Análisis semanal 501: El cibercrimen y su conexión con el crimen organizado (26 de junio de 2023)

Tatiana Peña Sequeira

Desde la pandemia por COVID-19 se incrementó la dependencia a la infraestructura digital debido al aumento del uso del internet y la digitalización de los ámbitos profesionales y sociales[1] que se dio como respuesta al distanciamiento social. No obstante, esto no ha significado que todo su empleo fue de beneficio común, sino más bien que aumentó en todos los aspectos, incluso los criminales. La ampliación de la conectividad al Internet por parte de los ciudadanos, las empresas y el sector público, junto con el número exponencialmente creciente de dispositivos y sensores conectados como parte del Internet de los implementos tecnológicos, crean nuevas oportunidades para los ciberdelincuentes[2].

Conceptos de cibercrimen y crimen organizado

Los delitos cibernéticos son aquellos que solo pueden cometerse utilizando una computadora, redes informáticas u otra forma de tecnología de la información y las comunicaciones. De manera que los ya delincuentes toman e integran rápidamente nuevas tecnologías en su *modi operandi* o producen nuevos modelos de negocios a su alrededor, por lo que el uso de nuevas tecnologías tiene un impacto en las actividades delictivas en todo el espectro de la delincuencia grave y organizada[3].

De acuerdo con la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y sus protocolos del 2004, un “grupo delictivo organizado” está “estructurado de tres o más personas que exista durante cierto tiempo y que actúe concertadamente con el

propósito de cometer uno o más delitos graves (…) con miras a obtener, directa o indirectamente, un beneficio económico u otro beneficio de orden materia"[4]. Y es que, debido a la facilidad de entrada en el ciberdelito, el uso de herramientas y servicios cibernéticos por parte de los grupos delictivos tradicionales para mejorar o expandir sus capacidades se vuelve cada vez más común[5].

Tipos de cibercrimen

En ese caso, los grupos delictivos no solo hacen uso de las tecnologías para cometer delitos, que serían las "ciber-asistidas, porque sin Internet el delito aún ocurriría pero por otros medios de comunicación, o están "ciberhabilitadas", cuando son de larga data las formas de delincuencia, como el juego ilícito, los fraudes y la extorsión, que tienen un alcance global gracias a las tecnologías digitales y en red. Sino que también llevan a cabo ciberdelitos, que serían los delitos "ciberdependientes", como la piratería informática, la denegación de servicio distribuido y los ataques de *ransomware*, y el correo no deseado que desaparecen cuando se elimina Internet de la ecuación[6].

Y es que es importante destacar que sigue creciendo la cantidad de individuos que ofrecen el "crimen como servicio" o *Crime-asa-Service* (CaaS). Esto permite a los delincuentes operar su propio negocio delictivo de comercio en línea de bienes y servicios ilícitos sin necesidad de las infraestructuras mantenidas por los grupos delictivos organizados 'tradicionales', lo que hace que se convierta en un desafío clave para las economías y sociedades digitales. Entre estos, la explotación sexual en línea y el fraude con tarjeta no presente, están cada vez más impulsados por las ganancias. Así también es relevante mencionar el tráfico ilícito de migrantes, con un mercado criminal grande, rentable y sofisticado, comparable a los mercados de drogas en la Unión Europea[7], los cuales tienden a ser mercados donde los grupos delictivos organizados se concentran.

Cibercrimen organizado

Como se mencionaba, se ha determinado que los grupos delictivos organizados han utilizado la tecnología de la información y la comunicación para explotar nuevos mercados delictivos en línea. Además, estos grupos se han involucrado en delitos cibernéticos para facilitar también sus actividades delictivas organizadas por fuera del internet. Y, aunque el alcance de estos actos delictivos todavía se desconoce, se han creado tipologías sobre los vínculos entre delincuencia organizada y ciberdelincuencia basadas en el grado de implicación de los grupos en actividades en línea contrapuestas a las que se dan por fuera del internet. Al respecto, se identificaron tres tipos generales de grupos: el Tipo 1, en el cual se encuentran grupos que operan principalmente en línea y cometen delitos cibernéticos, ya sean estructurados o no. El Tipo 2 que son los que trabajan en línea y por fuera del internet, y de la misma manera cometen delitos y ciberdelitos. Y el Tipo 3, en los cuales se utiliza únicamente la tecnología de la información y la comunicación para facilitar los delitos fuera de línea [8]

Situación mundial de la ciberseguridad

La realidad es que, "la materialización de ciberincidentes es una constante de la rutina diaria y cotidianeidad de gobiernos, empresas o individuos"[9] de manera que el cibercrimen se ha convertido en un fenómeno mundial que afecta a todos los Estados, no tiene fronteras y la cantidad de posibles víctimas sigue aumentando con el crecimiento de la digitalización, toda vez que más ciudadanos, empresas, servicios públicos y dispositivos se encuentran conectados a Internet[10]. Es por esto que se han comenzado a dar discusiones sobre la soberanía, las estrategias, la responsabilidad y los intereses de los Estados para adaptarse a los "ataques contra la seguridad de los sistemas de las Tecnologías de la Información y las Comunicaciones (TIC) de gobiernos, administraciones públicas y empresas con alto valor estratégico"[11].

La ciberseguridad "ha roto la barrera de los silos técnicos y se encuentra en la intersección de múltiples disciplinas y áreas de políticas: acceso digital y conectividad, resiliencia, justicia penal, diplomacia, seguridad y defensa internacional, y economía digital y comercio"[12]. El Reporte de Ciberseguridad del 2020 del Banco Interamericano de Desarrollo afirma que los países de América Latina "han dado importantes pasos en el desarrollo y la eficacia de sus estrategias nacionales de seguridad cibernética, que también han servido como vehículos para mejorar la cultura y las prácticas nacionales de seguridad cibernética". Así también, rescata que varios países, entre estos Costa Rica, se han adherido al Convenio sobre Cibercrimen del Consejo de Europa que busca "promover una política penal común contra el cibercrimen, ofreciendo un marco común de legislación nacional y cooperación internacional"[13].

Reflexiones finales

Es necesario que los Estados pongan énfasis en la ciberseguridad tanto en lo privado como lo institucional, basándose en los estudios y convenios que ya existen, pero tomando en cuenta que el avance de las tecnologías solo se va a seguir dando con mayor rapidez. De manera que es importante "armonizar los esfuerzos de los Estados para aumentar su ciberseguridad e incentivar a los Estados para que cooperen en un campo que convencionalmente se consideraría un área relacionada con sus asuntos internos" principalmente porque "la estabilidad cibernética global se basa en la capacidad local y nacional de todos los países para prevenir y reaccionar ante incidentes cibernéticos e investigar y procesar casos de delitos cibernéticos"[14]. Lo anterior, pues los esfuerzos en temas de ciberseguridad como implementar nuevas leyes, campañas de educación y el monitoreo de los sitos que facilitan y promueven los servicios en los que participa el cibercrimen organizado[15] son necesarios para la lucha constante contra el cibercrimen y los grupos delictivos organizados.

Notas:

[1] Barmpaliou, N. (2020). Amenazas emergentes en ciberseguridad: implicaciones para América Latina y el Caribe. Reporte de Ciberseguridad 2020. Banco Interamericano de Desarrollo. https://publications.iadb.org/publications/spanish/viewer/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

[2] United Nations Office on Drugs and Crime. (2019). Cyber organized crime: What is it? https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html

[3] Unión Europea. (2017). Serious And Organised Crime Threat Assessment (SOCTA) https://www.europol.europa.eu/cms/sites/default/files/documents/report_socta2017_1.pdf

[4] Naciones Unidas, (2004) Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional y Sus Protocolos. https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-s.pdf

[5] Unión Europea. (2017). Serious And Organised Crime Threat Assessment (SOCTA) https://www.europol.europa.eu/cms/sites/default/files/documents/report_socta2017_1.pdf

[6] United Nations Office on Drugs and Crime. (2019). Cyber organized crime: What is it? https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/cyber-organized-crime_what-is-it.html

[7] Unión Europea. (2017). Serious And Organised Crime Threat Assessment (SOCTA) https://www.europol.europa.eu/cms/sites/default/files/documents/report_socta2017_1.pdf

[8] United Nations Office on Drugs and Crime. (2019). Cyber Organized Crime. Criminal groups engaging in cyber organized crime. https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/criminal-groups-engaging-in-cyber-organized-crime.html

[9] Aguilar, J. (2020). La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas. https://seguridadinternacional.es/resi/html/la-brecha-de-ciberseguridad-en-america-latina-frente-al-contexto-global-de-ciberamenazas/

[10]Union Europea. (2017). Serious And Organised Crime Threat Assessment (SOCTA) https://www.europol.europa.eu/cms/sites/default/files/documents/report_socta2017_1.pdf

[11] Villalba, A. & Corchado, J. (2017). Análisis de las ciberamenazas. Cuadernos de estrategia. https://dialnet.unirioja.es/servlet/articulo?codigo=6115622

[12] Barmpaliou, N. (2020). Amenazas emergentes en ciberseguridad: implicaciones para América Latina y el Caribe. Reporte de Ciberseguridad 2020. Banco Interamericano de Desarrollo. https://publications.iadb.org/publications/spanish/viewer/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

[13] Ibid

[14] Mikser, S. (2020). La necesidad de una respuesta armonizada a las amenazas de ciberseguridad: El camino a seguir. Reporte de Ciberseguridad 2020. Banco Interamericano de Desarrollo. https://publications.iadb.org/publications/spanish/viewer/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

[15] United Nations Office on Drugs and Crime. (2019). Cyber Organized Crime. Preventing and countering cyber organized crime. https://www.unodc.org/e4j/en/cybercrime/module-13/key-issues/preventing-and-countering-cyber-organized-crime.html