COLADE
XXXVIII CONGRESO LATINOAMERICANO DE DERECHO FINANCIERO

Los Ciberataques Internacionales: experiencias de investigación y acciones judiciales

Descargo de responsabilidades:
La información y los argumentos de esta presentación no necesariamente reflejan los puntos de vista de la Secretaría General de la Organización de los Estados Americanos (OEA) o de los gobiernos de sus Estados Miembros

Kerry Ann Barrett

Especialista en Políticas **de** Seguridad Cibernética
Organización de los Estados Americanos

kabarrett@oas.org
@OEA_cyber

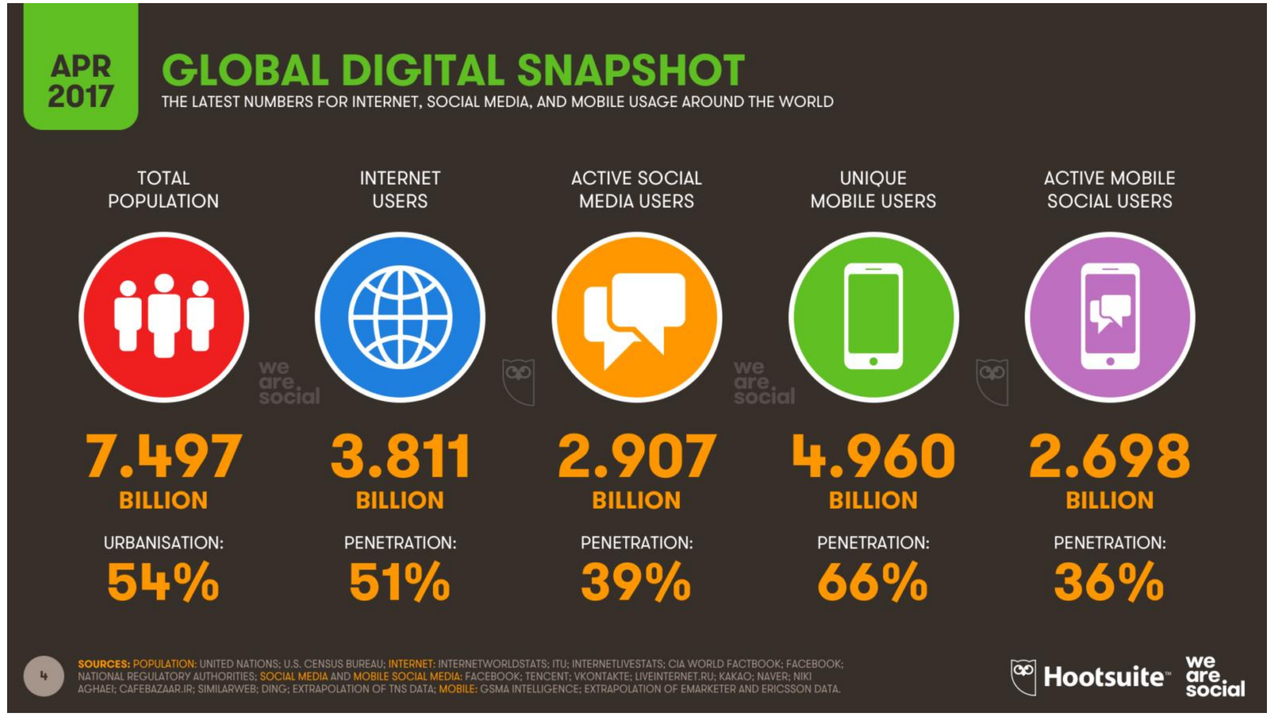
Panorama de amenazas en 2019

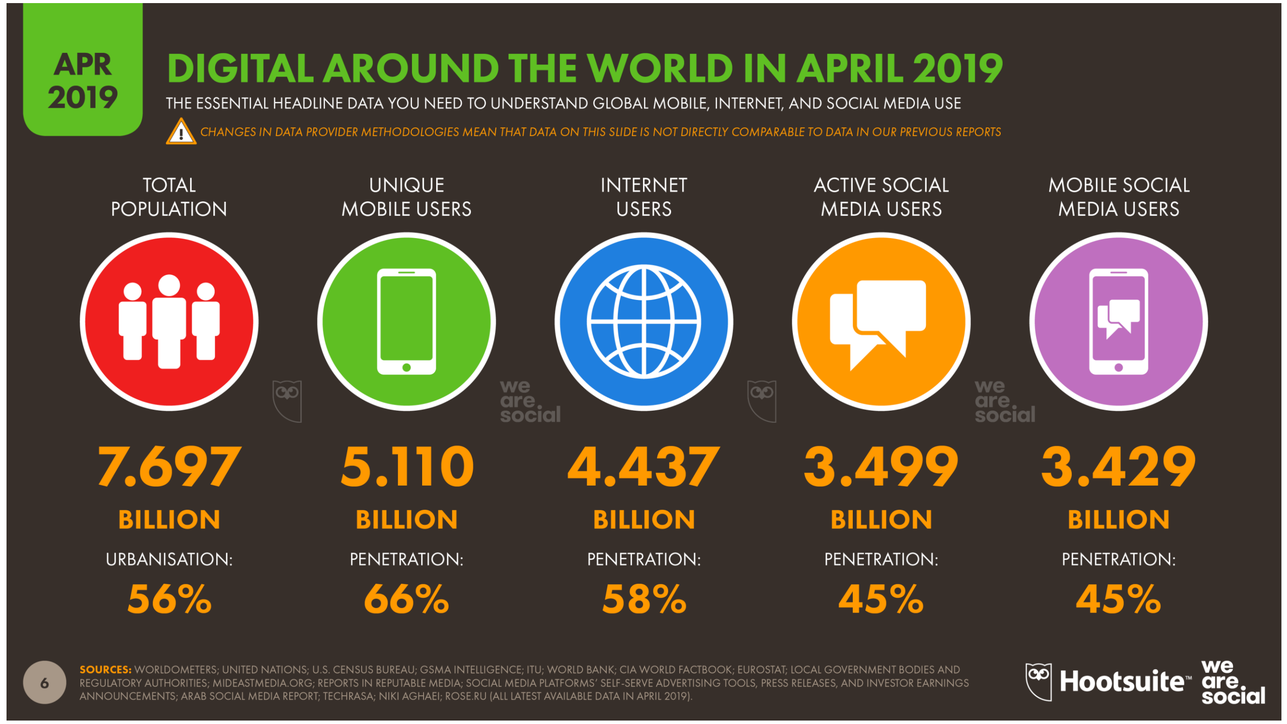
- Las tecnologías emergentes como la inteligencia artificial y 5G están creando mayores demandas de ciberseguridad y protección de la privacidad.
- Ciberseguridad Ventures, predice el cibercrimen costará el mundo más de $ 6 billones de dólares anuales para el año 2021, frente a los $ 3 billones en 2015.
- Hubo cerca de 4 mil millones de usuarios de Internet en 2018 (casi la mitad de la población mundial de 7,7 mil millones), frente a los 2 mil millones en 2015.
- ABI ha pronosticado que más de 20 millones de automóviles conectados se enviarán con tecnología de seguridad basada en software incorporada para 2020, y el proveedor español de telecomunicaciones Telefónica declara que para 2020, el 90 por ciento de los automóviles estarán en línea, en comparación con solo el 2 por ciento en 2012.

Fuentes: WEF, FOX and Cybersecurity Ventures

- Subinformación de delitos cibernéticos en todo el mundo
- Las principales amenazas provienen de grupos de ciberdelincuencia y piratas informáticos y de empleados internos no maliciosos
- Las organizaciones estructuradas con un CISO informan los niveles más altos de confianza en su capacidad para responder a un ataque, mientras que aquellas con un CIO más generalizado a cargo de la seguridad informan los niveles más bajos.
- Cybersecurity Ventures predice que una empresa será víctima de un ataque de ransomware cada 14 segundos para 2019, y cada 11 segundos para 2021.
- Se pronosticó que los costos globales de daños por ransomware superarán los $ 5 mil millones en 2017, más de 15 veces más que en 2015. Ahora se predice que los daños por ransomware costarán al mundo $ 11.5 mil millones en 2019 y $ 20 mil millones en 2021.

Visión global de internet





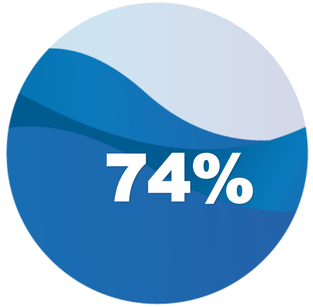
Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe

OEA
Más derechos para más gente

PRINCIPALES HALLAZGOS

- Bancos

Preparación y Gobernanza



Área única responsable

41%

Dos (2) niveles jerárquicos

72%

La junta directiva recibe reportes periódicos

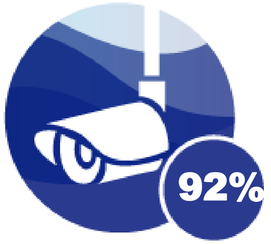
Detección y análisis de eventos

	Malware	Phishing	Clear Desk
	Grandes	Medianos	Pequeños
Identificación diaria de eventos de Malware	40%	28%	9%
% que no están implementando Tecnologías Digitales Emergentes	26%	44%	67%

PRINCIPALES HALLAZGOS

Bancos

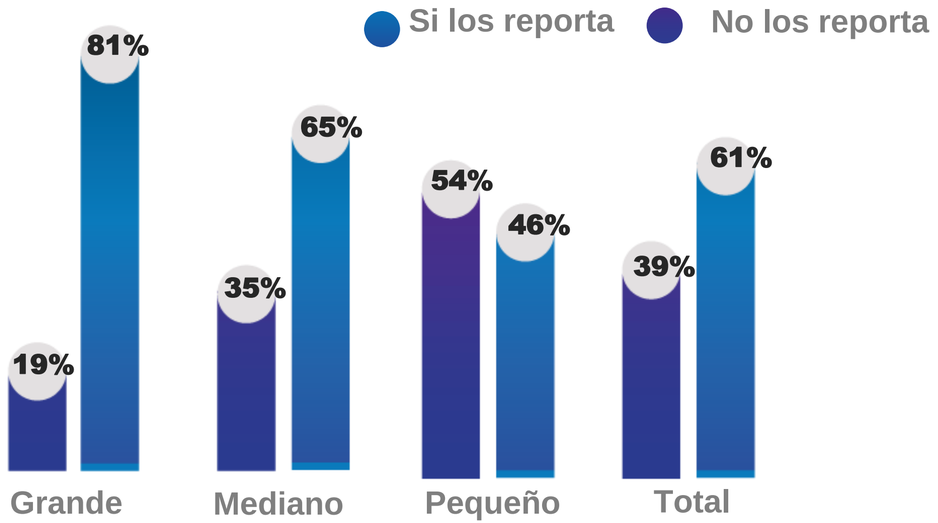
Gestión, respuesta y recuperación



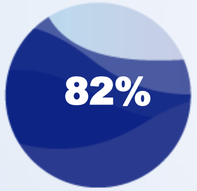
Identificaron algún tipo de evento
(ataques exitosos y ataques no exitosos)
de seguridad digital

Fueron víctimas de incidentes (ataques exitosos)

Reporte de incidentes



Capacitación y Concientización



Capacitaciones internas de información
Con planes de preparación, respuesta y capacitación
para sus empleados e Insourcing Bancarios

Las vulnerabilidades en la automatización del hogar y la Internet de las cosas

Los dispositivos IoT no solo recopilan datos valiosos del usuario. Podrían convertirse en un punto de entrada para un atacante o herramienta para lanzar un ataque distribuido de denegación de servicio (DDoS). Los dispositivos IoT no son seguros por diseño, ya que centrarse en la seguridad aumentaría significativamente los gastos de fabricación y mantenimiento.

(Fuente WEF, 2019)

https://www.weforum.org/agenda/2019/03/here-are-the-biggest-cybercrime-trends-of-2019/

Amenazas

- Flujo rápido de información y comunicación segura con los miembros del grupo criminal.
- Los ataques cibernéticos pueden dirigirse a los datos o tomar el control de los sistemas nacionales críticos (por ejemplo, la red eléctrica o el suministro de agua)
- Los ciberataques por lo general no permiten suficiente tiempo de detección o reacción
- Manipulación de las vulnerabilidades de día cero.
- Mercado cibernético negro y gris para el comercio de información sobre infraestructura crítica, credenciales de alto nivel, botnets, etc.

Amenazas

Los ataques cibernéticos se están volviendo cada vez más sofisticados y ahora son amenazas híbridas – una mezcla de planificación en línea/cibernética y ejecución cinética/física

No hay ninguna barrera física o puntos de control para escanear o evaluar el nivel de la amenaza.

El reclutamiento en línea ha aumentado. Por ejemplo, ISIS recluta en base a diferentes perfiles, diversos trasfondos y etnias, usualmente hombres de 26 años en promedio que completaron la secundaria o la universidad.

(Fuente: Seamus Hughes, Program on Extremism at George Washington University's Center for Cyber and Homeland)

Terminologías – sin consenso real

- El Departamento de Justicia de los Estados Unidos define el delito informático como "cualquier violación del derecho penal que implique un conocimiento de la tecnología informática para su perpetración, investigación o enjuiciamiento“.

- La Asociación de Jefes de Policía (ACPO) del Reino Unido ha definido el delito electrónico como: el "uso de computadoras en red, telefonía o tecnología de Internet para cometer o facilitar la comisión del delito“

- El Centro Australiano de Investigación Policial (ACPR) define los delitos electrónicos (cibercrimen) como: "delitos en los que una computadora se utiliza como herramienta en la comisión de un delito, como el objetivo de un delito, o como un dispositivo de almacenamiento en la comisión de un delito"

Terminologías – sin consenso real

- El Ciberterrorismo significa ataques premeditados y políticamente motivados por grupos sub-nacionales o agentes clandestinos, o individuos que esten contra los sistemas de información e informáticos, programas informáticos, y datos resultan en violencia contra objetivos no combatientes. El ciberterrorismo provoca miedo y daño a cualquier persona que se encuentre en el entorno donde se dirija el ataque. (Dogrul, Aslan , Celik 2011)

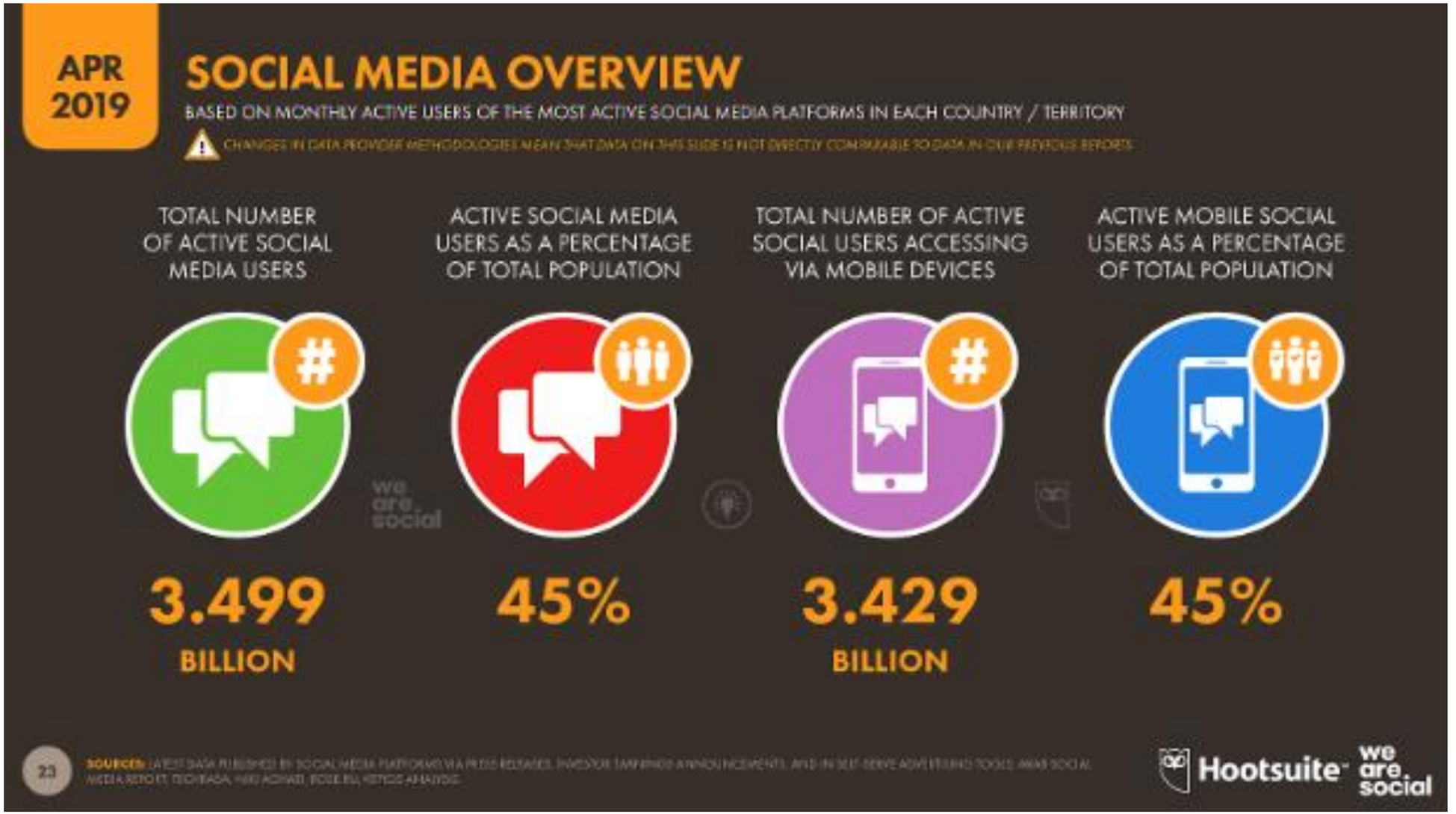
- La disuasión cibernética es evitar que un enemigo lleve a cabo futuros ataques al hacerlo cambiar de opinión, al atacar su tecnología, o por medios más palpables (como la confiscación, la terminación, el encarcelamiento, muerte o destrucción) (TJ Mowbray , Solution architecture for cyber deterrence," 2010)

- La Ciberdefensa está relacionada con la capacidad del Estado para prevenir y contrarrestar cualquier amenaza cibernética o incidente que afecte la soberanía nacional, incluyendo el uso de Internet con fines terroristas, actos de guerra cibernética y espionaje.

Perfil de los atacantes

Los atacantes, motivos y sus objetivos

Ingeniería social


APR 2019
SOCIAL MEDIA OVERVIEW
BASED ON MONTHLY ACTIVE USERS OF THE MOST ACTIVE SOCIAL MEDIA PLATFORMS IN EACH COUNTRY / TERRITORY
CHANGES IN DATA PROVIDER METHODOLOGIES MEAN THAT DATA ON THIS SLIDE IS NOT DIRECTLY COMPARABLE TO DATA IN OUR PREVIOUS REPORTS
TOTAL NUMBER OF ACTIVE SOCIAL MEDIA USERS
3.499 BILLION
ACTIVE SOCIAL MEDIA USERS AS A PERCENTAGE OF TOTAL POPULATION
45%
TOTAL NUMBER OF ACTIVE SOCIAL USERS ACCESSING VIA MOBILE DEVICES
3.429 BILLION
ACTIVE MOBILE SOCIAL USERS AS A PERCENTAGE OF TOTAL POPULATION
45%
we are social
Hootsuite
we are social

Estapas para investigar

Desarrollo de políticas y procedimientos

- ¿Qué constituye evidencia?
- ¿Dónde buscar evidencia?
- ¿Cómo manejarlo una vez que se ha recuperado?

Evaluación de evidencia

- Comprensión clara de los detalles del caso.
- El investigador debe definir los tipos de evidencia buscados (incluidas plataformas y formatos de datos específicos)
- Comprensión clara de cómo preservar los datos pertinentes.

Adquisición de evidencia

- Determine la fuente y la integridad de dichos datos antes de ingresarlos como evidencia
- Se necesita una amplia documentación antes, durante y después del proceso de adquisición.
- Asegure los dispositivos y obtenga órdenes judiciales
- Se debe registrar y preservar la información detallada, incluido todo el hardware y software utilizado en el proceso de investigación.

Examen de evidencia

- Los investigadores penales, abogados y otro personal técnico calificado deben trabajar en colaboración para garantizar una comprensión profunda de las complejidades del caso.
- Identifique los cargos apropiados (según el derecho consuetudinario existente y los estatutos estatales y federales) y determine qué información o evidencia adicional se necesitará antes de presentar los cargos

Fuente: University of Norwich

Consideraciones nacionales

Marcos legales y capacidad

Ley sustantiva

A. Un acto ilegal debe ser claramente descrito y prohibido por la ley. una persona no puede ser castigada por un acto que no fue prohibido por la ley en el momento en que la persona cometió el acto (UNODC, 2013, p. 53).

B. Las fuentes de la ley sustantiva incluyen los estatutos y ordenanzas promulgadas por las legislaturas de la ciudad, el estado y el gobierno federal (ley legal), las constituciones federales y estatales, y las decisiones judiciales y abordan "mens rea" y elementos del delito.

C. Por ejemplo, Alemania, Japón y China, han modificado las disposiciones pertinentes de su código penal para combatir el delito cibernético. Los países también han utilizado las leyes existentes que fueron diseñadas para la delincuencia del mundo real (fuera de línea) para atacar ciertos delitos cibernéticos y cibercriminales. Como otro ejemplo, en Iraq, el código civil existente (Código Civil Iraquí No. 40 de 1951) y el código penal (Código Penal Iraquí No. 111 de 1969) se utilizan para enjuiciar delitos del mundo real (por ejemplo, fraude, chantaje, identidad robo) perpetrado a través de Internet y tecnología digital.

Fuente: UNODC

Ley procesal

A. Procesos y procedimientos a seguir para aplicar el derecho sustantivo y las normas que permitan la aplicación del derecho sustantivo

B. La ley procesal del delito cibernético incluye disposiciones sobre jurisdicción y poderes de investigación, reglas de evidencia y procedimientos penales relacionados con la recopilación de datos, escuchas telefónicas, búsqueda e incautación, preservación y retención de datos.

C. Sin embargo, no todos los países exigen salvaguardas (es decir, el requisito de orden legal). En 2014, Turquía modificó la Ley 5651 de Internet para exigir a los proveedores de servicios de Internet que retengan los datos de los usuarios y los pongan a disposición de las autoridades que lo soliciten sin exigirles que primero obtengan una orden legal (por ejemplo, una orden judicial o una orden de allanamiento) para obtener estos datos. En Tanzania, la Ley de Delitos Cibernéticos de 2015 otorgó a la policía poderes de investigación excesivos e irrestrictos en el delito cibernético. En particular, la autorización policial es el único requisito para permitir la búsqueda e incautación de pruebas y para obligar a la divulgación de datos

Fuente: UNODC

¿Quién puede investigar?

Los primeros en responder en las investigaciones de delitos cibernéticos son responsables de "asegurar" la evidencia digital en la "escena" (la ubicación) de un delito cibernético (por ejemplo, este podría ser el objetivo o los objetivos del delito cibernético y / o la tecnología de información y comunicación utilizada para cometer ciberdelincuencia -dependiente y / o delito cibernético). Un primer respondedor puede ser un agente de la ley, un experto forense digital, un oficial de policía militar, un investigador privado, un especialista en tecnología de la información u otra persona (p. Ej., Un empleado de la fuerza laboral) que tenga la tarea de responder a incidentes de cibercrimen

Los agentes de justicia penal, como los agentes de la ley, los fiscales y los jueces, son responsables de la prevención, mitigación, detección, investigación, enjuiciamiento y adjudicación del delito cibernético. Las agencias específicas responsables de los casos de delitos informáticos varían según el país. En el Reino Unido, por ejemplo, más de una agencia investiga el delito cibernético, incluidas las agencias policiales regionales y la Unidad Nacional de Delitos Cibernéticos, que forma parte de la Agencia Nacional del Delito en Ecuador, la "Unidad de Investigaciones de Delitos Tecnológicos de la Dirección Nacional de la Judicatura y la policía de investigación es responsable de investigar el cibercrimen

Fuente : UNODC

Retos Identificados

A. Análisis del riesgo

B. Balance de políticas existentes.

C. Estructura clara de gobernanza y cooperación efectiva entre los actores

B. Balance de las Políticas Existentes

La ciberseguridad es parte del marco general de la política de seguridad nacional.

Tener en cuenta otras políticas nacionales ya desarrolladas que tienen alguna relación con seguridad cibernética.

Considerar las funciones y responsabilidades de entidades/departamento gubernamentales existentes encargados de llevar a cabo políticas, reglamentaciones de seguridad y ciberseguridad. Identificar superposiciones y lagunas.

Consideraciones internacionales

Cooperación y derecho internacional

¿Qué es la Ley Internacional y cuál es su relación con el ciberespacio?

La ley que rige el recurrir a la fuerza entre los estados (jus ad bellum) - En qué circunstancias pueden ciberoperaciones iguales a (a) una amenaza internacionalmente ilícita o el uso de "fuerza" , (b) un "ataque armado", justificando el uso de fuerza necesaria y proporcional en defensa propia, o (c) una "amenaza a la paz y seguridad internacional" o “una violación de la paz" sujeta a la intervención del Consejo de Seguridad de la ONU.

La ley de neutralidad - El uso de la infraestructura de telecomunicaciones de Estados neutrales con el propósito de efectuar ataques cibernéticos. Cuáles son las responsabilidades de los estados "neutrales" con respecto a los actores no estatales que llevan a cabo ataques desde adentro o a través de su territorio o infraestructura.

La ley de los conflictos armados (jus in bello) – Derecho Internacional Humanitario (DIH), “guerra cibernética" se debe distinguir de las zonas que no se rigen por el DIH, tales como la "cibercriminalidad".

UNIDIR, 2011

Aplicación del Derecho Internacional Humanitario

- El Grupos de Expertos Gubernamentales de las Naciones Unidas (GGE) en relación a los avances en la informatización y las telecomunicaciones en el contexto de la seguridad internacional, recomendó en el 2013 que "los esfuerzos del estado para hacer frente a la seguridad de las TIC deben ir mano a mano con respecto hacia los derechos humanos y las libertades fundamentales consagradas en la Declaración Universal de Derechos Humanos y otros instrumentos internacionales “

- Adicionalmente, el Consejo de Derechos Humanos de las Naciones Unidas, afirmó que" los mismos derechos que tienen las personas cuando no están en línea también deben protegerse en línea.

- No existe una definición acordada por unanimidad de la guerra cibernética, sin embargo, hay algunos borradores autorizados. El Manual 2.0 de Tallin distingue entre (a) los medios y (b) los métodos de guerra cibernética como: a) las armas cibernéticas y sus sistemas cibernéticos asociados; b) tácticas cibernéticas, técnicas y procedimientos por los cuales se llevan a cabo las hostilidades (Manual de Tallin, p. 452). El DIH solo será aplicable a una ocurrencia de guerra cibernética si el ataque ocurre durante o desencadena un conflicto armado. Es cuestionable si un ciberataque puede constituir el "uso de la fuerza" o un "ataque armado" para que se aplique el DIH.

Cooperación

Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (2000). Este tratado, también conocido como la ***Convención de Palermo***, obliga a los Estados partes a promulgar delitos penales nacionales que se dirigen a grupos delictivos organizados y a adoptar nuevos marcos para la extradición, la asistencia legal mutua y la cooperación policial. Aunque el tratado no aborda explícitamente el delito cibernético, sus disposiciones son muy relevantes.

Una "dimensión transnacional" de un delito de cibercrimen surge cuando un elemento o efecto sustancial del delito es otro territorio, o cuando parte del modus operandi del delito se encuentra en otro territorio - Convención de las Naciones Unidas contra la Delincuencia Organizada (UNODC)

- Tratados de extradición
- Asistencia Legal Mutua
- Información - comunicación de aplicación de la ley

Cooperación

- Convención sobre el delito cibernético (2001) También conocido como la Convención de Budapest, este es el primer acuerdo internacional destinado a reducir la delincuencia informática mediante la armonización de las leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación internacional.

- La Convención sobre Cibercrimen entró en vigencia el 1 de julio de 2004, y su estado al 22 de enero de 2009 es que ha sido firmada por 46 Estados y ratificada por 23, incluidos los Estados Unidos de América (como un estado no miembro del CoE), donde entró en vigor el 1 de enero de 2007, y los Países Bajos, donde entró en vigor el 1 de marzo de 2007.

    - Derecho penal sustancial

    - Derecho procesal

    - Reglas sobre cooperación internacional

- Estados miembros de la OEA que se han unido: Argentina, Canadá, Chile, Colombia, Costa Rica, República Dominicana, México, Panamá, Paraguay, Perú y Estados Unidos.

La cuestión de la jurisdicción

La jurisdicción tiene varias formas:

- jurisdicción para prescribir: la autoridad de un soberano "para hacer que su ley sea aplicable a las actividades, relaciones o estatus de las personas, o los intereses de las personas en las cosas por legislación, por acto ejecutivo u orden, por regla administrativa o por determinación una corte

- jurisdicción para juzgar, y

- jurisdicción para hacer cumplir.

Casos de Estudios

International cyber crime ring smashed after more than $530 million stolen

By **Ben Westcott**, CNN

Updated 2:09 AM ET, Thu February 8, 2018

Hackers from the Infraud Organization are accused of trying to steal billions of dollars worth of goods and services by US authorities

SEGURIDAD • Según el Grupo de Delitos Telemáticos

El cibercrimen, un delito con una impunidad de "casi el 100%" en España

DANIELA BAÑOS MAFUD
@dbanosm94
Madrid

Actualizado Sábado, 21 septiembre 2019 - **02:12**

La mayoría de los ciberdelitos son ejecutados por criminales que se encuentran en cuatro países: Rusia, Ucrania, Rumanía y Nigeria

Dos usuarios utilizando sus móviles DANIELA BAÑOS

La sociedad ha migrado de lo analógico a lo digital. Hemos depositado nuestras vidas en el ciberespacio -cuentas de banco, redes sociales, móviles...- y en este éxodo también se ha colado el crimen. De esta mutación nació el cibercrimen y heredó el ingrediente más peligroso de la delincuencia: la impunidad. Una impunidad que es "casi del 100%", afirma el jefe del **Grupo de Delitos Telemáticos** de la Guardia Civil, el teniente coronel **Juan Rodríguez de Sotomayor**, en una conversación con EL MUNDO.

ESTUDIO DE CASO

Vitek Boden, trabajaba para Hunter Watertech, una firma Australian que instaló equipo de alcantarillado SCADA (Supervisory Control And Data Acquisition - Sistema de Control y Adquisición de Datos) controlado por radio para el consejo del condado de Maroochy Shire en Queensland, Australia. Él solicitó un trabajo con el consejo del condado de Maroochy Shire y el Consejo decidió no contratarlo. En consecuencia, Boden decidió ajustar cuentas con el Consejo y su antiguo empleador. Empacó su coche con equipos de radio robados, conectados a una computadora. Él condujo alrededor de la zona en al menos 46 ocasiones del 28 de febrero al 23 de abril de 2000, emitiendo comandos de radio para el equipo de alcantarillado que ayudó a instalar. Boden causó que 800.000 litros de aguas residuales se derramaran en parques, ríos e incluso los terrenos de un hotel Hyatt Regency.

CASO: CYBER BERKUT (2015)

Un grupo de hackers rusos tomó responsabilidad por los ataques contra la página web oficial Alemana.

Un grupo que exigía que Alemania rompiera los lazos con Ucrania y detuviera el apoyo financiero y político para el gobierno en Kiev, la capital, se atribuyó la responsabilidad por el cierre de al menos dos sitios, el del canciller y el sitio web del Bundestag, o cámara baja del Parlamento.

El grupo CyberBerkut también se atribuyó la responsabilidad de derribar tres sitios web de la OTAN en una serie de ataques de denegación de servicio distribuidos, en los cuales los servidores quedan inundados con el tráfico hasta que colapsan.

ESTUDIO DE CASO

Russian Man Sentenced to 27 Years in U.S. Cybercrime Case

Mon, 04/24/2017 - 11:03am 2 Comments by Martha Bellisle, Associated Press

Igor Litvak, right, the attorney for Russian hacker Roman Seleznev, talks to reporters, Friday, April 21, 2017, in Seattle, following the federal court sentencing of Seleznev to 27 years in prison after he was convicted of hacking into U.S. businesses to steal credit card data. (Photo: AP/Ted S. Warren)

(2017) Un juez federal dictó la sentencia más larga jamás impuesta en los Estados Unidos por un caso de delito cibernético al hijo de un miembro del Parlamento ruso condenado por piratear más de 500 empresas estadounidenses y robar millones de números de tarjetas de crédito, que luego vendido en sitios web especiales.

Roman Seleznev fue sentenciado a 27 años de prisión y se le ordenó pagar casi $ 170 millones en restitución a los negocios y bancos que fueron víctimas de su plan de varios años.

ESTUDIO DE CASO

Hacker Alex Bessell jailed for cyber crime offences

18 January 2018 Share

Alex Bessell was arrested after an investigation by West Midlands Police

A computer hacker has been jailed for two years for committing thousands of cyber crimes, including attacks on Google and Skype.

(2018) Alex Bessell, de 21 años, de Aigburth, Liverpool, también fue condenado en el Tribunal de la Corona de Birmingham por otros delitos, incluido el lavado de dinero y una "tienda de piratas informáticos en línea".

La policía de West Midlands allanó su casa y encontró en su computadora 750 nombres y contraseñas de computadoras infectadas.

El investigador oficial Det Con Mark Bird dijo: "Este es uno de los enjuiciamientos por delitos cibernéticos más importantes que hemos visto, estaba ofreciendo un servicio en línea para cualquiera que quiera llevar a cabo un ataque web".

Aduanas y Protección Fronteriza

En mayo de 2019, un contratista de vigilancia de Aduanas y Protección Fronteriza de EE. UU. Sufrió una violación y los piratas informáticos robaron fotos de viajeros y placas relacionadas con aproximadamente 100,000 personas. El contratista con sede en Tennessee, afiliado de CBP desde hace mucho tiempo conocido como Perceptics, también perdió información detallada sobre su hardware de vigilancia y cómo CBP lo implementa en múltiples puertos de entrada de EE. UU.

CBP ha pasado las últimas dos décadas aumentando su uso de tecnologías de vigilancia fronteriza, y parece que no hay un final a la vista. Por ejemplo, la agencia quiere que los escaneos de reconocimiento facial sean estándar en los 20 principales aeropuertos de EE. UU. Para 2021. Pero los defensores de los derechos civiles y la privacidad dicen que estas iniciativas agresivas representan un peligro para los ciudadanos estadounidenses y la comunidad global en general.

Sistemas industriales

En 2019, una cepa destructiva llamada LockerGoga ha estado victimizando específicamente a las empresas industriales y manufactureras, a veces obligando a las plantas de producción a cambiar al control manual o al daño a largo plazo en sistemas que controlan equipos físicos. Por ahora, LockerGoga solo está siendo utilizado por delincuentes con motivación financiera.

Fraude de tarjeta de crédito

Las autoridades estadounidenses han acusado a 36 personas por robar más de $ 530 millones de víctimas en todo el mundo en una de las "mayores empresas de ciberfraude jamás procesadas".

Según la declaración del Departamento de Justicia, a marzo de 2017 había 10,901 miembros registrados de la Organización Infraud, que se dividieron en roles específicos.

Desde los "administradores" que supervisaron la planificación estratégica de la organización y aprobaron la membresía, hasta los "miembros" que utilizaron el foro Infraud para facilitar sus actividades criminales.

Los organismos encargados de hacer cumplir la ley de todo el mundo colaboraron en la investigación de Infraud, incluidos Italia, Australia, el Reino Unido, Francia y Luxemburgo, entre muchos otros.

(Fuente: CNN **https://www.cnn.com/2018/02/08/world/us-cyber-crime-ring-arrests-intl/index.html**

Recomendaciones y reflexiones

Los cibercriminales están utilizando herramientas más avanzadas y escalables para violar la privacidad del usuario, y están obteniendo resultados. Dos mil millones de registros de datos se vieron comprometidos en 2017, y más de 4.5 mil millones de registros se violaron solo en la primera mitad de 2018

(Fuente: WEF 2019)

La pregunta ahora es si los ataques cibernéticos realmente se pueden usar como una alternativa al conflicto cinético, como han propuesto algunos estudiosos de la guerra, o si solo sirven para intensificar el combate en el mundo real.

Lily Hay Newman (2019)
WIRED.com

FBI

Reconociendo la amenaza, el FBI ha producido una pagina web interactiva que pretende prevenir el reclutamiento para grupos extremistas. Tiene elementos similares a juegos, donde se hace click en imagenes para “liberar a la marioneta.” *FBI- de febrero de 2019* (https://cve.fbi.gov/home.html)

▲ The main screen of the FBI's Don't Be a Puppet online game on extremism, which was launched in February. Photograph: FBI

PREGUNTAS Y RESPUESTAS

Gracias