MODELO ONU ASOBILCA XXXII

GUÍA ACADÉMICA

ONUDD

Presidentes: Juan S. Uribe y Jacobo Ospina
Supervisora: Sara Agudelo

WWW.ONUASOBILCA.ORG
ONUDD.ASOBILCA32@GMAIL.COM

ASOBILCA
ASOCIACIÓN DE COLEGIOS BILINGÜES DE CALI

Índice

¡BIENVENIDOS A ASOBILCA XXXII!

Estimados Participantes,

Con mucho orgullo y entusiasmo, les doy la bienvenida a la trigésimo segunda edición del Modelo de Naciones Unidas ASOBILCA. Hoy iniciamos una nueva edición de un proyecto que, a lo largo de los años, se ha consolidado como un espacio de formación, diálogo y liderazgo para jóvenes comprometidos con la construcción de un mundo más justo y consciente de sus realidades.

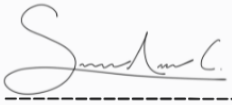
Esta edición representa mucho más que una nueva versión de un Modelo de Naciones Unidas, representa un espacio donde las ideas encuentran sentido, donde el diálogo se convierte en aprendizaje y donde jóvenes comprometidos deciden asumir con responsabilidad y criterio, el reto de comprender y transformar el mundo que los rodea. El Modelo ONU ASOBILCA es el resultado de la convicción de que la educación va más allá del aula y de que el debate informado, la escucha activa y el respeto por la diferencia son herramientas fundamentales para la construcción de sociedad. Cada uno de los comités ha sido diseñado con el propósito de retarlos intelectualmente, de invitarlos a cuestionar lo establecido y de permitirles explorar la complejidad de los asuntos internacionales desde una mirada crítica, empática y propositiva.

Para mí como Secretario General, el Modelo ONU ASOBILCA XXXII es la materialización de un proyecto colectivo construido con esfuerzo, compromiso y vocación. Detrás de cada guía, cada tema y cada detalle organizativo hay personas que creemos profundamente en este modelo y en el impacto que puede tener en la formación de quienes participan en él. Nada de esto sería posible sin el trabajo del secretariado, los presidentes, el staff y los sponsors, cuyo esfuerzo sostiene la esencia de este proyecto.

Pero la realidad es que este modelo pertenece, ante todo, a ustedes. A quienes deciden prepararse, investigar, debatir y representar con seriedad y respeto. Este modelo no busca discursos perfectos ni respuestas simples, sino reflexiones honestas, posturas bien fundamentadas y la disposición constante a aprender del otro. Aquí, el verdadero valor está en el proceso: en cada argumento construido, en cada negociación intentada y en cada perspectiva comprendida. Espero que esta experiencia trascienda lo académico y se convierta en un espacio de crecimiento personal. Que el Modelo ONU ASOBILCA XXXII les deje preguntas, aprendizajes, vínculos que permanezcan más allá del modelo y, sobre todo, recuerdos inolvidables. Que al cerrar esta edición, puedan reconocer en ustedes mismos una voz más consciente, más crítica y más comprometida con la realidad que los rodea.

Gracias por hacer parte de este sueño llamado ASOBILCA XXXII y por confiar en este proyecto. Que estas páginas sean el inicio de una experiencia significativa, formativa y memorable.

Atentamente,



Sebastián Ávila Cabal
Secretario General

CARTA DE BIENVENIDA

Honorables delegados,

Es un placer darles la bienvenida al comité de ONUDD del modelo ASOBILCA XXII. Somos Juan Sebastián Uribe y Jacobo Ospina. Ambos hemos disfrutado de una experiencia ONU sumamente educativa, diversa, y entretenida. Al inicio, los modelos de ONU sirvieron mucho para mejorar nuestras habilidades de oratoria y discutir temas de interés con otras personas. Sin embargo, con el tiempo hemos encontrado un lugar especial y seguro en los modelos donde hemos adquirido una valiosa experiencia para estar con ustedes hoy.

La ONU nos ha ayudado a comprender múltiples conflictos globales y las consecuencias de no resolverlos. La ONUDD, la cual trata con temas de relevancia internacional relacionada con el crimen internacional, tiene una posición esencial en el futuro de la comunidad global. Por eso, hemos considerado dos temas relevantes para ser considerados en el modelo de este año. Debatir sobre el uso de criptomonedas y el desarrollo de la ciberseguridad ayudarán a generar soluciones para un futuro digitalizado.

Como sus presidentes, esperamos que se mantengan dedicados y concentrados durante todo el debate. Esto incluye comprender su rol en la diplomacia y el debate, completar su portafolio a tiempo, defender las posiciones de su delegación y buscar posibles soluciones. Sin embargo, nuestro trabajo es apoyarlos en todo lo que necesiten, entonces si tienen alguna inquietud, no duden en contactarnos para obtener ayuda, ya sea que apenas estén empezando a debatir, o ya tengan experiencia considerable. Nuestro somos una alternativa confiable a la que puedan recurrir si se sienten nerviosos, confundidos, o con alguna duda.

Por supuesto, esperamos que este modelo sea una experiencia tan enriquecedora para ustedes como ojalá lo será para nosotros. Reiteramos que no duden en contactarnos al correo

electrónico del comité si tienen alguna inquietud sobre los temas, el debate o si simplemente necesitan alguna aclaración. Estaremos encantados de ayudarles.

Atentamente,

INTRODUCCIÓN A LA COMISIÓN

La Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD), establecida oficialmente en 1997, es el resultado de la fusión entre dos estructuras previas de la ONU: el Programa Internacional para el Control de Drogas (creado en 1991) y el Centro para la Prevención del Delito y la Justicia Penal (activo desde 1981). Esta integración respondió a una preocupación creciente de la comunidad internacional: la expansión del narcotráfico, el crimen organizado y la corrupción como amenazas cada vez más globales y complejas.

Desde finales del siglo XX hasta hoy, la ONUDD ha evolucionado para convertirse en una institución esencial dentro del sistema de Naciones Unidas. Su labor se centra en apoyar a los Estados miembros con asistencia técnica, elaboración de datos confiables, fortalecimiento institucional y promoción de estándares internacionales en áreas clave como: la lucha contra las drogas ilícitas, la trata de personas, el tráfico ilícito de migrantes, el terrorismo, el lavado de activos y, más recientemente, los delitos cibernéticos. A lo largo de estas décadas, la Comisión ha impulsado instrumentos internacionales de gran relevancia, como la Convención de Palermo contra la Delincuencia Organizada Transnacional (2000) y la Convención contra la Corrupción (2003), las cuales se consolidan como instrumentos claves para la ONUDD porque ofrecen la base jurídica para responder a amenazas que generan impactos globales medibles: según estimaciones de Naciones Unidas, la corrupción representa hasta el 5 % del PIB mundial (aprox. 2,6 billones de dólares anuales), mientras que la delincuencia organizada transnacional mueve cientos de miles de millones de dólares cada año y afecta directamente a la seguridad y gobernanza de los Estados. En este contexto, la Convención de Palermo (2000) permite coordinar acciones frente a fenómenos como la trata de personas con decenas de miles de víctimas detectadas anualmente a nivel global y el lavado de activos, mientras que la Convención contra la Corrupción (2003) fortalece la prevención, sanción y

recuperación de activos ilícitos, un aspecto clave para restituir recursos públicos y reforzar el Estado de derecho, pilares centrales de la labor de la ONUDD.

En la actualidad, la importancia de la ONUDD es mayor que nunca. Las redes criminales operan a escala transnacional, utilizan tecnologías avanzadas y se adaptan rápidamente a los cambios sociales, económicos y políticos, lo que plantea desafíos significativos para la cooperación internacional, que no siempre es automática ni equitativa entre los Estados. En este contexto, la Comisión ofrece un espacio multilateral clave para reducir estas asimetrías, facilitando el intercambio de información, la coordinación de estrategias y el desarrollo de políticas más coherentes. Asimismo, su labor se articula de manera transversal con la Agenda 2030, en particular con el ODS 16, que constituye un eje central del trabajo de la ONUDD al orientar sus acciones hacia la promoción de sociedades pacíficas, justas y con instituciones sólidas.

En síntesis, la ONUDD representa un pilar estratégico para la seguridad internacional. Su papel no solo consiste en combatir el delito, sino también en fortalecer la prevención, mejorar la gobernanza y apoyar a los Estados para que puedan proteger mejor a sus ciudadanos y mantener la estabilidad social.

TEMA 1:

EL CRECIENTE USO DE CRIPTOMONEDAS PARA BURLAR AUTORIDADES Y REALIZAR TRANSACCIONES SIN INTROMISIÓN GUBERNAMENTAL

Contexto Histórico

Antes de las criptomonedas que conocemos hoy en día, se crearon otros sistemas los cuales utilizaban el cifrado para proteger información digital. Sin el desarrollo de esta área, la base del blockchain en la que dependen las criptomonedas actuales no existiría, lo cual las dejaría vulnerables a ataques cibernéticos, así como a ser duplicadas o falsificadas. En los años 90, algunos bancos intentaron aprovechar la nueva tecnología de cifrado para desarrollar monedas digitales, o "DigiCash". Sin embargo, al depender de dichos bancos privatizados y estar controlados por ellos, nunca obtuvieron confianza generalizada y debido a esto terminaron fallando, por lo que posteriormente abriría rienda suelta a la creación de nuevas monedas de este tipo, las cuales no estuvieran amarradas a bancos, y se popularizó en gran parte gracias a esto, ya que el libre albedrío que estas proporcionaban, generaba un gran atractivo en organizaciones delincuenciales, por lo que facilitaba actividades de transacción ilegal.

Se considera que el origen de las criptomonedas que conocemos hoy en día se dio durante la crisis financiera del 2008. Un año de muchísima incertidumbre económica, el 2008 fue la oportunidad perfecta para que emergiera una nueva forma de comprar y vender en el mercado internacional. En octubre de dicho año, un usuario con el nombre de Satoshi Nakamoto publicó un artículo detallando el funcionamiento de una nueva moneda digital conocida como "Bitcoin". Al inicio del 2009, sé generaron las primeras 50 unidades de bitcoin, y desde entonces, una infinidad de criptomonedas se han popularizado no solo en el mercado

internacional, sino también en las redes criminales que utilizan esta tecnología para ocultar sus transacciones.

Para empezar a explorar el uso de estas monedas digitales en la economía ilegal, primero se debe entender como funcionan estos sistemas, y de donde obtienen su valor. Para hacer esto, utilizaremos la criptomoneda más popular; el bitcoin. Como una moneda corriente, el bitcoin obtiene su valor debido a que existe una cantidad limitada. Cada bitcoin está conformado por bloques de ecuaciones cifradas almacenadas en una red descentralizada operada por una gran cantidad de servidores individuales. Gracias a la gran complejidad de dichos cifrados, las criptomonedas, son imposibles de duplicar y falsificar, ya que cada moneda es verificada y corroborada durante cada transacción. No solo esto, sino que también son extremadamente difíciles de generar. Las criptomonedas como el bitcoin pueden ser "minadas" utilizando sistemas de descifrado extremadamente complejos, los cuales resuelven dichas ecuaciones del blockchain para generar nuevas monedas. Sin embargo, este proceso es extremadamente costoso en términos de energía y hardware, y tomando en cuenta la volatilidad del bitcoin, muchas veces no resulta rentable. La última consecuencia de este sistema complejo es la más importante en términos del mercado ilegítimo; Dado que las criptomonedas existen en un servidor descentralizado y no regulado, las transacciones de dichos recursos no dejan ningún rastro digital concreto de la transacción, ya que lo único que dejan son registros recubiertos bajo pseudónimos, los cuales resultan imposibles de rastrear. Esta característica es extremadamente útil para los mercados ilegítimos, y representa una complicación grave cuando se trate de regular el flujo de dichas criptomonedas para la obtención de bienes y servicios no regulados, así como para financiar actividades ilegales.

En los últimos años, el mundo ha notado cómo las criptomonedas han empezado a ser utilizadas por organizaciones de crimen internacional para financiar sus operaciones de manera rápida y segura, así como para lavar sus activos ilegítimos y generar ingresos imposibles de rastrear. Gracias a esto, los gobiernos en todo el mundo han empezado a desarrollar organizaciones y sistemas encargados de monitorear y regular el tráfico de criptomonedas en el mundo de las operaciones ilegítimas. Sin embargo, las características que hacen de las criptomonedas tan confiables como moneda global también la hacen increíblemente difícil de rastrear, y este comité necesita desarrollar medidas efectivas para prevenir que estas tecnologías sean utilizadas de manera ilícita y desarrollar estándares para poder diferenciar entre uso legitimo e ilegitimo para evitar normativas sesgadas.

Situación Actual

La expansión global de las criptomonedas ha transformado de manera profunda el escenario financiero actual. Desde su aparición, estos activos digitales han desafiado las estructuras tradicionales de supervisión, revelando vulnerabilidades que los Estados aún intentan comprender y regular. La descentralización, el carácter pseudónimo de las direcciones y la posibilidad de realizar transferencias internacionales inmediatas sin intermediarios han creado un entorno donde la capacidad de los gobiernos para monitorear, rastrear o bloquear flujos monetarios se ve significativamente limitada, por ende es actualmente materia de debate el cómo introducir mediaciones a este tipo de transacciones para poder seguir fomentando el uso de estos mismos, ya que hasta que no se pueda garantizar una legalidad completa a la hora de su uso, será un campo por el cual los grupos al margen de la ley se podran aprovechar para continuar con sus actos delictivos.

A nivel internacional, los Estados enfrentan un reto doble: por un lado, deben promover la innovación tecnológica y permitir el desarrollo de nuevas formas de economía digital; por otro,

deben impedir que estas herramientas se conviertan en un canal para prácticas ilícitas como el lavado de dinero, la financiación de actividades criminales, la evasión fiscal o la fuga de capitales. La ausencia de normas específicas para el uso de estos activos empeora esta situación, pues mientras algunas jurisdicciones han implementado regulaciones estrictas, otras mantienen restricciones laxas o inexistentes, incentivando el desplazamiento de actividades delictivas hacia espacios de menor supervisión, como este.

La parte técnica del mundo cripto también representa un reto. Herramientas como los *mixers*, las redes enfocadas en la privacidad y las plataformas de finanzas descentralizadas hacen que al Estado le resulte muy difícil conectar una transacción con una persona real, mostrando que la velocidad del estado para garantizar una regulación va a un ritmo distinto y ciertamente inferior que el de los que se aprovechan de estas monedas para actos delincuenciales. Además, aparecen constantemente nuevas tecnologías, cadenas de bloques y métodos para ocultar la identidad que avanzan más rápido que las leyes. Todo esto genera un entorno donde las criptomonedas funcionan casi como un sistema financiero paralelo que escapa, en parte, al control estatal tradicional.

Caso de Estudio

Dentro del contexto actual del mundo, Estados Unidos representa el mejor ejemplo de los desafíos regulatorios actuales. Este país enfrenta una de las crisis de salud pública más severas de su historia debido al alto consumismo de fentanilo, un opioide sintético extremadamente potente que ha provocado un aumento significativo en las muertes por sobredosis. La compleja cadena de producción, distribución y financiamiento del fentanilo muestra con claridad cómo las criptomonedas se han integrado en actividades ilícitas a nivel internacional y como estas pueden pasar de manera prácticamente indetectada

En las primeras etapas de la cadena de la distribución del fentanilo, las criptomonedas son utilizadas para la adquisición de los químicos para su producción, los cuales son provenientes principalmente de proveedores internacionales. Estos pagos suelen realizarse en Bitcoin, stablecoins como USDT o, en algunas ocasiones, en criptomonedas centradas en la privacidad, a veces siendo presuntamente diseñadas propiamente por los mismos grupos criminales, como por ejemplo carteles como el de Sinaloa o el Jalisco. Su uso permite a las organizaciones criminales evadir los mecanismos de control presentes en el sistema bancario, evitando reportes de transacciones sospechosas y restricciones regulatorias que sí existirían en las transacciones vigiladas estatalmente.

(Figura 1, Las dos monedas más usadas en trafico Ilegal, USDT (TETHER) y BITCOIN)

A medida que el producto se mueve a través de la cadena de distribución, las criptomonedas siguen siendo muy importantes. Los grupos criminales usan métodos como dividir los pagos, crear direcciones temporales, usar mezcladores y servicios descentralizados para ocultar de dónde vienen los fondos y hacer más difícil su seguimiento. La rapidez de las transacciones y la capacidad de mover dinero entre lugares con diferentes reglas hacen que este método sea una forma efectiva y discreta de mantener un mercado ilegal muy rentable.

Ante esta situación, Estados Unidos ha creado varias estrategias para regular, usar tecnología y aplicar leyes. Las agencias federales han empezado a usar herramientas avanzadas para analizar blockchain, lo que les ayuda a identificar patrones, conectar direcciones con actividades ilegales y entender flujos financieros complejos. Al mismo tiempo, se han impuesto sanciones a plataformas relacionadas con el lavado de dinero, especialmente a los servicios que mezclan criptomonedas para ocultar transacciones de actividades delictivas.

Sin embargo, persisten importantes obstáculos. La regulación estadounidense es fragmentada, con diferencias entre estados y con múltiples agencias reclamando jurisdicción sobre distintos aspectos del ecosistema. La ausencia de un marco de penalización o de acción frente a estos grupos unificados entre todos los estados genera incertidumbre y limita la eficacia de las medidas implementadas. Además, la naturaleza global y descentralizada del tráfico de fentanilo implica que ninguna acción nacional aislada puede resolver completamente el problema, ya que las redes delictivas pueden adaptarse, migrar a plataformas extranjeras o recurrir a nuevas tecnologías que eviten la supervisión estatal.

También es importante agregar que el Fondo Monetario Internacional (FMI) desempeña un papel crucial en la regulación financiera global, lo que incluye la supervisión del uso de criptomonedas, desde un ámbito de experiencia en el área del control técnico-financiero. Su experiencia puede ser valiosa para Estados Unidos al desarrollar políticas que aborden los desafíos regulatorios asociados con el uso de criptomonedas en el tráfico de fentanilo desde su vasta experiencia lidiando con los desafíos que se presentan a través de la evolución del area de las finanzas. El FMI ha advertido sobre los riesgos que estas monedas digitales representan para la estabilidad económica, y su enfoque en la cooperación internacional, puede facilitar la creación de estándares globales que limiten su empleo en actividades ilícitas. Además, el FMI puede proporcionar asesoría sobre la utilización de tecnologías avanzadas para rastrear transacciones y promover programas de capacitación para funcionarios, mejorando así la capacidad de los gobiernos para enfrentar este problema de manera efectiva.

En conjunto, el caso estadounidense y su vínculo con el fentanilo revela cómo las criptomonedas no solo facilitan transacciones ilícitas, sino que también potencian mercados capaces de operar más allá de la capacidad de intervención del Estado. Este fenómeno subraya la necesidad de avanzar hacia regulaciones coherentes, coordinación internacional y desarrollo de instrumentos tecnológicos que permitan enfrentar de manera efectiva un ecosistema financiero, dinámico y globalizado, En este sentido, la cooperación multilateral se

vuelve indispensable para enfrentar redes criminales transnacionales que aprovechan tanto las criptomonedas como las brechas regulatorias entre Estados. Este enfoque se alinea directamente con el mandato de la Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD), que promueve la acción conjunta, el fortalecimiento institucional y la armonización normativa como pilares para combatir el crimen organizado y el tráfico ilícito en un entorno globalizado.

Puntos Clave

Regulación

- La naturaleza descentralizada de las criptomonedas como obstáculo para la regulación y supervisión de las transacciones.
- La falta de regulaciones estandarizadas a nivel internacional para prevenir el uso de criptomonedas en el crimen organizado.

Tecnología

- La modificación o adaptación de la tecnología para dejar un rastro digital de las transacciones que permita su supervisión posterior.
- El uso de *mixers*, VPNs u otras tecnologías que impiden o dificultan el rastreo de transacciones digitales.
- El principio de privacidad en el que se basan las criptomonedas y la necesidad de reducir dicha privacidad para facilitar la trazabilidad.

Seguridad

- Las actividades ilícitas, como el lavado de activos o la adquisición de bienes prohibidos, que se aprovechan del uso de criptomonedas.

Soberanía monetaria

- La adopción de criptomonedas como moneda nacional (caso de El Salvador) y sus implicaciones para la seguridad fiscal y financiera del Estado.
- La creación de alternativas estatales, como las Monedas Digitales de Bancos Centrales (CBDC), que permitan un control más estricto sobre el sistema monetario nacional.

Cooperación internacional

- La cooperación internacional para generar regulaciones coherentes acordes a la escala global de la problemática.
- La creación de instituciones internacionales que regulen y administren el flujo de criptomonedas en el mercado internacional.

Preguntas Orientadoras

- ¿Cómo pueden los países regular el uso de criptomonedas sin impedir el desarrollo de esta tecnología o debilitar a la economía?
- ¿De qué manera organismos como el FMI pueden ayudar a los gobiernos a utilizar tecnologías avanzadas para monitorear y rastrear transacciones con criptomonedas, y cómo esto puede impactar en la efectividad de las políticas contra el tráfico de drogas?
- ¿Qué crímenes dependen de transferencias en criptomonedas y que otras maneras hay de prevenirlos para desincentivar el uso de estas transacciones digitales?
- ¿Qué responsabilidades legales y jurídicas tienen los creadores de las criptomonedas originales, así como los "miners" en controlar y restringir el flujo de criptomonedas en el mercado internacional?
- ¿Es viable exigir sistemas de verificación de identidad para autorizar transferencias de criptomonedas?
- ¿Cómo se deben adaptar las organizaciones internacionales para poder lidiar con el crimen que se aprovecha de las criptomonedas?
- ¿Deberían los países desarrollar criptomonedas estatales que son más fáciles de regular como alternativa a las criptomonedas descentralizadas?

- ¿Qué riesgos trae la adopción masiva de criptomonedas en economías como la de El Salvador, considerando los riesgos a la seguridad de un país que acoge una moneda no controlada por las instituciones nacionales?
- ¿Es mejor regular las criptomonedas existentes o crear monedas digitales estatales como alternativa más controlable?
- ¿Cómo se pueden balancear la necesidad de privacidad y confidencialidad con la regulación y control de estas criptomonedas descentralizadas?
- ¿Cómo se pueden desarrollar alianzas internacionales para prevenir la existencia de "paraísos cripto" donde las regulaciones son limitadas y por ende facilitan las actividades ilícitas relacionadas con las criptomonedas?

Referencias

Aleph Comunicación. (2021, November 15). El origen de las criptomonedas y cómo funcionan. Santanderconsumer.es; Banco Santander. https://www.santanderconsumer.es/simplefinance/blog/tu-futuro/ciberseguridad/post/el-origen-de-las-criptomonedas-y-como-funcionan

Banco Central de Reserva del Peru. (n.d.). Riesgos de las criptomonedas. Www.bcrp.gob.pe. https://www.bcrp.gob.pe/sistema-de-pagos/articulos/riesgos-de-las-criptomonedas.html

Farah, D., & Richardson, M. (2023, March 20). The Growing Use of Cryptocurrencies by Transnational Organized Crime Groups in Latin America. Georgetown Journal of International Affairs. https://gjia.georgetown.edu/2023/03/20/the-growing-use-of-cryptocurrencies-by-transnational-organized-crime-groups-in-latin-america/

Federal Trade Commission. (2021, April 13). Lo que hay que saber sobre las criptomonedas y las estafas. Consumer Information. https://consumidor.ftc.gov/articulos/lo-que-hay-que-saber-sobre-las-criptomonedas-y-las-estafas

Kabra, S., & Gori, S. (2023). Drug trafficking on cryptomarkets and the role of organized crime groups. Journal of Economic Criminology, 2, 100026. https://doi.org/10.1016/j.jeconc.2023.100026

Taboada, P. S. (2023). Análisis criminológico de la delincuencia con criptomonedas cometida por grupos criminales y su aproximación desde los sistemas inteligentes. Dialnet, 1. https://dialnet.unirioja.es/servlet/dctes?info=link&codigo=315830&orden=0

United Nations. (2023). Money laundering through cryptocurrencies. United Nations : UN Toolkit on Synthetic Drugs. https://syntheticdrugs.unodc.org/syntheticdrugs/en/cybercrime/launderingproceeds/money laundering.html

Fondo Monetario Internacional. (2021). Cryptocurrency: A new challenge for monetary policy and financial stability. https://www.imf.org/en/Publications/WP/Issues/2021/06/15/Cryptocurrency-A-New-Challenge-for-Monetary-Policy-and-Financial-Stability-460536

Fondo Monetario Internacional. (2022). The rise of digital currencies: Implications for monetary policy and financial stability. https://www.imf.org/en/Publications/WP/Issues/2022/01/10/The-Rise-of-Digital-Currencies-Implications-for-Monetary-Policy-and-Financial-Stability-474029

Zohar, A. (2015). Bitcoin: Under the hood. Communications of the ACM, 58(9), 104-113. https://doi.org/10.1145/2701411

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? The Review of Financial Studies, 32(5), 1798-1853. https://doi.org/10.1093/rfs/hhz015

Gans, J. S. (2019). The case for an open digital currency. Harvard Business Review. https://hbr.org/2019/03/the-case-for-an-open-digital-currency

FBI. (2021). 2020 Internet Crime Complaint Center report. https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

U.S. Department of Justice. (2020). National drug threat assessment 2020. https://www.dea.gov/documents/2020/2020-10/national-drug-threat-assessment-2020

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. Journal of Economic Perspectives, 29(2), 213-238. https://doi.org/10.1257/jep.29.2.213

European Monitoring Centre for Drugs and Drug Addiction. (2021). Fentanyl and synthetic opioids in Europe. https://www.emcdda.europa.eu/publications/topic-overviews/fentanyl-and-synthetic-opioids-europe_en

Friedman, H. (2021). The impact of cryptocurrencies on the global drug trade. Journal of Drug Issues, 51(3), 450-467. https://doi.org/10.1177/0022042621998531

Friedman, J. (2022). Cryptocurrencies and the drug trade: A growing concern for law enforcement. Journal of Criminal Justice, 80, 101-109. https://doi.org/10.1016/j.jcrimjus.2021.101109

United Nations Office on Drugs and Crime. (2021). World drug report 2021. https://www.unodc.org/unodc/en/data-and-analysis/wdr2021.html

Mansfield, D. (2021). The dark side of digital currencies: How cryptocurrencies facilitate drug trafficking. International Journal of Drug Policy, 89, 102-110. https://doi.org/10.1016/j.drugpo.2020.102110

Zhang, B., & Wang, L. (2021). The role of blockchain technology in drug trafficking and money laundering: A review. Journal of Financial Crime, 28(4), 1014-1025. https://doi.org/10.1108/JFC-09-2020-0118

Baker, S. (2022). The intersection of crypto and crime: Understanding the challenges of regulation. Harvard Law Review, 135(4), 1205-1223. https://harvardlawreview.org/2022/02/the-intersection-of-crypto-and-crime-understanding-the-challenges-of-regulation/

Imagenes

Bitcoin.com. (2023). Tether lanzará el stablecoin USDT en el protocolo RGB de Bitcoin. [Imagen].https://news.bitcoin.com/de/tether-wird-den-usdt-stablecoin-auf-dem-bitcoin-rgb-protokoll-ausgeben/

TEMA 2:

LA INVERSIÓN EN CIBERSEGURIDAD. ¿UN ARMA DE DOBLE FILO O UNA NECESIDAD?

Contexto Histórico

Desde finales del siglo XX, el desarrollo acelerado de internet transformó profundamente la comunicación, la economía y la organización de los Estados. Lo que comenzó como una red experimental entre instituciones científicas se convirtió rápidamente en la base de servicios bancarios, sistemas gubernamentales, procesos democráticos y demás. A medida que la digitalización avanzaba, también lo hacían las amenazas y la manera de operar a consecuencia de los criminales: primero surgieron virus relativamente simples, ataques de curiosos y fraudes en línea; luego, con el año 2000, aparecieron grupos organizados capaces de coordinar operaciones globales, botnets masivas y herramientas diseñadas para infiltrarse en redes de amplia importancia a nivel nacional y/o económico. La ausencia de fronteras en el ciberespacio comenzó a generar desafíos legales y estratégicos para los Estados, que no estaban preparados para gestionar ataques que podían surgir desde cualquier parte del mundo en cuestión de segundos. Esto dio origen a los primeros debates sobre la necesidad de integrar la ciberseguridad en las políticas de defensa nacional, regular su uso y fortalecer la cooperación internacional. Debido a la ausencia de claras regulaciones internacionales, muchos Estados son incapaces de reaccionar debidamente a estos ataques cibernéticos, ya que no existen protocolos aprobados por lidiar con este tipo de situaciones. Esto resulta en que los ciberataques sean excesivamente peligrosos para la infraestructura digital, puesto que las respuestas de los países son normalmente tardías e inefectivas.

Hay de tener en cuenta las diferentes variaciones de las amenazas cibernéticas. El crimen cibernético es aquel perpetrado por individuos u organizaciones criminales las cuales quieren lucrarse de dichas actividades ilegales. Cosas como el lavado de activos digitales, o el uso de ransomware para obtener pagos para la liberación de información se asemejan mucho al

crimen común, con la diferencia de que son perpetrados a través de medios digitales. El ciberterrorismo es llevado a cabo por organizaciones terroristas nacionales e internacionales que buscan generar miedo o daños con tal de conseguir atención o debilitar al estado. Cosas como la filtración de datos confidenciales, la destrucción de servicios digitales esenciales u otros ataques que generan caos son normalmente clasificados como ciberterrorismo, ya que su objetivo no es generar ganancia, sino causar desorden para los Estados. Finalmente, el ciberconflicto entre estados se asemeja mucho al ciberterrorismo, pero también incluye un componente militar importante en el cual los países buscan conseguir una ventaja estratégica sobre sus oponentes al generar conmoción interior o debilitar sus fuerzas armadas. Este tipo de ataque cibernético es perpetrado exclusivamente por Estados, los cuales atacan la infraestructura digital de sus oponentes.

En este contexto global se inscribe el caso de Estonia en 2007, uno de los episodios más influyentes en la historia de la ciberseguridad moderna y la principal motivación a la inversión en esta misma. Estonia, tras independizarse de la Unión Soviética en 1991, emprendió un proceso de digitalización muy ambicioso que convirtió a su administración pública, banca y servicios cotidianos en algunos de los más automatizados y por consiguiente "dependientes" de internet en Europa. Sin embargo, esa fortaleza tecnológica también se transformó en vulnerabilidad política en medio de tensiones con Rusia. El conflicto surgió debido a la decisión del gobierno estonio de trasladar el monumento soviético conocido como el "Bronze Soldier" desde una plaza central de Tallin a un cementerio militar. La medida provocó protestas internas, ataques físicos, una fuerte reacción diplomática rusa y, a partir del 27 de abril de 2007, una serie de ciberataques masivos sin precedentes.

Durante semanas, Estonia sufrió ataques coordinados de denegación de servicio distribuida (DDoS), defacements y campañas de saturación contra servidores de instituciones públicas, medios de comunicación, bancos y proveedores de servicios esenciales. Los ataques sobrecargaron la infraestructura nacional, ya que este país con la reciente transformación y transición a un carácter mucho más tecnológico, tenía muchos más sistemas conectados a la red y por eso un posible ataque cibernético fue mucho más devastador comparado a lo que

podría suceder en algún otro país menos digitalizado. La infraestructura de Estonia, al ser completamente basada en la tecnología, fue dañada fuertemente y el país no podía prácticamente funcionar bien, obligando a aislar redes enteras y a colaborar con expertos de otros países. La complejidad y volumen de los ataques, procedentes de botnets distribuidas internacionalmente, dificultaron la atribución directa, pero el carácter político del conflicto y la coordinación demostrada llevaron a considerarlo un posible ejemplo temprano de guerra híbrida, la cual es caracterizada por el uso de estrategias bélicas convencionales combinadas con métodos menos comunes (ciberataques, presión económica, desinformación). El caso reveló la fragilidad de los Estados altamente digitalizados, la necesidad urgente de marcos legales internacionales y la importancia de invertir en capacidades de defensa cibernética. Como respuesta, Estonia impulsó dentro de la OTAN la creación del NATO Cooperative Cyber Defence Centre of Excellence en Tallin en 2008, marcando un antes y un después en la comprensión del ciberespacio como dominio estratégico. Desde entonces, este episodio se estudia como un hito que aceleró la institucionalización de la ciberdefensa, definió nuevas doctrinas y mostró que los conflictos del siglo XXI pueden desarrollarse sin disparar un solo tiro, pero con efectos reales sobre la vida cotidiana y la estabilidad política.

Situación Actual

Nuevas herramientas digitales facilitan nuevas formas de eficiencia, almacenamiento de datos, y recompilación de información. Sin embargo, cuando los países empiezan a depender excesivamente de los sistemas digitales, esto los deja vulnerables a ataques cibernéticos que pueden ser devastadores e increíblemente difíciles de rastrear. Debido a esto, muchos países han desarrollado sistemas y organizaciones dedicadas a rastrear, proteger, y prevenir ataques cibernéticos a los sistemas nacionales o del gobierno. A esta protección digita se le conoce como ciberseguridad.

En años recientes, se han detectado una infinidad de organizaciones criminales que utilizan las redes digitales y se aprovechan del anonimato para perpetrar ataques en contra de la

infraestructura digital pública de manera indiscriminada. El anonimato que caracteriza a muchos de estos sistemas digitales ha sido aprovechado por los actores ilegales para proteger sus identidades y transferir bienes y activos sin ser detectados por las autoridades estatales e internacionales, como los organismos regulatorios sujetos a la ONUDD Este mundo digital es propenso a actividades ilícitas como la evasión fiscal, "ransomware", e incluso la deshonestidad institucional. Por esta razón, las diferentes delegaciones y organizaciones deberán colaborar y compartir regulaciones y tecnologías para prevenir la expansión de estas actividades digitales irregulares.

Uno de los mayores problemas relacionados con el crimen digital es la poca atención que ha recibido la protección de sistemas digitales esenciales para los gobiernos. Muchos países en estado de desarrollo no tienen sistemas suficientemente avanzados y protegidos para resistir ataques cibernéticos coordinados que tienen como objetivo hacerse con datos sensibles, manipular archivos privados, u obtener información esencial para dichos gobiernos. Muchos de estos enemigos digitales se apoderan de sistemas y datos importantes para el funcionamiento de países u organizaciones, para después exigir pagos en criptomonedas que son imposibles de rastrear. Los incidentes de estos ransomwares a nivel mundial han aumentado de manera significativa en años recientes y, en muchos casos, los pagos exigidos para liberar los datos o sistemas capturados se han solicitado mediante criptomonedas y no han podido ser rastreados. Esta situación deja en evidencia la disparidad de tecnología entre los atacantes digitales en comparación con los sistemas de defensa gubernamentales, lo cual resulta en un entorno en el que estos quedan expuestos a ataques digitales constantes que ponen en riesgo la seguridad nacional. Especialmente considerando que las tecnologías de vanguardia han empezado a revertir los problemas del pseudonimato característico del blockchain, pero la mayoría de los países no cuentan con estas tecnologías que cada vez son más esenciales.

Otra parte importante del problema es la falta de adaptación institucional y estructural a las nuevas herramientas tecnológicas emergentes. Mientras que algunos países han avanzado en la creación de unidades y organizaciones dedicadas a la modernización digital, la mayoría no posee suficientes recursos, personal capacitado o herramientas tecnológicas para desarrollar

dichas soluciones. Muchos miembros del gobierno y la administración desconocen la mayoría de conceptos básicos de tecnologías como blockchain, comunicación digital, o minado de bitcoin, lo que los deja vulnerables ante amenazas digitales e incapaces de reconocer riesgos o responder adecuadamente ante incidentes de seguridad. De la misma manera, muchos expertos advierten que mayor regulación digital conlleva menos libertades para los ciudadanos, lo cual podría considerarse como una intromisión gubernamental y, por lo tanto, el nacimiento de un Estado vigía en las vidas privadas de sus nacionales. La ausencia de soluciones bien desarrolladas limita la habilidad de los países en desarrollo para investigar, rastrear, y capturar a los perpetradores detrás de redes de fraude, fondos ilícitos o campañas de desinformación coordinadas a través de medios digitales de comunicación. Si los gobiernos nacionales no desarrollan mejoras tecnológicas para enfrentarse a los enemigos digitales avanzados, seguirán sucediendo estas problemáticas de seguridad digital.

Por otro lado, la vulnerabilidad digital no solo pone en riesgo a los gobiernos e instituciones, sino también a los ciudadanos. Con el desarrollo del mundo digital, los consumidores están cada vez más expuestos a estafas, fraudes, y noticias falsas que representan riesgos en el mundo virtual. Mientras que el desarrollo tecnológico de bancos e instituciones financieras trae muchos beneficios relacionados con la eficiencia y accesibilidad, también representan un riesgo donde los criminales digitales se aprovechan del desconocimiento de los usuarios para hacerse con datos o fondos monetarios, lo cual es una clara violación de la privacidad garantizada de las víctimas de dichos crímenes. Por esta razón, otro componente importante de la ciberseguridad es la inversión en educación digital, un aspecto que no es trabajado en la mayoría de los sistemas educativos del mundo y representa una oportunidad para los actores ilegales de la era digital. La filtración de contraseñas o el robo de activos digitales ocurren gracias a que los perpetradores se aprovechan del desconocimiento de las víctimas, y las campañas de educación y seguridad digital pueden proveer la información al público para ser capaz de identificar y evitar estas situaciones.

Finalmente, ya que muchos de estos mecanismos digitales operan de manera descentralizada, es extremadamente difícil para los gobiernos nacionales regular y prevenir el crimen cibernético. Cosas como las criptomonedas o la comunicación digital operan de manera

internacional o privada, dificultando la intervención por un solo gobierno. Por esta razón, es importante estandarizar regulaciones sobre el crimen digital, garantizando la cooperación internacional como la ISO 27001 para rastrear y capturar a estos criminales que muchas veces operan desde países lejanos. La falta de regulación en algunos países atrae y facilita las actividades de los "hackers" que muchas veces perpetran ataques desde la seguridad del anonimato y el vacío legislativo. Debido a esto, hay que garantizar la eliminación de estos vacíos regulatorios que complican la seguridad digital de todos los países del mundo.

Caso de Estudio

Aunque se enfatiza la relevancia de las organizaciones y grupos criminales, los cuales se aprovechan de los vacíos regulatorios, también es verdad que muchos países han desarrollado divisiones cibernéticas dedicadas a interferir con la infraestructura digital de otras naciones. Un claro ejemplo de esto es Rusia, quienes acostumbran a desplegar ataques cibernéticos contra naciones vecinas. En la actualidad, Rusia utiliza su división digital para interferir con redes eléctricas, de comunicaciones, o de transporte en el conflicto contra Ucrania. Por otro lado, también han utilizado sus capacidades digitales para intervenir en los sistemas del parlamento estonio, así como los bancos, periódicos, ministerios o emisoras de Estonia durante una disputa por la reubicación del Soldado de Bronce de Tallin. Este se encuentra en el cementerio militar de Tallin, pero fue el centro de una gran controversia cuando el gobierno estonio decidió traerlo a este lugar desde su ubicación original a las afueras de la ciudad. Esta decisión causó revuelo en Estonia, pero más aún en Rusia. Debido a este desacuerdo, el gobierno ruso decidió lanzar una serie de ciberataques coordinados que serían recordados como los ciberataques rusos del 2007.

Como mencionado anteriormente, el gobierno ruso atacó infraestructura digital esencial para Estonia, desde redes bancarias y medios de comunicación hasta las propias plataformas del gobierno y el parlamento. Debido a la gran disparidad de desarrollo tecnológico entre Rusia y Estonia, estos últimos fueron incapaces de frenar o reducir la gravedad y el impacto de los

ataques. Y aunque el propósito de estos ciberataques de parte de países no tienen como propósito lucrarse con el robo de activos, igualmente generaron caos y confusión en Estonia, lo cual representa un riesgo muy importante en materia de seguridad para cualquier país que pueda ser víctima de dichos ataques.

Estos ataques fueron mayormente del tipo de denegación de servicio, donde los sistemas son desactivados o inhabilitados con el propósito de generar perdidas, confusión, o exigir condiciones a cambio de su liberación. En el caso de los ataques rusos, esto se hizo con metodologías como el "Ping flood", el cual inunda los sistemas con tanta información que estos terminan colapsando, o el uso de "botnets" que se dedican a enviar spam o mensajes repetidos al recibidor de la red, lo cual también abruma a los sistemas y los deja inoperables. Finalmente, también es importante aclarar que muchos de estos ataques no fueron perpetrados por las autoridades rusas, sino por muchos civiles habitantes de los dos países. Tomando en cuenta esto y el avance tecnológico de los últimos años, es posible deducir que uno de los mayores riesgos relacionados con la ciberseguridad es lo accesible y lucrativo que es para los criminales perpetrar sus ataques (debido a la emergencia de nuevos "mercenarios digitales" quienes son contratados por Estados para atacar la infraestructura digital de otra nación), lo cual fuerza a los sistemas de defensa digitales a ser robustos y extremadamente completos, ya que cualquier fallo u omisión puede ser descubierta y utilizada para lograr modificar o atacar los sistemas o plataformas.

Para evidenciar la relevancia y magnitud de este problema, también hay que referenciar a los ataques cibernéticos conocidos como "Titan Rain". Estos ataques, sufridos por los Estados Unidos en el 2003, causaron una filtración masiva de información confidencial relacionada con el espionaje y algunas de las instituciones más protegidas por el gobierno, como la NASA o Lockheed Martin. Aunque los Estados Unidos aseguran que estos ataques fueron el resultado de una intervención china, no hay pruebas contundentes que demuestren el origen de estas infiltraciones. Esto prueba que incluso los países con mayor desarrollo tecnológico están expuestos a un ataque cibernético, y que la ciberseguridad depende del mayor nivel de alerta constante para prevenir la filtración de información o datos sensibles a los perpetradores. Sin

embargo, es importante aclarar que por más que se invierta en ciberseguridad, es imposible eliminar el riesgo por completo, por lo cual los Estados también deben desarrollar planes de contingencia que les permitan recuperarse de posibles ataques ciberneticos que debiliten las instituciones esenciales.

Puntos Clave

- Importancia estratégica de invertir en ciberseguridad en Estados y empresas.
- Riesgo de que las capacidades defensivas se transformen en herramientas de vigilancia u ofensivas.
- Dependencia creciente de infraestructuras digitales críticas.
- Caso Estonia 2007 como ejemplo de vulnerabilidad nacional ante ataques DDoS masivos.
- Necesidad de cooperación internacional y marcos legales claros.
- Dificultad de atribuir ataques en el ciberespacio.
- Relevancia de la educación digital y la preparación institucional.
- Evolución de las amenazas: IA, ransomware, desinformación, ataques a la cadena de suministro.
- El balance entre la regulación digital y la privacidad de los usuarios.
- Los ataques cibernéticos como herramienta para debilitar estados y denegar el acceso a necesidades y derechos básicos.
- Importancia de protocolos de respuesta rápida y centros especializados (CERT, SOC).
- Impacto económico y reputacional de los ataques cibernéticos.

Preguntas Orientadoras

- ¿Debe priorizarse la seguridad digital aunque implique ceder parte de la privacidad?
- ¿Hasta qué punto la inversión en ciberseguridad puede convertirse en un arma política?
- ¿Qué responsabilidad tienen las grandes empresas tecnológicas en la defensa digital de un país?

- ¿La ciberseguridad debe considerarse un derecho, un servicio público o un asunto militar?
- ¿Qué límites deberían existir en el uso estatal de herramientas de vigilancia digital?
- ¿Cómo debería prepararse una sociedad altamente digitalizada frente a ataques masivos?
- ¿Cómo equilibrar seguridad digital y protección de derechos?
- ¿Cómo afecta sectores primarios como la salud o la economía?

Referencias

Lewis, J. A. (2007, 15 de junio). *Cyber Attacks Explained.* Center for Strategic and International Studies (CSIS). https://www.csis.org/analysis/cyber-attacks-explained

Ottis, R. (2008). *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective.* NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

"2007 cyber-attacks on Estonia." (s. f.). In *StratCom CoE.* https://stratcomcoe.org/cuploads/pfiles/cyber_attacks_estonia.pdf stratcomcoe.org

Davis, J. (2007, 21 de agosto). *Hackers Take Down the Most Wired Country in Europe.* WIRED. https://www.wired.com/2007/08/ff-estonia/

"Estonia: NATO's Brand New Center of Cyberwarfare Excellence." (2008, 30 de abril). *WIRED / Radio Free Europe.* https://www.wired.com/2008/04/estonia-natos-b/ wired.com+1

"The 2007 Estonian cyber attacks." (s. f.). *AFRINIC 11 Conference Presentation.* https://meeting.afrinic.net/afrinic-11/slides/aaf/Estonia_cyber_attacks_2007_latest.pdf meeting.afrinic.net

"Cyber defence." (2024, 30 de julio). NATO. https://www.nato.int/en/what-we-do/deterrence-and-defence/cyber-defence

Vollmer, B. (2021). *NATO's Mission-Critical Space Capabilities under Threat: Cybersecurity Gaps in the Military Space Asset Supply Chain.* arXiv. https://arxiv.org/abs/2102.09674

"Strengthening Cyber and Information Resilience in the Baltic Sea Region." (2025, 16 de octubre). BSPC. https://www.bspc.net/news/strengthening-cyber-and-information-resilience-in-the-baltic-sea-region

"Estonia: NATO CCD-COE — how cyber-defence cooperation makes cyberspace safer." (2018, 16 de octubre). E-Estonia. https://e-estonia.com/nato-ccdcoe-expertise-cyber-space-safer/

RECOMENDACIONES FINALES

Estimados delegados, para nosotros es extremadamente importante recalcarles los valores clave del modelo ONU; la cooperación, investigación, y honestidad académica deben verse reflejados en todo momento dentro del comité. En el momento de redactar sus portafolios, por favor no duden en contactarnos con cualquier duda al correo onudd.asobilca32@gmail.com donde estaremos pendientes para responder sus inquietudes.

La experiencia ONU está condicionada por el esfuerzo y la cooperación que generan resoluciones, así como recuerdos e inmensa satisfacción. Por esto, es importante que se involucren de lleno en su preparación, y eviten el plagio o la inteligencia artificial para que reemplace su pensamiento propio. Como dijimos anteriormente en la carta de bienvenida, esta es una oportunidad para desarrollarse profesional y personalmente, y nosotros estaremos aquí para apoyarlos y hacer del comité lo más productivo posible.