XXVII
TECMUN Jr.

Organización
Internacional de Policía
Criminal

“La palabra no fue dada al hombre. Él la tomó”
Louis Aragón

Delegado:

He estado en tu lugar antes, hace exactamente 2 años en este mismo comité. Al igual que tú, sentía temor y nervios y durante 2 días dudé de mi capacidad y de mis ideales hasta que las últimas tres sesiones algo en mí cambió. Decidí dar todo lo que tenía y a esforzarme al máximo, sin importar el resultado. El trofeo, la mención, el reconocimiento, nada de eso importaba más que demostrarme a mí que puedo cambiar el mundo. Con todo y eso, sí había una cosa que nunca perdí...la fe en mis acciones. Finalmente salí de ese modelo con un reconocimiento como Mejor Delegado representando a los Estados Unidos de América, pero mejor aún comprendí el verdadero potencial del ser humano, la fe y el esfuerzo que juntos, son poderosos. Estos tres días me complace ser partícipe del instrumento que cambiará tu manera de verte a ti mismo y a tu mundo. Es por ello que te invito a confiar en tu potencial, en tus ideas, tu perspectiva y tu historia. Te aseguro que todo lo que tengas para ofrecer al bienestar global es digno de ser escuchado y realizado. Desde que fui delegado de los Estados Unidos el mundo ha cambiado bastante, cada vez nuestra sociedad se ve envuelta en una ignorancia que crece a un nivel alarmante. La gente en todos lados no quiere ver y menos escuchar. Existe la pobreza extrema, la desigualdad, el abuso, la indignación y la peor de todas, la indiferencia. Te aseguro que en algún momento, tú también te has vuelto ciego ante estos problemas por miedo o por pereza. A partir de hoy tú tendrás la oportunidad de cambiar eso en nuestra sociedad. Este país requiere de que alces la voz y digas lo que pienses, pero nunca te quedes hasta ahí. El mundo no necesita de tu opinión pues está suplicando por tus acciones. Nunca ha existido un cambio en toda tu vida que no haya empezado desde lo más hondo de tu corazón. Durante estos 3 días tendrás uno de los poderes esenciales para marcar una diferencia, la oportunidad. Con ella tendrás la posibilidad de empujar al mundo al cambio que deseas, sin embargo te pido que mantengas tu mente abierta al cambio que desean tus semejantes y elijas sabiamente, puede que esta sea tu última oportunidad. Este poder no sirve si no existe iniciativa de tu parte, para hacer una realidad tu deseo. Tampoco es muy efectivo si trabajas solo, puede que tardes toda tu vida en lograr que se cumpla tu cambio, por ello debes cooperar con las visiones de otro y lograr lo imposible. Nuestros tiempos no son de competencia sino de cooperación. Por último lo más importante, esta oportunidad de la que te hablo es igual de fugaz que una estrella, aprovéchala bien. El mundo seguirá cambiando y todo depende de cómo aproveches tu oportunidad para que este cambie para bien o para mal. Si descuidas tu poder, si lo desaprovechas o si dejas de creer en que es esencial para el mundo, simplemente desaparecerá. Finalmente quiero decirte algo, de ahora en adelante confía en tu potencial. Aquel que no espera vencer, ya está vencido; es un hecho. Te diría que te deseo suerte pero no lo haré por dos razones. En primera, no la necesitas y en segunda, la suerte solo es para los mediocres y esa palabra no aplica para ti. No lo olvides, mereces ser escuchado, y mereces una oportunidad. Úsala sabiamente.

Armando Daniel Navarro Sánchez

Presidente de la Organización Internacional de Policía Criminal

XXVII TECMUN Jr.

Antecedentes de la Organización Internacional de Policía Criminal

La Organización Internacional de Policía Criminal (INTERPOL) fue creada en 1923 y es el mayor órgano policial del mundo. Tiene el objetivo de mantener la cooperación internacional para preservar la seguridad, por medio de la lucha contra el crimen, a través de la innovación. La INTERPOL tiene su sede en Lyon, Francia, además cuenta con siete oficinas regionales alrededor del mundo y una sede oficial ante la Organización de las Naciones Unidas y la Unión Europea. Actualmente, la INTERPOL está integrada por 194 países, los cuales reciben apoyo técnico, operativo, e informático por parte del organismo. Sus principales enfoques son la prevención y el combate a problemáticas que atenten contra el bienestar internacional, como terrorismo, ciber-delincuencia, tráfico de personas y bienes, peligro químico, entre otros. Dentro de sus propósitos, INTERPOL mantiene las relaciones de apoyo entre las organizaciones nacionales de policía. La Organización, puede brindar apoyo y asesoramiento estratégico para vigilar, controlar y promover acciones que estén dirigidas a eliminar situaciones de riesgo.

Tópico A

Medidas para mejorar los protocolos de defensa en Europa ante nuevas tendencias de ciberataques en la región

Por: Armando Daniel Navarro Sánchez

Antecedentes

El 12 de mayo de 2017, alrededor de 150 países fueron amenazados por uno de los ciberataques con mayor impacto en la historia, conocido como *WannaCry*. Este era un *ransomware*, cuyo fin era secuestrar información de las computadoras. *WannaCry* tenía la consigna de exigir una suma de dinero en un periodo determinado para así devolver el poder del ordenador al usuario. Como una consecuencia de este evento, más de 200,000 dispositivos fueron atacados a nivel mundial, de acuerdo con la Oficina Europea de Policía (EUROPOL). Este virus provocó que hospitales, aeropuertos, estaciones de tren, fábrica de automóviles, entre otros, se vieran gravemente afectados a causa de la suspensión de sus actividades. A pesar de que el virus fue detenido, se estima que los cibercriminales lograron recolectar alrededor de 140,000 dólares en *bitcoins*. Un mes después, surgió *Petya*, un ransomware propagado y ejecutado de forma similar a *WannaCry*.

Con la finalidad de evitar ataques de esta naturaleza, la Unión Europea (UE) creó un sistema de gobierno que permite imponer sanciones a los delincuentes que intenten o cometan un ciberataque que constituya una amenaza externa para el bloque. El marco jurídico, dirigido por el Reino Unido de Gran Bretaña e Irlanda del Norte y el Reino de los Países Bajos, también permitirá imponer sanciones por ciberataques perpetrados contra países no pertenecientes a Europa u organizaciones internacionales cuando atenten contra los objetivos de la política exterior y de seguridad común europea. El nuevo marco permite congelar los activos de los individuos y organizaciones gubernamentales afiliadas, así como prohibir la entrada al territorio europeo. Su objetivo es establecer una política de prevención continental enfocada en los ciberataques y de tal forma mejorar la resistencia de los países europeos ante esta problemática. A pesar de esto, el marco jurídico no ha mostrado resultados positivos hasta el momento lo cual provoca que este continente sea el blanco prioritario de los cibercriminales.

Protocolos de defensa ante ciberataques

Recientemente, la condición deficiente de ciberseguridad en Europa ha sido una amenaza constante para los usuarios de cualquier sistema electrónico, al igual que para la economía del continente, que ha corrido grandes riesgos debido a los ciberataques. Por ello, la Unión

Europea ha decidido tomar medidas de prevención, para evitar un ciberataque en cualquier país de Europa, los cuales le cuestan alrededor de 400,000 millones de euros cada año a la economía mundial. El Consejo Económico y Social Europeo (CESE), en conjunto con la Empresa Nacional de Innovación de Sociedad Anónima (ENISA) y la Agencia de Ciberseguridad de la UE, trabajaron en el Reglamento del Parlamento Europeo, destinado a prevenir crisis cibernéticas y mantener informados a los ciudadanos sobre estas. El documento declara que la ciberseguridad debe volverse una prioridad para asegurar la prosperidad y seguridad internacional, además de adquirir mayor relevancia para los responsables políticos del país en el cual el reglamento se lleve a cabo. Dicho protocolo coordina la lucha contra ataques informáticos, al realizar operativos e investigaciones que previenen incidentes cibernéticos en sectores fundamentales dentro de la economía y la sociedad europea.

La Comisión Europea es consciente de la deficiencia de conocimientos sobre la ciberseguridad, entre la población de Europa. Estudios han revelado que, al menos, 50 % de la ciudadanía continental está poco informada sobre las inminencias informáticas, y casi un 70 % de las empresas no conocen los riesgos a los que están expuestas. Este reglamento reconoce que se deben hacer mejoras en la seguridad y protección de datos de las empresas para que su aplicación sea totalmente efectiva. El CESE afirma que se debe mejorar la resistencia a ataques cibernéticos en los sistemas europeos, así mismo evaluar la preparación de los Estados Miembros para responder a un ataque. El documento también aconseja que la ENISA proporcione informes periódicos acerca de las acciones para prevenir y contrarrestar un ciberataque de los Estados Miembros. El alcance de este reglamento hace una extensión a aquellos ataques informáticos, maliciosos y criminalistas que pudieran significar una amenaza a la seguridad mundial.

El protocolo promueve un plan de acción de siete etapas para un ciberataque, desde la clasificación de una amenaza, hasta el cierre del protocolo de respuesta. Las medianas y pequeñas empresas deben garantizar su competitividad en lo relacionado con la economía digital. Por lo anterior, existe un sistema de respuesta a los ataques informáticos a gran escala, sin embargo, no se ha desarrollado por completo. La alta demanda del uso de internet, junto con el análisis avanzado de datos, modifica en su totalidad el modo de comunicación

entre empresas y usuarios. En consecuencia, este Reglamento busca aplicar las bases de una normativa de privacidad que se adapte a la tecnología actual. Las directivas que se planean establecer son: la creación de obligaciones gubernamentales en ciberseguridad, mejorar la cooperación estratégica en el bloque europeo, y crear un reglamentación única en el mercado digital. Su objetivo es homogeneizar en los sitios de navegación dentro de Europa la regulación legal en materia de protección de datos. El Reglamento señala que las empresas tienen la obligación legal de informarse acerca de los peligros cibernéticos y conocer formas efectivas de protegerse ante ellos. Por otra parte, este documento no ofrece ningún apoyo económico para que se mejoren los niveles de ciberseguridad en la Unión Europea.

Nuevas tendencias de ciberataques

Desde finales de 2017, los ciberdelincuentes han modificado las tácticas que utilizan para irrumpir en sistemas computacionales y robar, o encriptar, datos. En 2018, después de 25 años, reapareció una técnica llamadas *Living of the Land* (LotL). Esta técnica consiste en utilizar aplicaciones, procesos naturales del equipo electrónico y archivos seguros ya descargados, para aprovecharlos como una puerta de entrada y salida para cualquier *malware*. Cuando el virus logra implantarse en un sistema seguro, puede comenzar a robar datos dentro de una red local. Los ataques de LotL aprovechan el movimiento común de datos para esconderse y dirigir sus acciones, lo que dificulta su detección por los antivirus y los usuarios. Esta técnica es muy fácil de conducir y utilizar para los cibercriminales.

LotL había dejado de ser un peligro en 2010, pues el número de ataques que se registraron en Europa en ese año fueron solamente 20. Los sistemas informáticos que se utilizaban en aquel año hacían que los virus quedarán expuestos, al no poderse esconder entre los archivos. Su desaparición, por casi 8 años, permitió que el método LotL se perfeccionara debido a que se adaptó a las nuevas vulnerabilidades de los usuarios, como la utilización de la nube, el envío de archivos por vía *Bluetooth*, la edición de documentos en línea, el amplio uso de archivos de respaldo y la inseguridad en las herramientas de *Windows* 10. Estos procedimientos de trabajo son lo que ha dado paso a la nueva amenaza para la ciberseguridad. *Living of the land* implica una nueva era de inseguridad para los sistemas informáticos, al comprometer la privacidad y el bienestar de los usuarios.

Diversos grupos de ciberterrorismo han comenzado a aprovechar esta vulnerabilidad para lanzar diferentes programas maliciosos con intenciones de lucro, espionaje, destrucción o interferencia. La tendencia de LotL vuelve más complicado identificar un ataque dirigido, pues todos los grupos dedicados a esto pueden ser sospechosos. Su utilización ha aumentado desde finales del año pasado, cuando se registraron ciberataques dirigidos al sector de telecomunicaciones y defensa en los Estados Unidos de América y la República Popular China. A pesar de la situación actual, aún no hay un programa realmente efectivo para interceptar los ataques perpetrados con LotL. Existen varias empresas que han resultado seriamente afectadas por la problemática, perdiendo grandes cantidades de recursos económicos, a causa del robo de datos de LotL. Cada mes, el número de ataques registrados crece y los ciberdelincuentes adquieren más capital para sus operaciones internacionales.

Formjacking

Estos ataques son fáciles de ejecutar, ya que consisten en cargar un código infectado en una página de compra en línea para que los usuarios, al llenar datos personales y financieros, inconscientemente envíen su información a una red cerrada, controlada por cibercriminales. Actualmente, es la forma más lucrativa para financiarse que utilizan los grupos de ciberterroristas, afectando a más de 4,800 sitios de internet cada mes, en lo que va de 2019. Empresas, como *British Airways* y *Ticketmaster*, fueron gravemente afectadas el año pasado, perdiendo alrededor de 17 millones de dólares americanos, en el caso de aerolínea británica. El *Formjacking* se utiliza, también, para vender datos en la red oscura, lo que compromete la seguridad de los usuarios y de su privacidad. En primera instancia, no se puede saber si un sitio web está infectado con este virus, debido a que no existen signos que delaten esta infección. El *malware* utiliza el lenguaje de programación para navegadores web, *JavaScript,* para secuestrar servidores de sitios de navegación. *Formjacking* se aprovecha de las vulnerabilidades que puedan tener los navegadores dentro de su programación, lo cual hace que desactivar *Java,* para evitar un hackeo, solo sea útil para el 5% de los usuarios. La corporación dedicada al desarrollo de *softwares* para seguridad informática, la protección de datos y el análisis de amenazas a la seguridad informática, *Symantec* mencionó que bloqueó más de 3.7 millones de intentos de *Formjacking* en diciembre de 2018*,* aunque también asegura que esa cifra solo fue 40 % de los ataques registrados en esa temporada.

El peligro del *Formjacking* no se remite únicamente a sitios de venta en línea y negocios pequeños y medianos. Con el caso de *Facebook* y *Cambridge Analytica* del año pasado, donde la información de 87 millones de usuarios fue utilizada indebidamente por varias aplicaciones, los ciberdelincuentes tienen la posibilidad de vender información sobre cuentas, correos y eventos que encuentren en los perfiles de cualquier red social. Los dispositivos inteligentes también son un blanco para el cibercrimen, ya que, es la forma más completa y efectiva de espionaje, al contar con un rastreador de ubicación, una cámara y un micrófono. Si bien, los sistemas de defensa en los dispositivos móviles son efectivos, no se sabe con certeza si podrían detectar técnicas de LotL dentro de su sistema operativo. En 2018, en Norteamérica, se registró un incremento del 60 % de dispositivos móviles que fueron hackeados por completo a causa de programas cargados en ligas de internet.

Ransomware* y *Cryptojacking

Después del caso de *WannaCry*, los ataques de tipo *ransomware* han disminuido exponencialmente. Estos virus secuestran los archivos de una computadora para, luego, exigir un rescate que se debe pagar en criptomonedas; aunque, en la mayoría de los casos, pagar el rescate resulta inútil. *Petya* es otro virus que no cifra los archivos, sino que impide el acceso al disco duro, por completo, cifrando la tabla maestra de archivos (MFT). Esto ocasiona que de ninguna forma el sistema pueda leerse ni operar correctamente (Natour, 2017). Su disminución, durante 2018, se debe al poco valor monetario que han adquirido las criptomonedas, además de que los usuarios comenzaron a respaldar sus datos en la nube. Los cibercriminales ya no obtienen utilidad al realizar ataques como este, sin embargo, algunos grupos siguen lanzando este tipo de virus y modificando su programación. El objetivo de estos programas maliciosos, después de lo ocurrido en 2017, comenzó a concentrarse en compañías trasnacionales. Los informes de diversas empresas de seguridad informática indican que el 81 % de los ataques en 2018 iban dirigidos a esta clase de empresas. Los sistemas ahora pueden detectar, con mayor facilidad, correos o archivos descargables que están infectados con un *ransomware*. Esto también implica que ya no se elaboran actualizaciones preparadas contra códigos modificados de este virus. La falta de dichas actualizaciones puede llevar dentro de unos años a otra gran crisis similar a la de *Petya* y *WannaCry.*

Como fue mencionado, uno de los mayores obstáculos de estos virus es la nube. Los usuarios, al tener sus archivos cargados en un sitio de respaldo, ya no deben preocuparse por pagar un rescate para recuperarlos de su sistema de cómputo. Aún con ese respaldo, existe un gran riesgo de perder control sobre su información, debido a que, la nube también es vulnerable ante ataques de *hackers*. Al estar conectada a un servidor de Internet, resulta más sencillo cargar un virus malicioso y capturar información distribuida, dentro del almacenamiento de la nube. Los programas de robo convencionales solo logran capturar un pequeño porcentaje de datos ya que, al moverse entre ellos, son detectados por los antivirus del equipo electrónico. A pesar de eso, los programas cargados con LotL se pueden mover con total libertad junto con los archivos que lleve la nube. Esto vuelve especialmente inseguras a las redes locales dentro de las compañías, poniendo en riesgo sus recursos y su información.

Acciones de la INTERPOL ante las nuevas tendencias de ciberdelincuencia.

La INTERPOL está encargada de garantizar y proteger la ciberseguridad a nivel internacional. La Organización ayuda a coordinar y supervisar operaciones trasnacionales sobre ciberdelincuencia, además de brindar información y capacitación a las fuerzas policiales para desmantelar redes cibercriminales. Bajo la problemática internacional que ocasionan las nuevas tendencias del cibercrimen, la INTERPOL ha creado la Estrategia Mundial contra la Ciberdelincuencia 2016-2020. Uno de los principales objetivos de esta táctica, es abordar la ciberdelincuencia pura. Este nombre refiere a los delitos que se cometen contra ordenadores y sistemas de información con el propósito de acceder a los datos de equipos electrónicos sin autorización. La estrategia, en principio, evalúa y analiza las amenazas, para poder acceder a la programación del virus. Posteriormente, un equipo de análisis forense digital gestiona las pruebas electrónicas, con el fin de encaminar a la investigación y el enjuiciamiento de los grupos criminales. De esta forma, el equipo forense recopila pistas informativas legales con patrones de grupos cibercriminales, idioma de programación y posicionamiento de ordenadores para llevar a cabo la conservación de pruebas y hacerlas comprensibles y lógicas para ser utilizadas por el sistema judicial.

La ciberdelincuencia involucra situaciones y términos que apenas existían hace diez años, lo que provoca que la sociedad aún no comprenda la gravedad del problema y busque

formas de solucionarlo. La INTERPOL tiene la facilidad de crear grupos especializados que puedan asesorar a las delegaciones para enriquecer la cantidad y calidad de datos con la intención de analizar la información de todo tipo obtenida de sus operaciones policiales. Desde 2013, la Organización implementa una conferencia anual, en la que se reúnen expertos en cibernética de todo el mundo, incluidos socios del sector privado, Organizaciones No Gubernamentales (ONG) y Equipo de Respuestas ante Emergencias Cibernéticas (CERT, por sus siglas en inglés). Su objetivo es discutir sobre las amenazas cibernéticas que impliquen un riesgo para la comunidad internacional y analizar formas efectivas para combatirlas. Asimismo, en 2018, la conferencia: Esfuerzos globalizados para combatir el crimen cibernético, formó parte de la semana de seguridad cibernética de Singapur, en la que se realizó diversos eventos relacionados con la lucha contra la ciberdelincuencia. La conferencia se enfocó en discutir las amenazas del cibercrimen en 2018, dominio del Internet y el negocio del cibercrimen. El realizamiento de estos eventos aumenta la cantidad de información que existe en el mundo acerca del cibercrimen, además de ayudar a los gobiernos en su preparación para evitar los daños de una crisis tecnológica. La INTERPOL, por su parte, actualiza sus programas policiales y bases de datos de cibercrimen, a través de estas conferencias y, de este modo, también propicia la cooperación de las fuerzas policiales, internacionalmente.

La INTERPOL tiene la capacidad de coordinar operaciones transnacionales a gran escala para desmantelar y detectar grupos de ciberdelincuentes. La finalidad de estos operativos es mantener la seguridad internacional, pero también fomentar la cooperación entre Estados, ONGs y asociaciones públicas. Un ejemplo de esto fue la operación ASEAN, de 2017, realizada en el Complejo Global para la Innovación de la INTERPOL (CGII), en Singapur. ASEAN reunió investigadores de varias naciones de la región asiática -tal como la República Popular China, el Reino de Tailandia y la Federación de Malasia-, al igual que expertos de compañías del sector privado como *Kaspersky Lab, Cyber Defense Institute, British Telecom, Palo Alto Network*, entre otros. La información brindada por el sector privado, combinada con los ataques registrados por los países, permitió que un equipo de analistas de la INTERPOL elaborara 23 reportes de ciberactividad en los que se identificaron amenazas potenciales y recursos necesarios para neutralizarlas. Se encontraron alrededor de 270 sitios de internet infectados con un código malicioso que obtenía información personal

de los usuarios y la enviaba a un servidor encriptado localizado en la República Federal de Nigeria. Esta operación es uno de los ejemplos más claros del resultado de la cooperación internacional entre el sector público y privado, apoyada por las capacidades de la Organización.

Actualmente, la INTERPOL ha aumentado su participación en el continente europeo a causa de la vulnerabilidad en la red a la que se expone la región. Los gobiernos europeos, a su vez, han comenzado a llevar una relación más estrecha con la Organización. Desde 2014, el uso de las bases de datos de la INTERPOL sobre ciberdelincuencia ha aumentado un 200 %, lo que ocasiona un aumento en el número de detenciones criminales relacionados con la ciberdelincuencia y otros delitos. Más de 60 criminales buscados por la INTERPOL han sido detenidos en Europa en los últimos cuatro años. Europa es considerada por la Organización como una región fundamental para el funcionamiento efectivo de la misma, por tanto, se deben fortalecer las relaciones de intercambio de datos y coordinación de operaciones entre la región europea y la INTERPOL.

Referencias

1. Agencia Estatal. (2018). REGLAMENTO (UE) 2016/679. Recuperado el 18 de junio de 2019, de *Diario Oficial de la Unión Europea*. Web. <https://www.boe.es/doue/2016/119/L00001-00088.pdf>

2. BBC Mundo. (2017). Ciberataque masivo: ¿quiénes fueron los países e instituciones más afectados por el virus WannaCry? Recuperado el 18 de junio de 2019, de *BBC NEWS*. Web.<https://www.bbc.com/mundo/noticias-39929920>

3. Consejo de la Unión Europea. (2019). Reforma de la ciberseguridad en Europa. Recuperado el 18 de junio de 2019, de *Consejo de la Unión Europea*. Web. <https://www.consilium.europa.eu/es/policies/cyber-security/>

4. Diario Oficial de la UE. (2018). Corrección de errores del Reglamento. Recuperado el 18 de junio de 2019, de *Diario Oficial de la Unión Europea.* Web. <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679R(02)&from=EN>

5. FIDE. (2017). La estrategia de la Unión Europea ante las amenazas cibernéticas. Recuperado el 18 de junio de 2019, de *El Confidencial*. Web. <https://blogs.elconfidencial.com/espana/blog-fide/2017-12-07/la-estrategia-de-la-union-europea-ante-las-amenazas-ciberneticas_1488593/>

6. Fundación Mapfre. (2019). El nuevo reglamento es clave para elaborar y revisar los protocolos de ciberseguridad. Recuperado el 18 de junio de 2019, de *Fundación Mapfre*. Web. <https://noticias.fundacionmapfre.org/reglamento-ciberseguridad-de-las-empresas/>

7. Hideout, B. (2018). Protocolo (Ciberseguridad). Recuperado el 18 de junio de 2019, de *Glosario Servidor*. Web. <https://glosarios.servidor-alicante.com/ciberseguridad/protocolo>

8. INTERPOL. (2017). Apoyo a la investigación sobre la ciberdelincuencia. Recuperado el 25 de junio de 2019, de *INTERPOL.* Web.<https://www.interpol.int/es/Delitos/Ciberdelincuencia/Apoyo-a-la-investigacion-sobre-ciberdelincuencia>

9. INTERPOL. (2018). El uso de las bases de datos de Interpol en Europa aumenta en más de un 200 %. Recuperado el 24 de junio de 2019, de *INTERPOL.* Web. <https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2018/El-uso-de-las-bases-de-datos-de-INTERPOL-en-Europa-aumenta-en-mas-de-un-200>

10. INTERPOL. (2018). Estrategia mundial contra la ciberdelincuencia. Recuperado el 25 de junio de 2019, de *INTERPOL.* Web. <https://www.interpol.int/es/content/download/5586/file/Summary_CYBER_Strategy_2017_01_SP%20LR.pdf>

11. INTERPOL. (2017). INTERPOL-led cybercrime operation across ASEAN unites public and private sectors. Recuperado el 25 de junio de 2019. de *INTERPOL*. Web. <https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2017/INTERPOL-led-cybercrime-operation-across-ASEAN-unites-public-and-private-sectors>

12. INTERPOL. (2018). 6th INTERPOL-Europol Cybercrime Conference. Recuperado el 24 de junio de 2019, de *INTERPOL.* Web. <https://www.interpol.int/es/Noticias-y-acontecimientos/Eventos/2018/6th-INTERPOL-Europol-Cybercrime-Conferences>

13. Jaimovich, D. (2018). Cómo surgió y se propagó WannaCry, uno de los ciberataques más grandes de la historia. Recuperado el 18 de junio de 2019, de *Infobae*. Web. <https://www.infobae.com/america/tecno/2018/05/12/como-surgio-y-se-propago-wannacry-uno-de-los-ciberataques-mas-grandes-de-la-historia/>

14. Jara, J. (2019). Facebook mostrará la información usada de los usuarios. Recuperado el 16 de junio de 2019, de *Digital Trends ES.* Web. <https://www.google.com/amp/s/es.digitaltrends.com/sociales/facebook-analytica-datos-personales/%3famp>

15. Jiménez, J. (2019). Qué es el formjacking y cómo pone en peligro tu información y tus datos. Recuperado el 16 de junio de 2019, de *Redeszone*. Web. <https://www.google.com/amp/s/www.redeszone.net/2019/03/25/que-es-formjacking-datos-bancarios/amp/>

16. López, C. (2018). ¿La ciberseguridad es algo más que protección?. Recuperado el 18 de junio de 2019, de *Ciberseguridad de EY LATAM*. Web. <https://www.ey.com/Publication/vwLUAssets/EY-library-la-ciberseguridad-es-algo-mas-proteccion/%24File/EY-library-la-ciberseguridad-es-algo-mas-proteccion.pdf>

17. Luján, J. (s.f). ¿Qué es WannaCry?. Recuperado el 17 de junio de 2019, de *EDTeam*. Web. < https://ed.team/blog/que-es-wanna-cry>

18. Natour, L. (2017). Petya, el virus protagonista de la segunda ola mundial de ciberataques. Recuperado el 16 de junio de 2019, de *ABC Redes*. Web. <https://www.abc.es/tecnologia/redes/abci-petya-virus-protagonista-segunda-mundial-ciberataques-201706280129_noticia.html>

19. Notimex. (2019). Formjacking, nueva estrategia de cibercriminales. Recuperado el 15 de junio de 2019, de *El economista*. Web. <https://www.google.com/amp/s/www.eleconomista.com.mx/amp/finanzaspersonales/Formjacking-nueva-estrategia-de-cibercriminales-20190226-0128.html>

20. Open Europe. (2019). Cómo mejorar la Ciberseguridad. Recuperado el 17 de junio de 2019, de *openexpo europe*. Web. <https://openexpoeurope.com/es/mejorar-ciberseguridad-organizaciones/>

21. Palazuelos, F. (2017). Petya, un virus más peligroso y sofisticado que WannaCry. Recuperado el 17 de junio de 2019, de *EL PAÍS*. Web. <https://elpais.com/tecnologia/2017/06/28/actualidad/1498639459_556568.html>

22. Press Europa. (2019). La UE aprueba un régimen para sancionar ciberataques. Recuperado el 17 de junio de 2019, de *Europa press*. Web. <https://www.europapress.es/internacional/noticia-ue-aprueba-regimen-sancionar-ciberataques-20190517121456.html>

23. Protección Datos. (2018). La UE aprueba un nuevo protocolo de Ciberseguridad. Recuperado el 17 de junio de 2019, de *Ayuda ley protección de datos*. Web. <https://ayudaleyprotecciondatos.es/2019/03/28/ue-protocolo-ciberseguridad/>

24. Symantec. (2019). Formjacking the new get rich quick scheme for cybercriminals. Recuperado el 15 de junio de 2019, de *Symantec*. Web.<https://interactive.symantec.com/istr24-web>

25. Symantec. (2019). Internet Security Threat Report. Recuperado el 15 de junio de 2019, de *Symantec*. Web. <https://www.symantec.com/es/es/security-center/threat-report>

26. Symantec. (2018). Thrip: Espionage Group. Recuperado el 15 de junio de 2019, de *Symantec*. Web. <https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets>

27. Symantec. (2018). What is Living of the Land? Recuperado el 15 de junio de 2019, de *Symantec*. Web. <https://medium.com/threat-intel/what-is-living-off-the-land-ca0c2e932931>

A

Activo: Valor total de lo que posee una sociedad comercial.

Atentar: Cometer un atentado o amenaza.

B

Bitcoin: Un tipo de moneda electrónica producida por una red pública anónima y puede ser utilizada para intercambios comerciales.

C

Ciberataque: Actos en los que se cometen agravios a grupos o personas por medio de sistemas electrónicos.

Consigna: Orden que se da a los subordinados o que se transmite de unas personas a otras en una misión.

Constituir: Ser o significar las partes o elementos de una cosa determinada.

Criptomonedas: Un medio digital de divisas de intercambio que utiliza la criptografía para realizar transacciones financieras y transferencia de activos.

D

Directiva: Norma o conjunto de instrucciones que se establecen y se aplican al realizar una acción o plan.

E

Ejecutar: Llevar a cabo una acción, proyecto, encargo u orden con un fin.

Encriptar: Ocultar datos mediante una clave.

Extensión: Conjunto de elementos a los que se aplica con verdad un término.

F

Forense: De la administración de justicia o relacionado con ella.

H

Homogeneizar: Transformar en homogénea una cosa compuesta de diversos elementos.

Hacker: Persona con conocimientos de informática que se dedica a acceder ilegalmente a sistemas informáticos ajenos.

I

Imponer: Exigir a alguien cumplir, soportar, pagar, o aceptar una cosa.

Informático: De la informática o relacionado con ella.

Inminencias: Circunstancia de ser una cosa o riesgo, inminente, a punto de ocurrir.

Irrumpir: Aparecer violenta o repentinamente en un lugar.

Instancia: Momento o instante en el que se observa algo.

J

Jurídico: Del derecho o de las leyes o relacionado con ellos.

L

Lucro: Ganancia o beneficio que se obtiene en un asunto o negocio.

M

Malicioso: Que implica o denota malicia.

Marco: Conjunto de elementos que rodean una realidad no material y sirven para acotarla y comprenderla.

N

Normativa: Conjunto de leyes o reglamentos que rigen conductas y procedimientos, según los lineamientos de una organización.

O

Ordenador: Máquina ordenadora capaz de almacenar información y tratarla mediante operaciones matemáticas y lógicas.

P

Periódicos: Que sucede, o se realiza con intervalos regulares de tiempo o con cierta frecuencia.

Perpetrar: Llevar a cabo un delito o falta grave.

Programa: Conjunto de instrucciones detalladas que se dan a una computadora para que se realice o ejecute determinada operación.

Protocolo: Conjunto de reglas de comunicación que rigen el intercambio de comunicación entre dos equipos electrónicos y mantienen su regularidad.

R

Ransomware: Software diseñado por criminales para evitar a los usuarios acceder a archivos de su computadora, a menos que paguen cierta cantidad de dinero.

Red: Conjunto formado por un número determinado de aparatos y los circuitos que los unen e interconexionan.

Remitir: Enviar o mandar una cosa a un lugar o persona.

S

Servidor: Computadora conectada a una red informática que contiene datos y programas que dan servicio a otras computadoras por medio de esta red.

T

Transnacional: De varias naciones.

U

Utilidad: Provecho o beneficio que se saca de una cosa.

V

Virus: Programa de computadora que causa alteraciones y mal funcionamiento dentro de una computadora.

Tópico B

_____

Estrategias para aumentar la estabilidad social en Europa Central y evitar el surgimiento de grupos extremistas en Bosnia y Herzegovina

Por: Armando Daniel Navarro Sánchez

Antecedentes

La zona de los Balcanes ha entrado en un conflicto político, ideológico, diplomático y parcialmente militar, luego de conseguir estabilidad tras el conflicto bélico de 1992. Esta disputa ocurrió a partir de la desintegración de Yugoslavia y la formación de la República de Bosnia y Herzegovina. Los ejércitos de la República de Croacia y la República de Serbia buscaban luchar por la conquista del territorio bosnio y, por tres años, se cometieron los peores crímenes de guerra en la historia de Europa, después de la Segunda Guerra Mundial, que involucran asesinatos de niños, violaciones en masa, genocidios, campos de concentración y limpiezas étnicas en el centro del continente (Mastalic-Kosuta, 2017). Gran parte de la motivación de la contienda de Bosnia y Herzegovina fue el nacionalismo extremista de la República de Croacia y la República de Serbia, que fue causa de más de 100,000 decesos de musulmanes, croatas, serbios y bosnios. En 1995, los Estados Unidos de América y la Unión Europea (UE) intervinieron para crear los Acuerdos de Paz de Dayton. Este documento buscaba dar fin al enfrentamiento, a través de la modificación de las fronteras de Bosnia y Herzegovina para mantener la paz entre los diferentes grupos étnicos de los Balcanes. Se estableció un nuevo orden constitucional para esta nación, en el que se establece una división en dos entidades autónomas. Por un lado, la Federación de Bosnia y Herzegovina, constituida por musulmanes y croatas y, por otro, la República de Srpska con una población mayoritariamente serbia. A pesar de esto, la representación diplomática e internacional quedaría bajo el gobierno de la primera.

En 2017, surgió una estrategia para desequilibrar nuevamente a los Balcanes e impedir que Bosnia ingresara a organizaciones occidentales, como la Organización del Tratado del Atlántico Norte (OTAN). La autoproclamada República Independiente de Srpska conservó bajo protección, durante 20 años, a los grupos militares criminales que participaron en el conflicto de 1992, quienes ahora fungen como grupos paramilitares que buscan desestabilizar y dividir las fronteras de Bosnia y Herzegovina. Existen informes del Instituto de Investigación de Política Exterior de Estados Unidos y la Oficina del Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad (OAR), ambos organismos encargados de supervisar los Balcanes y el cumplimiento de los Acuerdos de Dayton; sobre la presencia del líder de la República de Srpska, Milorad Dodik, entre la organización de

diversos grupos paramilitares serbobosnios. La OAR ha informado, en repetidas ocasiones, sobre los lazos que tienen la Federación Rusa y la República de Srpska. Ambas naciones han impulsado a estos grupos a corromper a funcionarios públicos, atacar líderes políticos, apoyar a clanes de delincuentes y escenificar rebeliones contra el Estado.

En la actualidad, la República de Bosnia y Herzegovina es considerada insegura e inestable, debido a esta problemática. Al contar con el índice más alto del mundo de desempleo de jóvenes entre 14 y 25 años, y una inestabilidad social crónica, la región de los Balcanes podría convertirse en un nuevo bloque de asentamiento para grupos extremistas islámicos que comprometan la seguridad europea. Los Acuerdos de Dayton prohíben el ingreso de armas a la República de Bosnia y Herzegovina, mas la República de Srpska ignora constantemente esta norma y suministra armamento a sus grupos paramilitares. Desde 2015, se ha registrado que alrededor del 70 % de las armas que utilizan los terroristas en Europa provienen de los Balcanes. La República de Serbia y la República de Bosnia y Herzegovina han declarado que tienen un grave problema de control de armas.

Grupos extremistas que atentan contra Europa

Desde hace más de una década, el continente europeo ha sido víctima de numerosos ataques radicales que han afectado la seguridad e integridad de su ciudadanía. Actualmente, existen diversos grupos extremistas que, de forma continua, intentan cometer atentados contra símbolos culturales de Europa. Este radicalismo busca manifestar una creencia religiosa, ideología política o social opuesta a la cultura europea. Los grupos radicales aprovechan territorios empobrecidos y con poca o nula estabilidad social para implantarse y aumentar su número de tropas. Esta situación es constante en Europa Central y ha dado mayor facilidad para la comisión de atentados en el continente. La UE ha realizado una lista de grupos extremistas que se consideran un riesgo para la seguridad continental.

Entre las asociaciones más activas dentro y fuera de Europa, se encuentra el Estado Islámico (EI o ISIS, por sus siglas en inglés). Esta agrupación se compone de *yihadistas* establecidos principalmente en la República Árabe Siria y la República de Irak. El Estado Islámico destaca, entre sus objetivos, el antioccidentalismo y declaraciones de guerra santa (*yihad*) en contra de todo individuo, organización o gobierno que se oponga a su ideología.

La guerra santa se originó a partir de las discordias del Cristianismo y el Islam. Este enfrentamiento busca la victoria de la fe islámica, es decir, que el régimen político, económico y cultural musulmán sea instaurado en Occidente. A este régimen se le conoce como *Sharia*. La *Sharia* es un conjunto de juicios y leyes generales islámicas, e incluye los principios de la creencia, llamados leyes esenciales, los actos de adoración, la ética y las legislaciones civiles. El *yihadismo* es conocido como una de las ramas más violentas y radicales de la comunidad musulmana.

ISIS es considerado uno de los grupos radicales con más recursos armamentísticos e influencia en el mundo. Existen 40 grupos extremistas que han jurado lealtad y apoyo al Estado Islámico, entre los cuales destacan: *Boko Haram, Abu Sayyaf, Ansal al-Khilafah* y *Profetens Ummah*. La influencia de ISIS se extiende, en su mayoría, al Oriente, aunque existen células criminales que profesan la ideología *yihadista* en Sudamérica y Europa. Este alcance ha permitido al grupo perpetrar ataques extremistas en ciudades importantes como Nueva York, Madrid, Londres y Bruselas. Uno de los acometidos más recientes del Estado Islámico fue el ocurrido en París, Francia, el 13 de noviembre de 2015. Los miembros de EI dispararon armas de fuego a civiles en seis ubicaciones distintas, alrededor de la ciudad. Luego de este ataque, la UE propuso un planteamiento global para hacer frente a grupos extremistas. Esta estrategia consiste en una serie de medidas enfocadas en el refuerzo de las normas internacionales de seguridad, con el fin de evitar nuevas formas de extremismo, así como la intensificación en la seguridad fronteriza, el control de uso y tráfico de armas y el uso de recursos para frenar a grupos beligerantes ya existentes. El tráfico de armas de fuego es uno de los recursos más importantes para cualquier grupo extremista, ya que permite realizar cualquier actividad radical, además de mantener relaciones comerciales entre varias organizaciones.

Los principales proveedores de armas al Estado Islámico a lo largo de los años han sido: la Federación de Rusia, la República Popular China y la República Islámica del Irán. Esto se confirmó tras la reciente investigación que realizó, en 2017, el *Conflict Armament Research* (CAR). Aunado a lo anterior, CAR documentó 1,270 armas y 29,168 municiones recuperadas del Estado Islámico. De esto, apenas el 1.8 % provino de Estados Unidos de América. El abastecimiento de armas para ISIS ha sido necesario también para hacer frente a

la Guerra Civil de Siria. Actualmente, la Comisión Europea para la Unión de Seguridad, ha señalado, en la presentación del análisis de amenazas y seguridad continental europea; TEST 2018, que, según el último informe de situación y tendencia de la UE contra los grupos extremistas, Europa sigue siendo un objetivo para los atentados. Es por lo anterior que se necesita aumentar los esfuerzos de la UE para negar, a los *yihadistas*, los medios necesarios para llevar a cabo ataques (incluyendo armas, explosivos y recursos económicos)**,** y continuar abordando la radicalización y todo tipo de extremismo violento.

Guardia de Honor del Ejército Serbio

La Guardia de Honor del ejército Serbio ha existido como una escolta de seguridad para toda la población serbia y sus mandatarios, desde hace seis siglos. Se formó como un pequeño ejército impulsado por la ideología ultranacionalista para defender su territorio y patrimonio nacional. Al día de hoy funciona como un grupo paramilitar con el nombre de Honor Serbio, que sirve a la República de Srpska desde 1997. El grupo está destinado a desestabilizar a la Federación de Bosnia y Herzegovina, para evitar su llegada a la OTAN, a la vez que aumenta la influencia de Rusia en los Balcanes. Honor Serbio ha participado en desfiles del 9 de enero, durante el llamado Día Nacional de la República de Srpska, considerados ilegales para Bosnia y Herzegovina. Estos desfiles sirven como muestra de la independencia de la República de Srpska y llaman a la población serbia a iniciar un golpe de estado contra el gobierno bosnio. Los pertenecientes a este grupo se ven a sí mismos como defensores de su nación, y reciben apoyo armamentístico por parte de la Federación de Rusia. Algunos diarios europeos han afirmado que el dirigente de Honor Serbio es el líder político Milorad Dodik, y que el grupo tiene la intención de intervenir con violencia en las fronteras de Bosnia y Herzegovina. Desde 2017, los paramilitares serbios han adquirido más de 2,500 rifles rusos y ahora tienen la capacidad de armar al 75 % de sus fuerzas. La adquisición de este equipo, por parte de la República de Srpska, viola uno de los incisos en los Acuerdos de Dayton.

El grupo se compone de veteranos del conflicto de desintegración de Yugoslavia, en 1992. Algunos de sus miembros han participado dentro del ejército ruso en contra de la República de Ucrania y muchos otros, de acuerdo con el gobierno bosnio, son considerados criminales de guerra. La UE ha externado su temor ante el poder armamentístico que adquieren los serbios, debido a que, en 2018 se incrementó 90 % el número de armas de

fuego y municiones con las que cuenta la policía de la República de Srpska y Honor Serbio. Gran parte de este equipo no fue trasladado de una forma adecuada y no se tienen registros sobre su importación o el tipo de armamento. Por esto, la UE está considerando un posible caso de corrupción dentro del gobierno de Srpska y una situación grave de tráfico de armas de fuego en los Balcanes. A pesar de esto, ninguna organización ha tomado medidas en contra del grupo paramilitar o del gobierno de la República de Srpska, por lo que continúa habiendo casos de flujo ilegal de armas, en esta zona.

El tráfico de armas dentro de Europa

El tráfico de armas de fuego es un negocio desarrollado que existe en todo el mundo. Al ser consideradas, las armas de fuego, un bien de larga duración, los compradores no necesitan adquirirlas varias ocasiones. Cada año, el número de armas pequeñas adquiridas solo representa el 1 % de las que ya están en circulación alrededor del mundo. El tráfico de estos productos está enfocado en dos áreas: las utilizadas para fines delictivos y las adquiridas para fines políticos. El equipo armamentístico que transita en América se utiliza para el primer mercado, mientras que en Europa Central se comercia armas para el segundo. En ambos casos, la compra y venta de armamento, así como el ingreso de estas a cualquier país, está fuertemente ligado a actos de corrupción.

La existencia de grandes cantidades de armamento tiene lazos con la producción excesiva de estos bienes, en los países desarrollados. Todas las redes de comercio de armas en América Latina reciben equipo y municiones por parte de los Estados Unidos de América, en donde existen 270 millones de armas que son propiedad de civiles. Los cárteles de narcotráfico y las redes de trata de personas son abastecidas por la actividad ilícita del tráfico de armas, al tener en promedio 10 millones no registradas. Por otra parte, en Europa Central, el origen del armamento es la disolución de la Unión Soviética. La Federación de Rusia, la República Islámica del Irán, la República Federal de Alemania y la República de Ucrania son los países europeos que cuentan con el mayor arsenal dentro de sus fuerzas armadas, siendo el ejército ucraniano el más equipado, con 54 millones de armas. La existencia de estos suministros pone en riesgo la seguridad internacional y beneficia a grupos radicales, especialmente en África. El Instituto Internacional de Estudios Estratégicos de Europa, encargado de realizar informes sobre cualquier país de la UE y sugerir estrategias de mejora,

declaró que en 2017 se realizaron más de 500 traslados de armas no registrados desde Europa hacia África, lo cual refleja el riesgo que implica retener grandes cantidades de armamento dentro de una delegación.

La mayoría de los traslados en Europa se realizan bajo una falsa apariencia de legalidad. Esta situación implica que se utilice documentación falsa brindada por funcionarios públicos y se movilice armamento por vía marítima, terrestre e incluso aérea. En los Balcanes, el tráfico de armas se realiza por vía terrestre, ya que existen diversos rincones y ranuras en un automóvil donde se puede ocultar una pistola o un rifle desarmado (Nemac, 2015). Desde 2007, existe una ruta de tráfico de armas que va de la República de Serbia hasta el Reino de Bélgica, en la que la policía belga incautó, en 2018, 6,000 armas de fuego, que representan un 30 % del armamento que llega a dicha nación y la República Francesa. Otro método recurrente es a través de los inmigrantes que llegan de África y Asia a Europa. Los delincuentes sobornan o extorsionan a familias de migrantes para que trafiquen pistolas, cajas de munición u otro tipo de arsenal pequeño. Si logran llegar a territorio europeo occidental, son interceptados por miembros de redes de tráfico de armas para recoger su armamento. Europa aumenta cada año el número de armas de fuego sin registros que entran y salen del continente, y en cada país se encuentra una gran cantidad de delincuentes ligados a esta actividad. Actualmente, se han registrado casos de personas que pueden adquirir un rifle de asalto en cualquier parte de Europa, en tan solo media hora. Los Balcanes se han convertido en un centro de compra y venta de armamento conocido como un mercado negro del equipo militar.

Existen instituciones, como la Organización para la Seguridad y la Cooperación en Europa (OSCE), que han intentado por varios años frenar el flujo ilícito de armas dentro de Europa. La OSCE es encargada de establecer foros inclusivos para el diálogo de seguridad regional, que involucran el control de armamento. Esta institución, en 2011, estableció el Documento de Viena, el cual establece Medidas Destinadas a Fomentar la Confianza y la Seguridad (MFCS). La intención de este documento es reducir el riesgo de un conflicto armado en la UE por medio del control, la reducción y la concientización sobre el uso de armas de fuego. El Documento de Viena fomenta la cooperación de las naciones europeas para buscar el desarme en los excesos de equipo militar y obtener la desaparición del tráfico

de armas en Europa. A pesar de este y varios de los esfuerzos internacionales que se han creado en años recientes para frenar esta actividad, las redes de tráfico obtienen más personal implicado y más facilidad para burlar a la policía y a la milicia.

Acciones de INTERPOL ante el tráfico de armas de fuego en Europa

Desde su creación, la INTERPOL lucha constantemente contra el tráfico de armas de fuego de forma global. El uso de este tipo de objetos pone en riesgo la seguridad de los ciudadanos, exponiendo a la sociedad a delitos como la trata de personas, la corrupción, delincuencia organizada, piratería y el radicalismo. Los grupos delictivos transportan, diariamente, una gran cantidad de armas de fuego de forma local e internacional. Esta actividad resulta lucrativa y beneficiosa para el crimen organizado, ya que, al comerciar con estos bienes, se puede obtener financiamiento para realizar otro tipo de delitos. INTERPOL creó, en 2013, el Sistema para la Gestión de Registros y el Rastreo de Armas Ilícitas (*iARMS*). Este programa es una de las bases de datos sobre armas de fuego más completas del mundo. Este sistema es capaz de identificar modelos de planeación para el tráfico de armas y rutas de contrabando. Puede también, vincular a un sospechoso con un arma de fuego, identificar traficantes de armas y la localización de estos, detectar tendencias relacionadas con el contrabando y apoyar con información estratégica para frenar el suministro a beligerantes. El proceso para rastrear un arma inicia desde el país donde se fabricó e importó legalmente el arma, pasando por cualquier nación en el que haya sido ingresada de manera lícita y finaliza con el último propietario conocido. Para un funcionamiento adecuado, el proceso de rastreo de *iARMS* requiere de la participación policial de todos los países miembros de INTERPOL. Por otra parte, la utilización de este sistema cuenta con algunas limitaciones legales relacionadas con la jurisdicción del país en el que se encuentre el arma, las resoluciones del Consejo de Seguridad de la Organización de las Naciones Unidas (ONU), y la conformidad de las delegaciones con el proceso de rastreo. El sistema iARMS ha beneficiado a la cooperación internacional de la policía y a INTERPOL ha tenido mayor presencia y efectividad contra el tráfico ilícito de armas.

La Organización utiliza diferentes herramientas para identificar y contrarrestar el tráfico de armas de fuego. Una de estas herramientas es el Cuadro de Referencia de INTERPOL sobre Armas de Fuego, un sistema interactivo en línea que cuenta con

información, imágenes y referencias de 250,000 armas de fuego. Su objetivo es lograr mejor identificación de un arma de fuego que haya sido utilizada en un crimen, para su rastreo. Otra de las herramientas que más apoyan dentro de la investigación policial es la Red de Información Balística (IBIN). Este conjunto utiliza datos como marcas microscópicas de casquillos y balas encontradas en escenas del crimen. Una vez que se reúne la información, es utilizada para encontrar vínculos entre delitos aparentemente distintos, proporcionando información valiosa para investigar rutas y grupos delictivos que puedan estar relacionados. IBIN es capaz de generar alrededor de 220,000 coincidencias de una sola marca microscópica, por lo que se pueden encontrar patrones en el tipo de balas que utilizan los delincuentes y terroristas. Con esta herramienta, en 2017, INTERPOL logró identificar una red de contrabando de armas entre aduanas en ocho países africanos. Esta operación fue conocida como Trigger III y se logró incautar más de 152 armas de fuego, así como el arresto de 50 individuos relacionados con una pequeña red de tráfico.

En lo que respecta a la región de los Balcanes, la Organización ha mantenido una estrecha relación con todos los países de la zona, en especial con la República de Bosnia y Herzegovina. INTERPOL cuenta con una Oficina Central Nacional (OCN) en Sarajevo, desde la cual ha coordinado diversas operaciones en la República de Serbia, la República de Croacia y Bosnia y Herzegovina. La más reciente de estas operaciones se realizó en 2016, bajo el nombre de BALKAN TRIGGER. Este operativo se enfocó en atacar el tráfico ilícito de armas en los Balcanes, tras los atentados extremistas de 2015 en Europa que dejaron alrededor de 150 decesos en todo el continente. La operación condujo a la detención de 14 personas, miembros de una extensa organización criminal de tráfico de armas que va de Medio Oriente a los Balcanes. Del mismo modo, se incautaron 40 armas, seis kilogramos de explosivos, 1,300 unidades de munición y 11 granadas de mano; objetos que fueron identificados y añadidos a la base de datos de *iARMS*. INTERPOL supervisa posibles riesgos de seguridad para Europa y el mundo. Al mismo tiempo, la República de Bosnia y Herzegovina cumple un papel fundamental para la lucha contra el crimen en la zona de los Balcanes y sus alrededores.

Referencias

1. AFP. (2016). Bosnia y Serbia quieren frenar flujo ilegal de armas a Europa. Recuperado el 9 de julio de 2019, de *MILENIO*. Web. <https://www.google.com/amp/s/amp.milenio.com/internacional/bosnia-serbia-quieren-frenar-flujo-ilegal-armas-europa>

2. Bajrovic, R. (2018). Bosnia en el disparadero. Recuperado el 6 de julio de 2019, de *El País*. Web. <https://www.google.com/amp/s/elpais.com/internacional/2018/05/04/actualidad/1525452286_303181.amp.html>

3. Canchola, P. (2017). Tráfico de armas. Recuperado el 9 de julio de 2019, de *INSYDE*. Web. <http://insyde.org.mx/wp-content/uploads/2013/08/Tr%C3%A1fico-de-armas.pdf>

4. Consejo Europeo. (2019). La lucha contra el terrorismo en Europa. julio 9 de 2019, de *Consejo Europeo*. Web. <https://www.consilium.europa.eu/es/policies/fight-against-terrorism/>

5. Docto, T. (2019). Tráfico de armas . 8, julio de 2019, de *Centro de Estudios Sociales*. Web. <https://www.casede.org/BibliotecaCasede/Trafico-de-armas-docto183.pdf>

6. El Economista. (2015). Cinta adhesiva y 500 euros: así llegan las armas desde los Balcanes al corazón de Europa. Recuperado el 16 de julio del 2019, de *El Economista*. Web. <https://www.google.com/amp/s/ecodiario.eleconomista.es/noticias-amp/7184060/Cinta-adhesiva-y-500-euros-asi-llegan-las-armas-desde-los-Balcanes-al-corazon-de-Europa>

7. El Diario. (2018). Atentados yihadistas en Europa en los últimos cinco años. Recuperado el 8 de julio de 2019, de *El Diario*. Web.<https://www.eldiario.es/sociedad/Atentados-yihadistas-Europa-ultimos-anos_0_803519907.html>

8. Ferrero, R. (2015). Lo que Dayton no logró en los Balcanes. Recuperado el 7 de julio de 2019, de *Política Exterior*. Web. <https://www.politicaexterior.com/articulos/politica-exterior/lo-que-dayton-no-logro-en-los-balcanes/>

9. Foro Europa Ciudadana. (2019). La Comisión Europea presenta nuevas propuestas para mejorar el control de armas en Europa. Recuperado el 09 de julio de 2019, de *Foro Europa Ciudadana*. Web.<https://www.europaciudadana.org/la-comision-europea-presenta-nuevas-propuestas-para-mejorar-el-control-de-armas-en-europa/>

10. Hasic, N. (2017). Bosnia: 25 años de la guerra que horrorizó a Europa. Recuperado el 5 de julio de 2019, de *Levante*. Web. <https://www.google.com/amp/s/amp.levante-emv.com/internacional/2017/04/06/bosniºa-25-anos-guerra-horrorizo/1551318.html>

11. Indep, T. (2018). Seis siglos de Honor Serbio. Recuperado el 8 de julio de 2019, de *El País*. Web. <https://elpais.com/diario/1989/06/29/internacional/615074405_850215.html>

12. INTERPOL. (2012). Bosnia-Herzegovina celebra sus 20 años como miembro de INTERPOL. Recuperado el 9 de julio de 2019, de *INTERPOL*. Web. <https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2012/Bosnia-Herzegovina-celebra-sus-20-anos-como-miembro-de-INTERPOL>

13. INTERPOL. (2016). Incautación de armas y explosivos en una operación dirigida por INTERPOL. Recuperado el 9 de julio de 2019, de *INTERPOL*. Web. <https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2016/Incautacion-de-armas-y-explosivos-en-una-operacion-dirigida-por-INTERPOL>

14. INTERPOL. (2014). Red de INTERPOL de Información Balística. Recuperado el 9 de julio de 2019, de *INTERPOL*. Web. <https://www.interpol.int/es/Delitos/Trafico-de-armas-de-fuego/Red-de-INTERPOL-de-Informacion-Balistica>

15. INTERPOL. (2013). Sistema de INTERPOL para la Gestión de Registros y el Rastreo de Armas Ilícitas (iARMS). Recuperado el 9 de julio de 2019, de *INTERPOL*. Web. <https://www.interpol.int/es/Delitos/Trafico-de-armas-de-fuego/Sistema-de-INTERPOL-para-la-Gestion-de-Registros-y-el-Rastreo-de-Armas-Ilicitas-iARMS>

16. INTERPOL. (2019). Tráfico de armas de fuego. Recuperado el 9 de julio de 2019, de *INTERPOL*. Web.< https://www.interpol.int/es/Delitos/Trafico-de-armas-de-fuego>

17. Iriarte, D. (2018). Paramilitares serbobosnios entrenados por Rusia, el fenómeno que inquieta a Europa. Recuperado el 5 de julio de 2019, de *El Confidencial*. Web. <https://www.google.com/amp/s/www.elconfidencial.com/amp/mundo/2018-03-27/paramilitares-republica-serbia-bosnia_1540334/>

18. López, R. (2014) Los Acuerdos de Dayton, fin de la guerra de Bosnia. Recuperado el 7 de julio de 2019, de *El País*. Web. <https://viajeaeuropadeleste.com/2014/10/29/los-acuerdos-de-dayton-el-final-de-la-guerra-de-bosnia/>

19. Medina, G. (2013). Guerra de Bosnia. Recuperado el 8 de julio de 2019, de *Escuela ENAPE*. Web. <http://derechosenape.blogspot.com/2013/06/guerra-de-bosnia.html?m=1>

20. Organización para la Seguridad y la Cooperación en Europa. (s.f). Control de armamentos. Recuperado el 09 de julio de 2019, de *Organización para la Seguridad y la Cooperación en Europa*. Web.<https://www.osce.org/es/arms-control>

21. Organización para la Seguridad y la Cooperación en Europa. (s.f). ¿Qué es la OSCE?. Recuperado el 09 de julio de 2019, de *Organización para la Seguridad y la Cooperación en Europa*. Web.< https://www.osce.org/es>

22. Parlamento Europeo. (2018). Terrorismo en la UE: ataques terroristas, víctimas mortales y detenciones. Recuperado el 8 de julio de 2019, de *Noticias Parlamento Europeo* Web. <http://www.europarl.europa.eu/news/es/headlines/security/20180703STO07125/terrorismo-en-la-ue-ataques-terroristas-victimas-mortales-y-detenciones>

23. Público. (2019). El PSOE propone que la Unión Europea apruebe una lista de países vetados para la venta de armas. Recuperado el: 17 de julio de 2019, de *Público*. Web.<https://www.publico.es/politica/venta-armas-psoe-propone-union-europea-apruebe-lista-paises-vetados-venta-armas.html>

24. UNODC. (2016). Globalization of Crime Summary. Recuperado el 16 de julio del 2019, de *UNODC*. Web. <https://www.unodc.org/documents/data-and-analysis/tocta/Globalization_of_Crime-ExSum-Spanish.pdf>

Glosario

A

Arsenal: Depósito de armas o material de guerra.

B

Beligerante: Dispuesto a la hostilidad y al enfrentamiento con una persona o grupo.

C

Capacitación: Hacer que una persona o una cosa sea apta o capaz para determinada cosa.

Casquillo: Cartucho de metal vacío.

Criminalista: Persona que ha cometido o ha intentado cometer un crimen.

D

Desestabilizar: Perder la estabilidad.

Discordia: Falta de acuerdo o conformidad entre personas que a menudo conviven o se relacionan de algún modo.

Disolución: Acción de desintegrar o destruir.

E

Encaminar: Dirigir la intención hacia un fin determinado.

Enjuiciamiento: Forma legal de proceder en la tramitación y terminación de los negocios judiciales.

Extremista: Que es partidario de ideas o actitudes extremas, especialmente en política.

G

Gestionar: Dirigir, administrar.

I

Ideología: Conjunto de ideas que caracterizan a una persona, colectividad o movimiento.

J

Jurisdicción: Autoridad o poder para juzgar y aplicar leyes en un territorio.

L

Lucrativo: Que genera dinero por medio de la realización de algo.

Incautar: Tomar posesión legal de determinados bienes.

Inclusivo: Es aquel que encuadra, incorpora, o adjunta a una persona u elemento.

M

Mercado: Lugar teórico donde se encuentra la oferta y la demanda de varios productos.

N

Nacionalismo: Doctrina y movimiento político que reivindica el derecho de una nacionalidad para justificar un comportamiento sociopolítico.

P

Paramilitar: Se utiliza para calificar al grupo civil que se encuentra organizado bajo una estructura de estilo militar.

Perpetrar: Llevar a cabo un delito o una falta grave.

Previsibilidad: Dicho de una persona, que se puede saber con antelación cómo reaccionará o actuará frente a una situación porque es transparente o se la conoce.

Promulgar: Publicar solemnemente alguna ley u otra disposición.

R

Radical: Que tiene una actitud e ideas extremistas y poco flexibles, en todo ámbito social.

Red: Conjunto de personas distribuidas por varios lugares, organizadas para alcanzar un fin común, generalmente ilícito.

Régimen: Conjunto de normas o reglas que reglamentan o rigen cierta cosa.

T

Transparencia: se refiere a la honestidad, ética y responsabilidad que deben tener los gobiernos y los entes públicos.