de desarrollar y proponer los acuerdos internacionales para hacer frente a importantes áreas no cubiertas por sus instrumentos constitutivos. La Organización Marítima Internacional (OMI), por ejemplo, ha propuesto más de veinte tratados para tratar asuntos importantes de la seguridad o la eficiencia marítimo, la mayoría de los cuales han sido ampliamente ratificados. Además, el Consejo AIIP estaría autorizado a crear y poner en práctica, con el apoyo de la Asamblea, los programas de asistencia para ayudar a necesitados Estados Partes participen eficazmente en las actividades contempladas en el Proyecto de Stanford.

Las normas y recomendaciones para ser desarrollados por la AIIP serían diseñadas para tener el mismo valor jurídico atribuye a los SARPS desarrollados por la OACI. SARPS adoptados por la OACI no son jurídicamente vinculantes, se convierten en parte de anexos al Convenio de la OACI, y se espera que los Estados Partes para su aplicación. Los Estados Partes, sin embargo, que los demás Estados Partes de la falta de aplicación de los SARPS y éste sería libre de actuar para protegerse de las posibles consecuencias de la falta de un Estado de cumplir con la norma o práctica en cuestión. Este tipo de arreglo ha demostrado ser universalmente aceptable en la aviación civil y en otras áreas de la regulación transnacional, para garantizar que las normas y prácticas propuestas son examinadas a fondo, ampliamente apoyadas, y aceptadas voluntariamente sobre la base del interés propio soberano y la reciprocidad de la obligación.

La autoridad se establece en el artículo 12 de la AIIP en el Proyecto de Stanford para que pueda disciplinar a los Estados Partes o Estados que no son Partes pero que están participando en la infraestructura de la información. Cuando un Estado actúa o permite a las personas a actuar de una manera que socava los objetivos del proyecto, el Consejo está facultado para recomendar sanciones, y la Asamblea está facultada para imponerlas a una mayoría de dos tercios, hasta e incluyendo la expulsión de la AIIP, y una recomendación a los Estados de la exclusión de la infraestructura de la información. Mientras que el Proyecto evita la conducta del Estado regulador, las acciones que atentan contra sus propósitos, como permitir que las personas que utilizan el territorio de un Estado para lanzar ataques que afectan a otros Estados, permitiría la AIIP de excluir esos Estados miembros o para recomendar personas que castigan y / o no Estados Parte mediante la exclusión de la participación en la infraestructura de información internacional.

5. Protección de los Derechos Individuales . Regulación transnacional de Internet plantea varias cuestiones importantes relacionadas con la privacidad y otros derechos individuales. El Proyecto de Stanford asegura que, como mínimo, los derechos individuales ofrecidas por los Estados Partes no están afectados. Ningún Estado Parte tiene ninguna obligación bajo el Proyecto de Stanford para actuar en cualquier forma que pueda violar la privacidad u otros derechos de cualquier persona o entidad, según lo definido por la ley de ese Estado. Además, el Proyecto de Stanford autoriza a los Estados Partes a denegar o cesar la cooperación en las investigaciones o enjuiciamientos que consideran políticamente motivado o desleal. También crearía un subcomité de expertos en el marco del AIIP, asignó la tarea de seguimiento y presentación de informes sobre la protección de la privacidad y los derechos humanos. Por último, el proyecto establece que determinadas protecciones fundamentales deben hacerse extensivas a las personas detenidas por violaciónes de cualquiera de los delitos comprendidos en sus disposiciones, incluyendo notificación al representante del Estado del que el acusado es nacional, y el derecho a la asistencia de dicho representante.

Los esfuerzos para proteger la privacidad y otros derechos humanos implicará complicaciones para los Estados Partes, a las entidades privadas, y para el AIIP como organización. Las nociones de privacidad y el alcance de los derechos procesales y humanos varían considerablemente entre los Estados cuya participación es necesaria para un régimen internacional viable. Estas diferencias han llevado a la Alianza Internet para concluir que un régimen jurídicamente obligatorio sobre la delincuencia en Internet probablemente "causar estragos" en la protección de la privacidad. De hecho, no hay tal resultado es necesario contar con la cooperación multilateral eficaz. Al permitir a los Estados Partes a insistir en la preservación de las normas nacionales en un nivel mínimo de protección, el Stanford Proyecto impediría su uso para privar a una persona de los derechos concedidos por un Estado Parte, y los problemas que se prevén serán análogos a los creados en el marco del transporte aéreo y otras convenciones antiterroristas. Al igual que los Estados Unidos y la URSS eran capaces de vivir con tales diferencias en los contextos, y seguir beneficiándose de los acuerdos (por ejemplo, al asegurar la extradición y enjuiciamiento de los secuestradores), el Proyecto de Stanford ha sido diseñado para permitir a los Estados con diferentes sistemas políticos radicalmente valores para trabajar juntos en la consecución de objetivos de beneficio mutuo sin sacrificar esos valores. Si, sin embargo, una situación grave y sin solución surgió en los que, por ejemplo, el régimen de la cooperación técnica y operativa desarrollada bajo el proyecto fue abusado por un Estado, de alguna manera, la Asamblea tiene la facultad de imponer sanciones en los artículos 12, 13 y 21, incluyendo la expulsión de la AIIP o una recomendación en contra de la participación del Estado infractor en la infraestructura de la información internacional.

6. Seguridad Nacional . El Proyecto de Stanford deja claro, de una manera similar a otros acuerdos multilaterales, que es aplicable a la conducta del Estado y de los asuntos de seguridad nacional. Un acuerdo multilateral sobre la delincuencia cibernética tendrá objetivos nuevos, complejo e importante, aparte de la posible utilización de los sistemas informáticos de los Estados como militar o herramientas de inteligencia. Los esfuerzos para controlar la conducta del Estado en relación con la seguridad nacional será poco útil para avanzar en el desarrollo de un enfoque multilateral al problema de la delincuencia cibernética, e innecesario también. OACI protege aeronaves civiles del ataque, y la UIT protege las transmisiones de radio de interferencia. Sin embargo, estos tratados no tratan directamente con el control de los Estados en la conducción de sus asuntos de seguridad nacional. Para el uso de la tecnología cibernética medida como arma es una preocupación, los acuerdos de control de armamentos existentes, y los tratados que incorporan las leyes de la guerra, son todas potencialmente aplicable, así como las disposiciones de la Carta de las Naciones Unidas sobre el uso de la fuerza.El proyecto proporciona sanciones contra la conducta que socava sus propósitos. Si otras medidas deben ser consideradas para limitar el uso de las tecnologías cibernéticas en las áreas de seguridad nacional, los que debían examinarse por separado y no se utiliza para mantener como rehenes a la elaboración de un régimen multilateral para avanzar en el proceso de hacer frente a las actividades delictivas perjudiciales para todos Unidos, sus pueblos y sus economías.

7. Resolución de Disputas . El Proyecto de Stanford se basa inicialmente en la resolución consensual de litigios mediante la negociación y la mediación. Los Estados Partes no pueden resolver sus diferencias por consenso están obligados a someterse al arbitraje en cualquier forma acordada. El Proyecto de Stanford contempla que el Consejo de la AIIP será, después de su creación, proponer a la consideración de la Asamblea un mecanismo de arbitraje a través del cual los conflictos se resolverían por paneles de expertos designados de antemano para conocer y resolver estas cuestiones, tal vez en forma relativamente informal preferido por la industria para la resolución de disputas sobre nombres de dominio de sitios web.

8. Modificaciones . El Stanford Proyecto contiene una disposición de un tratado estándar que permite a los Estados Partes a que propongan y aprueben modificaciones que sean necesarias y adecuadas.

**Convención Internacional**

**Para mejorar la protección de la Delincuencia Cibernética y Terrorismo**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Preámbulo*

Los Estados Partes en el presente Convenio,

Reconociendo que los avances en la ciencia y la tecnología han permitido a las comunicaciones transnacionales sin precedentes a través de las infraestructuras de información;

Afirmando los beneficios en todo el mundo habilitadas por las infraestructuras;

Comprender la creciente dependencia y la dependencia de las personas y los gobiernos sobre el correcto funcionamiento de las infraestructuras de información y su interdependencia cada vez mayor;

Reconociendo la vulnerabilidad de las infraestructuras de información a los ataques y la utilización indebida;

Teniendo en cuenta las posibles graves consecuencias de los ataques y la utilización indebida de las personas y los gobiernos de todo el mundo, incluidos los fallos de los sistemas y los daños a la infraestructura crítica, las pérdidas económicas y la interrupción de las comunicaciones;

Resolviendo que es necesario para proteger infraestructuras de información transnacionales de los ataques y la utilización indebida e impedir dicha conducta por medio de sanciones y tecnologías apropiadas;

Consciente de las limitaciones de los enfoques unilaterales;

Consciente también de la necesidad de garantizar una protección adecuada de la privacidad, la libertad de comunicación, y otros derechos humanos;

Deseando cooperación internacional activa a través de medidas voluntarias y obligatorias efectiva para investigar y enjuiciar a los criminales cibernéticos y terroristas y desarrollar normas y prácticas tecnológicas para mejorar la seguridad cibernética;

Deseando asimismo la creación de un organismo especializado, diseñado para reunir los conocimientos necesarios para alcanzar los objetivos voluntarios y obligatorios de la presente Convención, a través de una estructura basada en actividades voluntarias, del sector privado, la experiencia y la participación;

Convencidos de que existe un consenso sobre ciertas conductas que deben ser enjuiciados como criminales, así como sobre la necesidad de normas y prácticas para mejorar la seguridad acordadas y

Reconociendo la necesidad de garantizar que todos los Estados cooperantes deben tener las capacidades tecnológicas necesarias para participar y beneficiarse de los avances en la comunicación, y que toda la asistencia que sea posible debe ser proporcionada por los Estados tecnológicamente avanzados;

Han convenido en lo siguiente:

*Artículo 1*

*Definiciones y uso de términos*

A los efectos del presente Convenio:

1. "Ciberdelincuencia" significa conducta, con respecto a los sistemas cibernéticos, que se clasifica como un delito penado por el presente Convenio;

2. "Ciberterrorismo" significa uso intencional o amenaza de su uso, sin autoridad legalmente reconocida, de la violencia, la interrupción o interferencia contra los sistemas informáticos, cuando es probable que ese uso dé lugar a la muerte o lesiones de una persona o personas, daños sustanciales a la integridad física propiedad, desorden civil, o daños económicos significativos;

3. "Infraestructura de información" y "sistema cibernético" significa cualquier computadora o red de computadoras usado para transmitir, transmitir, coordinar y controlar las comunicaciones de datos o programas;

4. "Datos" es la información o el contenido de comunicaciones, incluyendo voz, texto, fotografías, sonido, video, señales de control y otros formatos de información o de comunicaciones;

5. un "programa" es una instrucción o conjunto de instrucciones destinadas o diseñado para causar un ordenador o red de ordenadores para manipular los datos, los datos de visualización, los datos de uso, realizar una tarea, realizar una función, o cualquier combinación de éstos;

6. "Infraestructuras de información transnacionales", las infraestructuras de información con los componentes físicamente presentes en el territorio de dos o más Estados Partes;

7. "Infraestructuras críticas" son las redes interconectadas de dispositivos físicos, los caminos, las personas y los ordenadores que proporcionan para la entrega oportuna de los servicios públicos, la atención médica, la protección de la población en general por la policía, bomberos, alimentos, agua, servicios de transporte, incluidos los viajes de personas y del transporte de mercancías por aire, agua, ferrocarril o carretera, suministro de energía, incluida la electricidad, el petróleo, los productos de petróleo y gas, servicios y transacciones financieras y bancarias, y servicios de información y comunicaciones;

8. una "persona" puede ser cualquiera de los siguientes: (a) un ser humano o (b) una empresa u organización empresarial reconocida como entidad jurídica propia en el derecho interno de gobierno de un Estado Parte, o (c) cualquier otra entidad legalmente reconocida capaz de realizar o contribuir a las conductas prohibidas por la presente Convención;

9. "Legalmente reconocida autoridad" es la autoridad de la jurisdicción interna de un Estado Parte que rigen a las personas para entrar en lugares privados, para examinar los papeles privados, para observar las comunicaciones privadas, o para participar en otras actividades de investigación legalmente autorizados;

10. "Legalmente reconocida permiso" o "consentimiento legalmente reconocida" es el permiso reconocido en el derecho interno de un Estado Parte de gobierno (cuando se administra por una persona con un interés jurídicamente reconocido en un lugar, la propiedad tangible o propiedad intangible) para entrar en lugares privados, para examinar documentos privados, para observar las comunicaciones privadas, o para participar en otras actividades de investigación legalmente autorizados;

11. "Misrouting" de contenido de las comunicaciones o de datos significa cambiar intencionadamente o la manipulación de la operación ordinaria de una infraestructura de información con el fin de retrasar o desviar la entrega de un paquete protegido en el camino a su destino, o con conocimiento de que dicho retraso o la desviación resultarán ;

12. un "paquete protegido" es un conjunto de datos que se utilizan para transmitir contenido de las comunicaciones a través de una infraestructura de información transnacional, conforme a una norma internacional para la transmisión de los datos establecidos por la Internet Engineering Task Force (IETF) u otro proceso ampliamente aceptada;

13. un "delito tratado" es una conducta prohibida por un tratado multilateral, convención o acuerdo (que no sea la presente Convención) para los que un individuo puede ser castigado bajo la ley nacional que rige la aplicación de las cláusulas de ese tratado, convención o acuerdo;

*Artículo 2*

*La promulgación de leyes internas*

Cada Estado Parte adoptará las medidas que sean necesarias para:

1. para tipificar como delitos penales en su derecho interno las conductas enunciadas en los artículos 3 y 4;

2. para que esa conducta con penas adecuadas que tengan en cuenta sus posibles graves consecuencias, incluyendo la posible pena de prisión de un año o más, y,

3. a tener en cuenta para la aplicación del sistema a través de leyes nacionales todas las normas y prácticas recomendadas propuestos por la Agencia de Protección de la Infraestructura de la Información (AIIP) de conformidad con el artículo 12.

*Artículo 3*

*Infracciones*

1. Delitos previstos en esta Convención se comprometen, si una persona se dedica ilícita e intencionadamente en cualquiera de las siguientes conductas sin legalmente reconocida autoridad, permiso o autorización:

(A) crea, almacena, altere, eliminaciones, transmite desvía, misroutes, manipula, o interfiera con los datos o programas en un sistema cibernético con el propósito de causar, oa sabiendas de que estas actividades provocarían, dicho sistema cibernético u otro sistema cibernético para dejar de funcionar como es debido, o para ejercer funciones o actividades no previstas por su propietario y se considera ilegal en virtud del presente Convenio;

(B) crea, almacena, altere, eliminaciones, transmite desvía, misroutes, manipula, o interfiera con los datos en un sistema cibernético de la finalidad y el efecto de proporcionar información falsa con el fin de causar daños considerables a personas o bienes;

(C) entra en un sistema cibernético para los que el acceso está restringido de manera bien visible y sin ambigüedades;

(D) interfiere con los mecanismos de autenticación de manipulación indebida o detección;

(E) fabrica, vende, los usos, los mensajes o no distribuye ningún dispositivo o programa previsto para el fin de cometer cualquier conducta prohibida por los artículos 3 y 4 de este Convenio;

(F) utiliza un sistema cibernético como un factor importante en la comisión de un acto hecho ilegal o prohibido por cualquiera de los siguientes instrumentos: (i) El Convenio sobre las infracciones y ciertos otros actos cometidos a bordo de las aeronaves, 14 de septiembre de 1963, 20 UST 2941 [ Tokio Convención], (ii) Convenio para la represión del apoderamiento ilícito de aeronaves (Secuestro), 16 de diciembre de 1970, 22 UST 1641 [Convención de La Haya], (iii) Convenio para la represión de actos ilícitos contra la seguridad de la aviación civil ( Sabotage), 23 de septiembre de 1971, 24 UST 564 [Convenio de Montreal], (iv) La Convención Internacional contra la toma de rehenes, 17 de diciembre de 1979, TIAS 11081 [Convención sobre los rehenes], (v) Convenio internacional para la represión de los atentados terroristas , 15 de diciembre de 1997, 37 ILM 249 [Convenio sobre bombas], (vi) Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas de 20 de diciembre de 1988, T.IA.S., 20 ILM 493 [Convención de Viena sobre Narcóticos], (vii) Convenio de la Organización Marítima Internacional para la represión de actos ilícitos contra la seguridad de la navegación marítima [Convenio sobre terrorismo marítimo], 10 de marzo de 1988, Doc. OMI. SUA/CON/15/Rev.1, 1993 Can. TS N º 10.

(G) se involucra en una conducta prohibida por los artículos 3 y 4 de este Convenio, con el propósito de atacar la infraestructura crítica de cualquier Estado Parte.

2. Propósito, la intención o el conocimiento con respecto a los delitos previstos en el párrafo 1 del presente artículo podrán inferirse de circunstancias fácticas objetivas.

*Artículo 4*

*Los intentos, la complicidad, la conspiración*

Un delito en virtud del presente Convenio se compromete si alguna persona que ilícita e intencionadamente:

1. tentativas de realizar cualquier conducta prohibida en el artículo 3;

2. ayude o instigue a otros a participar o intentar participar en una conducta prohibida en el artículo 3, o

3. conspira con los demás a participar en una conducta prohibida en el artículo 3.

Artículo 5

*Jurisdicción*

1. Cada Estado Parte en la presente Convención adoptarán las medidas que sean necesarias para establecer su jurisdicción respecto de los delitos enunciados en los artículos 3 y 4 en los siguientes casos:

(A) cuando el delito se haya cometido en el territorio de ese Estado oa bordo de un buque, aeronave o satélite matriculados en ese Estado o en cualquier otro lugar bajo su jurisdicción, reconocido por el derecho internacional;

(B) cuando el presunto delincuente sea nacional de ese Estado;

(C) cuando el presunto delincuente es una persona apátrida cuya residencia principal está en su territorio;

(D) cuando el presunto delincuente se encuentre en su territorio y dicho Estado no conceda la extradición de esas personas en virtud del presente Convenio.

2. Cada Estado Parte en la presente Convención podrá tomar las medidas que sean necesarias para establecer su jurisdicción respecto de los delitos enunciados en los artículos 3 y 4 en los siguientes casos:

(A) cuando el delito se comete con intención o el propósito de dañar ese Estado o de sus nacionales o de obligar a ese Estado a realizar o abstenerse de realizar un acto, o

(B) cuando el delito tenga efectos importantes en ese Estado.

3. La presente Convención no excluye ninguna jurisdicción penal ejercida de conformidad con la legislación nacional, incluida cualquier ley nacional de aplicación de los artículos 3 y 4, o de las competencias penales establecidas en virtud de cualquier otro tratado bilateral o multilateral.

4. Cada Estado Parte ejercerá sus derechos y cumplir sus obligaciones en virtud de la presente Convención en la medida de lo posible, de acuerdo con la siguiente prioridad de jurisdicción: en primer lugar, el Estado Parte en que el presunto delincuente estaba físicamente presente cuando el presunto delito se cometió, en segundo lugar, la Estado Parte en el que un daño sustancial se sufrió como consecuencia de la presunta infracción, en tercer lugar, el Estado Parte de la nacionalidad dominante del presunto delincuente, en cuarto lugar, todo Estado Parte en el que puede ser hallado el presunto delincuente, y quinto, cualquier otro Estado Parte con base razonable para la jurisdicción.

*Artículo 6*

*Asistencia Legal Mutua*

1. Los Estados Parte adoptarán las medidas que sean necesarias para que ellos mismos se presten mutuamente la más amplia asistencia jurídica mutua de manera expedita y continua (en las condiciones previstas por los tratados, las leyes nacionales o los reglamentos relativos a la asistencia) en las investigaciones, las extradiciones, enjuiciamientos y procedimientos judiciales incoados respecto de los delitos enunciados en los artículos 3 y 4, incluida la asistencia para los siguientes fines:

(A) identificar y rastrear los ataques contra los sistemas informáticos por medios electrónicos y de otro tipo;

(B) localización o identificación de personas;

(C) tomar declaración a personas;

(D) efectuar inspecciones e incautaciones por medios electrónicos y de otro tipo;

(E) el examen de objetos y lugares;

(F) asegurar y el intercambio de información y elementos de prueba, incluidos los documentos y registros, y,

(G) la transferencia de los detenidos.

2. Las solicitudes de asistencia se hará de conformidad con los acuerdos en virtud de los acuerdos existentes entre o entre los Estados Partes interesados, oa través de las autoridades centrales designadas por los Estados Partes en la ratificación de la presente Convención. Las solicitudes hechas para asistencia de emergencia serán tratados por equipos de respuesta que funcionan según sea necesario de forma continua.

3. Los Estados Partes promoverán métodos apropiados para la obtención de información y testimonios de personas que están dispuestos a cooperar en la investigación y el enjuiciamiento de los delitos tipificados en los artículos 3 y 4, y deberá, según proceda, prestarán asistencia mutua en la promoción de este tipo de cooperación. Tales métodos de cooperación podrán incluir, entre otras cosas: la concesión de inmunidad judicial a toda persona que colabora sustancialmente con las autoridades policiales en la investigación, extradiciones, procesos y actuaciones judiciales, teniendo en cuenta la disposición de una persona acusada de cooperación sustancial como factor atenuante en determinar el castigo de la persona, y la celebración de acuerdos en materia de inmunidad o no procesamiento o sanciones reducidas.

4. Cualquier propiedad física de un valor intrínseco importante tomado por un Estado Parte que posteriormente se entrega de conformidad con la solicitud de un Estado Parte enjuiciar a facilitar el enjuiciamiento de un presunto delito, previa solicitud en un plazo razonable después de la resolución final de todos los procesos de enjuiciamiento y apelación en los tribunales del Estado Parte procesar, se devolverá al Estado Parte que se apoderó de la propiedad para la venta de acuerdo al derecho interno de ese Estado Parte.

5. Los Estados Partes tendrán libertad para participar en razonables, los métodos electrónicos de investigación de conductas contempladas en los artículos 3 y 4 del presente Convenio, sobre los que tienen jurisdicción para juzgar en virtud del artículo 5, incluso si tales resultados conducta en la transmisión de señales electrónicas en el territorio de los demás Estados Partes. Todo Estado Parte en cuenta que sus esfuerzos de investigación probablemente resultará en que esas transferencias de señales electrónicas a la mayor brevedad posible, informará a todos los Estados Partes afectados de tales esfuerzos.

6. Los Estados Parte considerarán la posibilidad de la aplicación del sistema a través de la ley todas las normas y prácticas recomendadas adoptadas y propuestas por la AIIP conformidad con el artículo 12 como métodos para la mejora de la asistencia jurídica mutua prevista en este artículo 6.

7. Los Estados Partes se comprometen a extender en una cooperación voluntaria en todas las áreas posibles de la actividad de apoyo a la asistencia judicial recíproca, tanto por separado como mediante esfuerzos realizados bajo los auspicios de la AIIP u otras entidades gubernamentales y no gubernamentales.

*Artículo 7*

*Extradición*

1. Delitos tipificados en la legislación interna de cada Estado Parte en relación con cualquier conductas enunciadas en los artículos 3 y 4 se considerarán incluidos entre los delitos que dan lugar a extradición en todo tratado de extradición vigente entre los Estados Partes. Los Estados Partes se comprometen a incluir tales delitos como casos de extradición en todo tratado de extradición que celebren entre sí, sin embargo, el hecho de incluir estos delitos en esos tratados no afectará a las obligaciones contraídas en el presente documento.

2. Si un Estado Parte que subordine la extradición a la existencia de un tratado recibe una solicitud de extradición de otro Estado Parte con el que no tiene tratado de extradición, podrá considerar la presente Convención como la base jurídica de la extradición respecto de los delitos que abarca la conducta conjunto previstos en los artículos 3 y 4. Extradición quedará sujeto a ningún otro requisito de la ley del Estado requerido.

3. Los Estados Partes que no subordinen la extradición a la existencia de un tratado reconocerán los delitos que cubren las conductas enunciadas en los artículos 3 y 4 como casos de extradición entre ellos, con sujeción a cualquier otro requisito de la legislación del Estado requerido.

4. Ofensas que cubren las conductas enunciadas en los artículos 3 y 4 serán en esa medida serán consideradas, a los fines de la extradición entre Estados Partes, como si hubieran sido cometidos en el lugar donde ocurrieron, y también en el territorio del Estado o Estados obligados o autorizados a establecer su jurisdicción de acuerdo con el artículo 5.

5. Cuando se solicita la extradición de más de un Estado Parte requirente, el Estado Parte requerido responderá a las solicitudes de acuerdo con las prioridades de la competencia establecidas en el artículo 5, apartado 4.

*Artículo 8*

*Procesamiento*

1. El Estado Parte en cuyo territorio se encuentre un presunto delincuente, si no lo extradita, estará obligado, sin excepción e independientemente de si el delito se cometa en su territorio, a someter el caso sin demora a las autoridades competentes para a efectos de enjuiciamiento, según el procedimiento previsto en la legislación de ese Estado. Las autoridades deberán acudir a dichos procesos en la misma forma que otros delitos graves conforme a las leyes de ese Estado. Si un Estado Parte no puede o no quiere enjuiciar esos casos, se debe informar con prontitud al Estado Parte o Partes solicitante inicial.

2. El Estado Parte requirente podrá procesar a un presunto delincuente sobre el cual se asegura la competencia mediante la extradición sólo para los delitos especificados en la solicitud de extradición y encuentra legalmente suficiente por el Estado Parte requerido, a menos que el Estado Parte requerido se compromete a permitir el enjuiciamiento por delitos adicionales.

*Artículo 9*

*Medidas Cautelares*

1. A petición de un Estado Parte en base a su creencia razonable de que un presunto delincuente llamado participa en conducta que abarca el presente Convenio y se pueden encontrar en el territorio de un Estado Parte requerido, los Estados Partes se comprometen solicitados a detenerse al presunto delincuente llamado si se encuentra en su territorio y mantener al presunto delincuente hasta por un máximo de diez (10) días, durante los cuales el Estado Parte solicitante suministrará información suficiente para demostrar la causa de detención en espera de la resolución de su solicitud de extradición.

2. A petición de un Estado Parte en base a su creencia razonable de que una conducta contemplada en los artículos 3 y 4 de este Convenio se ha producido, y que la evidencia de tal conducta está presente en los datos almacenados contenidos en los sistemas cibernéticos situados en el territorio del Estado requerido Parte, el Estado Parte requerido tratará de preservar o de exigir la conservación de los datos almacenados en estos sistemas cibernéticos de un plazo razonable para permitir que el Estado Parte requirente que proporcione información suficiente para demostrar causa suficiente para la liberación de la totalidad o parte de la almacenada conservado datos al Estado Parte requirente.

3. Los Estados Parte considerarán la posibilidad de la aplicación del sistema a través de la legislación nacional con todas las normas y prácticas recomendadas adoptadas y propuestas por la AIIP conformidad con el artículo 12 como métodos para mejorar la capacidad de los Estados Parte para adelantar los propósitos de la presente Convención a través de medidas cautelares.

*Artículo 10*

*Los derechos de un acusado*

1. Toda persona detenida por un Estado Parte en virtud de uno o varios de los artículos 3, 4, 5, 6, 7, 8 o 9, tendrán derecho, además de los derechos concedidos en virtud del Derecho nacional de ese Estado Parte, a:

(A) comunicar sin demora innecesaria con el representante competente más próximo del Estado del que esa persona sea nacional o al que competa por otras razones proteger los derechos de esa persona o, si esa persona es apátrida, del Estado de la residencia principal de esa persona;

(B) recibir la visita de un representante de ese Estado;

(C) tener un representante de ese Estado físicamente presente para observar cualquier procedimiento legal que pueda resultar en un castigo, y,

(D) ser informada sin demora después de la detención de los derechos de esa persona conforme a los incisos (a), (b) y (c) de este artículo 10.

2. Los Estados Partes no negar a cualquier persona, o poner en peligro en modo alguno, los derechos descritos en el párrafo 1.

*Artículo 11*

*La cooperación en la aplicación de la Ley*

Los Estados Parte colaborarán estrechamente entre sí a través de sus agencias de aplicación de la ley para prevenir cualquier conducta establecidas en los artículos 3 y 4, por entre otras cosas:

1. tomar todas las medidas posibles para impedir que se prepare en sus respectivos territorios la comisión de dicha conducta dentro o fuera de sus territorios;

2. intercambio de información y coordinando la adopción de medidas administrativas y de otra índole apropiadas para prevenir la comisión de dicha conducta y,

3. teniendo en cuenta para la aplicación del sistema todas las normas y prácticas recomendadas adoptadas y propuestas por la AIIP conformidad con el artículo 12 como métodos para disuadir y prevenir los delitos comprendidos en la presente Convención.

*Artículo 12*

*Agencia para la Protección de la Infraestructura de la Información (AIIP)*

Los Estados Partes establecerán, y se comprometen a poner en funcionamiento tan pronto como sea posible después de la fecha de vigencia del presente Convenio, la Agencia de Protección de la Infraestructura de la Información (AIIP), un organismo internacional integrado por todos los Estados Partes como miembros, y que consiste en una Asamblea, un Consejo, una Secretaría dirigida por un Secretario General, y los comités y demás órganos subsidiarios que sean necesarios a juicio de la Asamblea o del Consejo para implementar los objetivos de la presente Convención. El AIIP y todas sus entidades y funciones de componentes serán financiados por una evaluación obligatoria cada dos años impuesta a sus miembros de acuerdo con una fórmula propuesta por el Consejo y aprobado por la Asamblea.

1. Asamblea . La Asamblea AIIP estará integrado por todos los Estados Partes, cada uno de los cuales serán representados por una persona competente en tecnologías de informática, que tendrá un solo voto en todas las actividades de la Asamblea. La Asamblea se reunirá al menos una vez cada tres (3) años y podrá tomar decisiones por una mayoría de votantes. La Asamblea tendrá las siguientes funciones y atribuciones:

(A) la adopción de los objetivos y políticas autorizadas por y de conformidad con el presente Convenio;

(B) dar instrucciones al Consejo para elaborar y / o aplicar medidas para alcanzar dichos objetivos y políticas;

(C) examinar y aprobar las normas y prácticas propuestas por el Consejo para su adopción por los Estados Partes;

(D) considerar y aprobar el presupuesto AIIP y la fórmula de evaluación elaborado y propuesto por el Consejo;

(E) recomendar a los Estados Partes las modificaciones o acuerdos suplementarios en la presente Convención, incluida la incorporación de los tipos de conducta que deben considerarse criminal;

(F) elegir no menos de la quinta parte y no más de una cuarta parte de sus miembros para el Consejo, que deberá incluir al menos un representante de cada uno de los cinco miembros permanentes del Consejo de Seguridad de las Naciones Unidas;

(G) examinar y aprobar las propuestas del Consejo de prestar asistencia técnica y material a merecer Estados Partes con el fin de fomentar el uso seguro y generalizada de la infraestructura de información internacional;

(H) proponer a todos los Estados Partes como recomendaciones o propuestas de enmienda a esta Convención, las normas, las prácticas y las medidas tecnológicas adoptadas por el Consejo;

(I) examinar y aprobar las medidas propuestas por el Consejo para evitar que un Estado sea utilizado como un refugio seguro o de otra manera con el fin de permitir a las personas para asegurar la protección de la prevención efectiva, la investigación o el enjuiciamiento de las conductas enunciadas en los artículos 3 y 4 , y,

(J) al adoptar reglamentos para su propio gobierno, que deberá incluir la autoridad para suspender o expulsar a los Estados Partes, y recomendar a los Estados Partes la exclusión de cualquiera de los Estados de la participación en la infraestructura internacional de información, por una conducta que atenta contra los objetivos de la presente Convención , en una votación de al menos dos terceras partes (2/3) de todos los Estados Partes votantes.

2. Consejo . El Consejo AIIP estará formado por representantes de los Estados Miembros elegidos por la Asamblea. El Consejo se reunirá al menos una vez cada año y decidirá todas las cuestiones por mayoría de votos. El Consejo tendrá las siguientes funciones y atribuciones:

(A) preparar el presupuesto AIIP y la fórmula de evaluación para su examen y aprobación por la Asamblea;

(B) nombrar y supervisar al Secretario General, y para proporcionar una secretaría para administrar las actividades AIIP con un personal limitado en número y función en la medida en que la confianza en los voluntarios no permanente y personal de contrato es posible;

(C) nombrar comisiones permanentes y especiales, que consisten en las personas de los sectores público y privado (incluyendo a los voluntarios) que son expertos en los campos de las actividades de los comités, que se reunirá cuando sea necesario para considerar y recomendar a las normas y prácticas del Consejo , así como las medidas tecnológicas para mejorar la seguridad de las infraestructuras de información, incluyendo las capacidades de los Estados Partes y los organismos encargados de hacer cumplir la ley para detectar, prevenir, investigar y enjuiciar con éxito conducta establecidas en los artículos 3 y 4, y para evitar que cualquier Estado del bienestar utilizada como un refugio seguro;

(D) tener en cuenta, y que el Consejo considere oportuno, proponer a la Asamblea para su aprobación como recomendaciones o propuestas de enmienda al presente Convenio, normas, prácticas o medidas elaboradas por la posición del AIIP o comisiones especiales, teniendo en cuenta la labor de las entidades públicas y privadas, como el IETF, con el fin de garantizar la coherencia de las normas y prácticas;

(E) recibir, examinar e informar a la Asamblea sobre los informes anuales presentados por los Estados Partes en virtud del artículo 14;

(F) considerar y recomendar a la Asamblea que los Estados Partes se considerará elegible para recibir asistencia técnica y financiera a fin de que puedan satisfacer sus obligaciones en virtud del presente Convenio y que participen en la medida posible, en actividades útiles relacionados con los sistemas informáticos;

(G) adoptar y poner en práctica programas de asistencia técnica y financiera a los Estados Partes, incluidos los programas de capacitación para personal policial y de seguridad informática, con especial atención a llegar a los Estados Partes pueden optar a la ayuda financiera, y para trabajar con otras organizaciones públicas y privadas a este respecto;

(H) considerar y recomendar en su caso de las sanciones de la Asamblea de los Estados Partes o de otros Estados de la conducta que socava los objetivos del presente Convenio, y

(I) adoptar los reglamentos para su propio gobierno.

3. Secretaría . La Secretaría funcionará como dirigida por el Secretario General. El personal de la Secretaría prevista por la Asamblea, por recomendación del Consejo, será nombrado por el Secretario General.

4. Participación Pública . Las reuniones de la Asamblea y el Consejo de la AIIP estarán abiertas al público, con tal participación pública como sea posible. Las reuniones de los comités, grupos de trabajo y otras entidades AIIP también estarán abiertos al público, sin perjuicio de la necesidad de considerar confidencial de la información sensible.

*Artículo 13*

*Protección de la privacidad y otros derechos humanos*

1. El presente Convenio no se interpretará para requerir una violación de la privacidad u otros derechos de cualquier persona como se define en las leyes del Estado Parte requerido para desempeñar cualquier trabajo estuvo de acuerdo en virtud del presente Convenio.

2. Como parte de la obligación de establecer un seguimiento sistemático de la aplicación del presente Convenio en virtud del artículo 14, un subcomité permanente de expertos serán establecidos por el Consejo para evaluar y comentar sobre la forma en que la Convención se está aplicando en lo que respecta a la protección de la privacidad y otros derechos humanos y recomendar las medidas apropiadas para el Consejo y la Asamblea con el fin de proteger esos derechos.

*Artículo 14*

*Informes anuales de los Estados Partes*

1. Cada Estado Parte en o antes del final de cada año natural a partir del año de su adhesión a este convenio a la AIIP cualquier información pertinente sobre:

(A) las medidas legislativas y administrativas adoptadas por ésta para la ejecución del presente Convenio.

(B) cualquier modificación de sus leyes y reglamentos nacionales que afectan a la aplicación del presente Convenio;

(C) las circunstancias de un delito sobre el que ha establecido su jurisdicción de conformidad con el artículo 5;

(D) las medidas adoptadas por ésta en relación con cada supuesto delincuente que fue detenido por un período de tiempo en virtud del Convenio o en virtud de su derecho interno la aplicación de la totalidad o parte de la Convención y, en particular, los resultados de cualquier extradición o otros procedimientos legales, y

(E) cualquier decisión de no aplicar una norma o método recomendado aprobada por la Asamblea AIIP.

2. La Secretaría AIIP recopilará anualmente y transmitir a todos los Estados Parte de la información recogida de los mismos en virtud de este artículo 14.

*Artículo 15*

*Firma, ratificación, aceptación, aprobación, adhesión y reservas*

1. El presente Convenio estará abierto a la firma de cualquier Estado después de \_\_\_\_\_\_\_\_\_ [fecha] en \_\_\_\_\_\_\_\_\_\_\_\_ [LOCALIZACIÓN EN ESTADO depositario], en el Estado de \_\_\_\_\_\_\_\_\_, que actuará como depositario.

2. La presente Convención está sujeta a ratificación, aceptación, aprobación o adhesión. Los instrumentos de ratificación, aceptación, aprobación o adhesión se depositarán en poder del Estado depositario.

*Artículo 16*

*Entrada en vigor*

1. El presente Convenio entrará en vigor el (30a) trigésimo día siguiente a la fecha del depósito del \_\_\_\_\_\_\_\_\_ [número ordinal] instrumento de ratificación, aceptación, aprobación o adhesión en poder del Estado depositario.

2. Para cada Estado que ratifique, acepte, apruebe o se adhiera a la Convención después del depósito del \_\_\_\_\_\_\_\_\_ [número ordinal] instrumento de ratificación, aceptación, aprobación o adhesión, la Convención entrará en vigor el (30a) trigésimo día después del depósito por tal Estado de su instrumento de ratificación, aceptación, aprobación o adhesión en poder del Estado depositario.

*Artículo 17*

*Enmiendas*

1. Un Estado Parte o de la AIIP pueden proponer enmiendas a la presente Convención y presentarlas al Estado depositario. El Estado depositario comunicará cada enmienda propuesta a los Estados Partes.Si dentro de los cuatro (4) meses desde la fecha de esa notificación, al menos un \_\_\_\_\_\_\_ [FRACCIÓN] la mayoría de los Estados Partes votar por la aprobación de la enmienda al Estado Depositario informará de ello a todos los Estados Partes que será a partir de entonces comunicar cualquier ratificación de dicho proyecto enmiendas. Las propuestas de enmienda serán efectivos a su ratificación, por un \_\_\_\_\_\_\_ [FRACCIÓN] la mayoría de los Estados Partes.

2. Cuando las enmiendas entren en vigor, serán obligatorias para los Estados Partes que lo han ratificado. Los demás Estados Partes seguirán obligados por las disposiciones de la presente Convención y por toda enmienda anterior que hubiesen ratificado.

*Artículo 18*

*Denuncia*

Todo Estado Parte podrá denunciar la presente Convención mediante notificación escrita dirigida al Estado depositario. El Estado depositario comunicará sin demora a la recepción de la notificación a los demás Estados Partes. La denuncia surtirá efecto un (1) año después de la fecha de recepción de dicha notificación.

*Artículo 19*

*Delitos políticos y acciones lesivas*

1. Ninguno de los delitos o conductas enunciadas en los artículos 3 y 4 se considerarán, a los fines de la extradición o de asistencia judicial recíproca, como delito político o un delito equivalente a un delito político.

2. Ninguna disposición de la presente Convención podrá interpretarse como la imposición de una obligación de extraditar o de prestar asistencia judicial recíproca si el Estado Parte requerido tiene motivos fundados para creer que la solicitud de extradición para los delitos previstos en los artículos 3 y 4 o de asistencia judicial mutua con relación con esos delitos se ha formulado con el fin de perseguir o castigar a una persona por razón de su raza, religión, nacionalidad, origen étnico u opinión política.

*Artículo 20*

*Conducta Estado*

El presente Convenio no se aplicará a cualquier conducta estatal realizado para un propósito público no comercial, incluidas las actividades realizadas por las fuerzas militares de un Estado Parte, o con las actividades de un Estado Parte en relación con un conflicto armado en curso.

*Artículo 21*

*Resolución de Disputas*

1. Los Estados Partes tratarán de resolver todas las disputas que surjan en virtud del presente Convenio mediante negociación y mediación, con la asistencia de la Secretaría AIIP.

2. Todo Estado Parte podrá notificar a la otra su intención de recurrir al arbitraje de una controversia especifica, para comenzar no antes de noventa (90) días después de recibida la notificación por la Parte a la que se envía. Si las Partes no consiguen ponerse de acuerdo en un tribunal de arbitraje o en cualquier otro aspecto necesario del arbitraje solicitado, el asunto se remitirá por la Parte requirente la decisión en el marco de \_\_\_\_\_\_\_\_\_\_ [MECANISMO DE ARBITRAJE ADD].

3. El Consejo AIIP a la mayor brevedad posible, elaborar y proponer a la Asamblea un mecanismo de resolución de conflictos que es informal, rápida, y con base en la participación de técnicos adecuados.

*Artículo 22*

*Idiomas y depositario*

El original de la presente Convención, cuyos textos en inglés, francés y ruso son igualmente auténticos, será depositado en poder del Estado depositario, que enviará copias certificadas de él a todos los Estados Partes.

EN FE DE LO CUAL, los abajo firmantes, debidamente autorizados por sus respectivos Gobiernos, han firmado el presente Convenio, abierto a la firma en \_\_\_\_\_\_\_\_\_\_ [LUGAR EN ESTADO depositario] de \_\_\_\_\_\_\_\_\_\_ [fecha].

**Abreviaturas**

AIIP Agencia de Protección de la Infraestructura de Información

CCIPS Delito y Sección de Propiedad Intelectual Computer (EE.UU. Departamento de Justicia)

CERT Computer Emergency Response Team

CISAC Centro para la Seguridad y la Cooperación Internacional (Universidad de Stanford)

COE Consejo de Europa

Consorcio QUEBRADIZO de Investigación sobre Seguridad y Política de la Información (Universidad de Stanford)

Departamento de Defensa DOD (EE.UU.)

FBI Oficina Federal de Investigaciones (EE.UU. Departamento de Justicia)

G-8 Grupo de los Ocho

Organización de Aviación Civil Internacional de la OACI

IETF Internet Engineering Task Force

Organización Marítima Internacional OMI

UIT Unión Internacional de Telecomunicaciones

ONG Organizaciones No Gubernamentales

SARP Normas y métodos recomendados

ONU Naciones Unidas

Programa de Desarrollo de las Naciones Unidas PNUD

EE.UU. Estados Unidos