FBINAA

March 2025


FBINAA
LATIN AMERICA & CARIBBEAN CHAPTER
NA
FBI NATIONAL ACADEMY
KNOWLEDGE COURAGE INTEGRITY

ÍNDICE

EDITORIAL

POR ANNIE A. CUELLO
PRESIDENTA

RESILIENCIA... es una palabra que siempre ha llamado la atención personal por el trasfondo tan subjetivo que puede llegar a tener. Para algunos implica quizás ahogarse en lo emocional y simplemente caminar por un sendero incómodo, por no describirlo de otra forma, sin embargo, en nuestro mundo de aplicación de la ley veo la resiliencia como algo más. Le veo como la oportunidad perfecta para detenernos y analizar dónde estamos y cómo estamos, para la reflexión, las críticas constructivas y luego preguntarnos hacia dónde vamos.

Mientras escribía esto razonaba sobre todos los hermanos y hermanas de aplicación de la ley que han dado su vida en el cumplimiento del deber, sobre las dificultades administrativas y presupuestarias que enfrentamos en nuestras agencias los que aún estamos activos en el servicio, pero también aquellas situaciones que vivieron los ya retirados. Pensaba en los sacrificios, personales y familiares, que son necesarios para trabajar cada día en nuestro propósito de comunidades más seguras.

Nuestro trabajo no se trata de simplemente aceptar que estamos en línea de fuego todos los días, afectando intereses criminales, o de realizar nuestro trabajo como si fuésemos máquinas, sino también de aplicar la inteligencia, para que nuestro trabajo sea más eficiente. Nuestras pequeñas acciones de todos los días pueden fortalecer a quienes se encuentran a nuestro alrededor, e impactar en el macro propósito de comunidades más seguras. Eso, para mí, es parte de la resiliencia.

Entender que no estamos solos en la labor, que la globalización es parte de las herramientas con las que contamos para obtener mejores resultados, y que bien se siente el tener la posibilidad de acudir a una red como la FBINAA, donde conversas no solo de estrategias en la lucha contra la criminalidad, sino también de las situaciones que entendemos afectan nuestro desempeño. Ante todo, somos personas y posiblemente está ese caso que te llena de orgullo, pero te veas en la necesidad de no ir a testificar a la corte, porque tu madre tiene cáncer y debes estar ahí para ella; o que debas decir "no" a un jefe que desconoce de habilidades gerenciales y acceder compromete tu responsabilidad administrativa, civil y en ocasiones, hasta penal. Estos temas también son parte de la resiliencia.

Algunos se preguntarán la relación entre la resiliencia y el tema central de esta publicación, pero no quería utilizar el editorial de la revista para hablar de los mismos artículos que se encuentran adelante, pero si quería hacer el llamado de atención, para que al leerlos podamos realizar un ejercicio de análisis y que podamos preguntarnos la manera en qué estamos enfrentando no solo los delitos relacionados con alta tecnología, sino todos aquellos a los que ponemos cara cada día. ¿Estoy permitiendo que me ahogue la creatividad de los criminales? O, ¿estoy siendo resiliente, manejando el estrés de forma adecuada, para cumplir con todas mis facetas (persona, trabajador, padre, madre, amigos, pareja, trabajo voluntario, capacitación continua, etc.) ?, porque al final, considero que lo primordial para entender la resiliencia es lograr la combinación de autocuidado, responsabilidad afectiva y eficiencia en nuestras actividades, como oficiales de cumplimiento de la ley.

EDITORIAL

BY ANNIE A. CUELLO
PRESIDENT

RESILIENCE... is a word that has always caught my personal attention due to the subjective depth it can have. For many people, it may perhaps imply drowning in emotions and simply walking down an uncomfortable path, not to describe it any other way. However, in our world of law enforcement, I see resilience as something more. I see it as the perfect opportunity to stop and reflect on where we are and how we are, for reflection, constructive criticism, and then ask ourselves where we are headed.

As I was writing this, I thought about all the brothers and sisters in law enforcement who have given their lives in the line of duty, about the administrative and budgetary difficulties we face in our agencies those of us still active in service, but also the situations experienced by those who are retired. I thought about the personal and family sacrifices necessary to work each day toward our goal of safer communities.

Our work is not simply about accepting that we are in the line of fire every day, affecting criminal interests, or doing our job as if we were robots, but also about how we can apply intelligence so that our work becomes more efficient. Our small daily actions can strengthen those around us and impact the larger purpose of safer communities. That, to me, is part of resilience.

Understanding that we are not alone in our work, that globalization is part of the tools we have to achieve better results, and how good it feels to have the possibility to approach a network like the FBINAA, where you can discuss not only strategies in the fight against crime but also the situations we understand affect our performance. Above all, we are people, and you are going to have that case that fills you with pride, but you won't be able to testify in court because your mother has cancer and you need to be there for her; or having to say "no" to a boss who lacks management skills and agreeing with that boss would compromise your administrative, civil, and sometimes even criminal responsibilities. These issues are also part of resilience.

Some may wonder about the connection between resilience and the main theme of this publication, but I didn't want to use the editorial of the magazine to talk about the same articles that are ahead. What I did want to do was raise awareness so that as we read them, we can engage in an exercise of analysis and ask ourselves how we are facing not only high-tech crimes but also those we confront every day. Am I allowing myself to be overwhelmed by the criminals' creativity? Or, am I being resilient, managing stress properly, to fulfill all my roles (person, worker, father, mother, friend, partner, volunteer, continuing education, etc.)? Because in the end, I believe the main key to understand resilience is achieving the combination of self-care, emotional responsibility, and efficiency in our duties as law enforcement officers.

LOS DESAFÍOS TRANSFRONTERIZOS DE LA CIBERSEGURIDAD EN LA ERA DE LA INFORMACIÓN

El destino nos ha ubicado en un momento de la humanidad definido como "la era de la información", siendo los datos el activo más importante del siglo XXI. Hay quienes afirman que quienes controlan los datos, controlan el mundo. En consecuencia, la configuración de un espacio comunicativo e interactivo denominado ciberespacio, paralelo al mundo físico, ha conllevado la modificación de las relaciones económicas, políticas, sociales y, especialmente, las personales (Miró, 2012).

En 2023 el número estimado de usuarios de Internet en todo el mundo era de 5.400 millones, frente a los 5.300 millones del año anterior. Esta proporción representa el 67% de la población mundial. En contraste, América Latina y el Caribe hoy cuentan con más de 430 millones de usuarios de internet, lo que representa alrededor del 75% de su población (Statista, 2024). Sin embargo, este nuevo entorno de interacción social, el ciberespacio, ha generado nuevos comportamientos reprochables socialmente, como el cibercrimen, así como también la diversificación de otros delitos, optimizando su modus operandi a través de los beneficios tecnológicos que buscan mayor efectividad en su ejecución por parte de las organizaciones criminales, y la ciberdelincuencia en general.

Por ello, entre las condiciones técnicas que permiten un ambiente favorable en el iter criminis del cibercrimen estarían, entre otros (Clough, 2015), el incremento exponencial de usuarios con acceso a internet, siendo proporcional a una mayor oportunidad de perfilar una víctima.

Captura realizada por el Centro Cibernético Policial - DIJIN, de la Policía Nacional de Colombia en la operación KAERB.

A su vez, el anonimato del ciberdelincuente mediante técnicas, protocolos y herramientas de acceso libre como es el caso de las plataformas de comunicación encriptada (E2EE). De acuerdo con Internet Watch Foundation (IWF, 2024) en 2023 se reveló la presencia de más de 20.000 imágenes generadas por IA en un foro de la web oscura en un mes, donde más de 3.000 representaban actividades delictivas de abuso sexual infantil. Sumado, la multijurisdiccionalidad, transfronterización (Posada, 2017) y descentralización de la información, los usuarios y la infraestructura digital (Clough, 2015), son factores facilitadores para el accionar de los actores criminales, que generan un costo del cibercrimen de USD 8 billones en 2023, con un potencial crecimiento a $10.5 billones para 2025 (AMCS, 2023).

Este panorama complejo y cambiante por la velocidad de los avances tecnológicos ha llevado a que la realidad esté superando la ficción cinematográfica de Hollywood, siendo retos para la ciberseguridad, las agencias de ley, la industria y los ciudadanos a nivel mundial, a través de diferentes modalidades como ataques de denegación distribuida de servicios (DDoS), software malicioso, skimming digital, fraudes románticos, extorsiones sexuales online, explotación de contenido sexual infantil, suplantación personal superando factores de autenticación, entre otros. Se suma el aprovechamiento ilegal de la IA por la ciberdelincuencia, identificándose nuevas técnicas de ingeniería social más efectivas, el desarrollo de nuevos códigos de software malicioso, producción de material de abuso sexual infantil, como fue el reciente caso del FBI en Wisconsin (Estados Unidos) donde fue acusado un hombre de haber creado más de 13,000 imágenes explícitas de abuso sexual a menores, que aparentemente generó con una popular herramienta IA (Telemundo, 2024).

De acuerdo con Europol (2024), la dinámica del mercado criminal de malware y servicios de phishing se asemeja a la dinámica de las industrias legítimas, mientras que el comercio

de datos hurtados se está convirtiendo en la principal amenaza relacionada con el crimen como servicio (CaaS), que se ofertan en la web oscura que pueden ayudar a los ciberdelincuentes en línea a desarrollar scripts y crear correos electrónicos de phishing, además del uso de deepfakes para imitar voces de directores y ejecutivos de compañías. Además, el phishing persiste como el vector de ataque más frecuente para el fraude en términos del número de campañas de este tipo de modalidad contra ciudadanos de la Unión Europea, empresas privadas e instituciones públicas, el smishing (phishing por SMS/texto) fue el tipo de phishing más común utilizado por los estafadores en 2023, mientras que el quishing (phishing por código QR) es una amenaza emergente.

De allí la prioridad de realizar acciones coordinadas bajo un enfoque de cooperación internacional, en cumplimiento a los compromisos adquiridos por los Estados en tratados internacionales como el Convenio de Budapest, y la nueva Convención de Cibercrimen de las Naciones Unidas, entre otros, que conduzcan a respuestas proporcionales, como han sido las operaciones "Cookie Monster", liderada por el FBI, la policía holandesa y otras agencias a nivel mundial, que permitió en 2023 inhabilitar al mercado ilegal Génesis, uno de los sitios de la Dark Web más peligrosos por donde vendían credenciales de cuentas robadas y bots utilizados por piratas informáticos de todo el mundo. Este sitio web tenía más de 1,5 millones de listados de bots que sumaban más de 2 millones de identidades digitales en el momento de su eliminación (EUROPOL, 2024). Por otra parte, la operación KAERB, realizada en 2024 por autoridades europeas y latinoamericanas y EUROPOL, resultó en el desmantelamiento de una red criminal internacional dedicada al desbloqueo de teléfonos móviles robados o perdidos a través de una plataforma de phishing. Los investigadores identificaron más de 2.000 desbloqueadores que se habían registrado en la plataforma de phishing a lo largo de los años. La investigación reveló que la red criminal había desbloqueado más de 1,2 millones de teléfonos móviles (EUROPOL, 2024)

Lo anterior ratifica que la cooperación internacional entre las fuerzas de ley, la industria de la tecnología y otros sectores de la sociedad es el camino correcto, ante el nivel de agresividad de estos nuevos fenómenos sociales, lo que nos obliga a repensarnos continuamente como organismos de seguridad responsables de la ciberseguridad en el orbe. Es un hecho consumado, las nuevas tecnologías han llegado para asumir un rol intrínseco y arraigado en la sociedad; sin embargo, el alcance de estas está en el uso indiscriminado o adecuado que le den los seres humanos. Existen grandes debates sobre la ética, la fragmentación social, por el impacto no solo por el aprovechamiento ilegal de las organizaciones criminales, sino además por la relación con la salud mental y la captología, es decir, la manipulación del comportamiento, las actitudes y creencias de las personas.

Finalmente, mientras el mundo académico y expertos en ciberseguridad avizoran efectos apocalípticos del internet por ser una criatura altamente vulnerable (Paniagua, 2021), y aún más con el nivel de desarrollo que está alcanzado la Inteligencia Artificial, nos debemos aferrar a que la gran diferencia entre los humanos y estas tecnologías disruptivas no radica en la inteligencia per se, porque no es exclusiva de nosotros, sino que está en el monopolio de los sentimientos de los seres vivos, que nos conllevan a la conciencia humana de pensar hasta dónde queremos que esta era de la información y los datos transforme la sociedad (Harari, 2018).

CROSS-BORDER CYBERSECURITY CHALLENGES IN THE INFORMATION AGE

Fate has placed us in a moment of humanity defined as “the information age”, with data being the most important asset of the 21st century. There are those who claim that those who control the data, control the world. Consequently, the configuration of a communicative and interactive space called cyberspace, parallel to the physical world, has led to the modification of economic, political, social and, especially, personal relations (Miró, 2012).

In 2023, the estimated number of Internet users worldwide was 5.4 billion, compared to 5.3 billion the previous year. This proportion represents 67% of the world's population. In contrast, Latin America and the Caribbean today have more than 430 million Internet users, representing around 75% of its population (Statista, 2024). However, this new environment of social interaction, the cyberspace, has generated new socially reprehensible behaviors, such as cybercrime, as well as the diversification of other crimes, optimizing their modus operandi through technological benefits that seek greater effectiveness in their execution by criminal organizations, and cybercrime in general.

Therefore, among the technical conditions that allow a favorable environment in the iter criminis of cybercrime would be, among others (Clough, 2015), the exponential increase of users with access to the Internet, being proportional to a greater opportunity to profile a victim.

Captura realizada por el Centro Cibernético Policial - DIJIN, de la Policía Nacional de Colombia en la operación KAERB.

In turn, the anonymity of the cybercriminal through techniques, protocols and tools of free access as is the case of encrypted communication platforms (E2EE). According to the Internet Watch Foundation (IWF, 2024), in 2023, the presence of more than 20,000 AI-generated images was revealed on a dark web forum in one month, where more than 3,000 represented child sexual abuse criminal activities. In addition, multijurisdictionality, cross-borderization (Posada, 2017) and decentralization of information, users and digital infrastructure (Clough, 2015), are facilitating factors for the actions of criminal actors, generating a cybercrime cost of USD 8 billion in 2023, with a potential growth to $10.5 billion by 2025 (AMCS, 2023).

This complex and changing panorama due to the speed of technological advances has led to reality surpassing Hollywood film fiction, posing challenges for cybersecurity, law enforcement agencies, industry and citizens worldwide, through different modalities such as distributed denial of service attacks (DDoS), malware, digital skimming, romance fraud, online sexual extortion, exploitation of child sexual content, personal impersonation overcoming authentication factors, among others. The illegal use of AI by cybercrime is added, identifying new, more effective social engineering techniques, the development of new malicious software codes, the production of child sexual abuse material, as was the recent case of the FBI in Wisconsin (United States) where a man was accused of having created more than 13,000 explicit images of sexual abuse of minors, which he apparently generated with a popular AI tool (Telemundo, 2024)

According to Europol (2024), the dynamics of the criminal market for malware and phishing services resemble the dynamics of legitimate industries, while the trade

in stolen data is becoming the main threat related to crime as a service (CaaS), which are offered on the dark web that can help online cybercriminals develop scripts and create phishing emails, in addition to the use of deepfakes to imitate the voices of company directors and executives. Furthermore, phishing remains the most frequent attack vector for fraud in terms of the number of such campaigns against EU citizens, private companies and public institutions, smishing (SMS/text phishing) was the most common type of phishing used by fraudsters in 2023, while quishing (QR code phishing) is an emerging threat.

Hence the priority of carrying out coordinated actions under an international cooperation approach, in compliance with the commitments made by States in international treaties such as the Budapest Convention, and the new United Nations Cybercrime Convention, among others, which lead to proportional responses, such as the "Cookie Monster" operations, led by the FBI, the Dutch police and other agencies worldwide, which in 2023 allowed the disabling of the illegal marketplace Genesis, one of the most dangerous Dark Web sites where stolen account credentials and bots used by hackers around the world were sold. This website had more than 1.5 million bot listings totaling more than 2 million digital identities at the time of its removal (EUROPOL, 2024). On the other hand, the KAERB operation, carried out in 2024 by European and Latin American authorities and EUROPOL, resulted in the dismantling of an international criminal network dedicated to unlocking stolen or lost mobile phones through a phishing platform. Investigators identified more than 2,000 unlockers who had registered on the phishing platform over the years. The investigation revealed that the criminal network had unlocked more than 1.2 million mobile phones (EUROPOL, 2024)

The above confirms that international cooperation between law enforcement, the technology industry and other sectors of society is the right path, given the level of aggressiveness of these new social phenomena, which forces us to continually rethink ourselves as security agencies responsible for cybersecurity in the world. It is a fait accompli, new technologies have arrived to assume an intrinsic and rooted role in society; However, the scope of these lies in the indiscriminate or appropriate use that human beings give them. There are great debates about ethics, social fragmentation, due to the impact not only due to the illegal exploitation of criminal organizations, but also due to the relationship with mental health and captology, that is, the manipulation of people's behavior, attitudes and beliefs.

Finally, while the academic world and cybersecurity experts foresee apocalyptic effects of the Internet for being a highly vulnerable creature (Paniagua, 2021), and even more so with the level of development that Artificial Intelligence is reaching, we must hold on to the fact that the great difference between humans and these disruptive technologies does not lie in intelligence per se, because it is not exclusive to us, but rather it is in the monopoly of the feelings of living beings, which lead us to the human consciousness of thinking about how far we want this era of information and data to transform society (Harari, 2018).

ADRIÁN VEGA

LIEUTENANT CORONEL

PROFESSIONAL PROFILE

Adrián Vega. Officer of the Colombian National Police in the rank of Lieutenant Coronel, with twenty-one years in the institution, of which 15 have been in the criminal investigation service, he served as head of the Police Cyber Center of the Criminal Investigation Directorate and Interpol. In turn, he was a Liaison Officer as an expert in cybercrime at the European Center against Cybercrime EC3 of EUROPOL in The Hague - Holland in 2017-2018. Mayor Vega is a lawyer, professional in criminology, specialist in legal psychology, master of computer law and new technologies. He has completed training in cybersecurity and computer crimes with law agencies in South Korea, Spain, the United States, Israel and the Netherlands. He is a member of the 288th class of the FBI National Academy of 2023.

References

- Clough, J. (2015). Principle of cybercrime. Cambridge.
- EUROPOL. (2024). Retrieved from https://www.europol.europa.eu/media- press/newsroom/news/criminal-phishing-network-resulting-in-over-480-000-victims- worldwide-busted-in-spain-and-latin-america
- EUROPOL. (2024). Retrieved from https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf
- Harari, Y. N. (2018). 21 lecciones para el siglo XXI. Debate.
- IWF. (2024). Retrieved from https://www.iwf.org.uk/about-us/why-we-exist/our- research/how-ai-is-being-abused-to-create-child-sexual-abuse-imagery/
- May, J. (n.d.). Naciones Unidas. Retrieved from https://www.un.org/es/chronicle/article/el- nexo-entre-las-tic-y-la-pobreza
- Miró, F. (2012). El Cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio. Madrid: Ediciones Jurídicas y Sociales, S.A.
- Paniagua, E. (2021). Error 404. España: Penguin Random House Grupo Editorial.
- Posada, R. (2017). Los cibercrímenes: Un nuevo paradigma de criminalidad. Bogotá: Ibañez.
- Statista. (2024, 09 20). Retrieved from https://es.statista.com/estadisticas
- Telemundo. (2024, 05 21). Retrieved from https://www.telemundo.com/noticias/noticias- telemundo/crimen-y-violencia/fbi-inteligencia-artificial-abuso-sexual-menores-ninos- imagenes-rcna153409

LA PRESENCIA DEL FBI EN PERÚ: UNA ALIANZA ESTRATEGICA EN AMÉRICA LATINA Y EL CARIBE EN LA LUCHA CONTRA EL CRIMEN ORGANIZADO TRANSNACIONAL

Durante décadas, impresionantes crónicas policiales han servido como fuente de inspiración para inolvidables producciones cinematográficas en Hollywood y la televisión estadounidense. En estas representaciones, hemos sido testigos de casos criminales complejos donde los investigadores demuestran su alta pericia en criminalística y ciencias forenses, obteniendo importantes evidencias que permiten esclarecer los móviles e identificar a los autores de los delitos.

Sin embargo, más allá de los elementos de ficción o imaginación que puedan acompañar estas historias, existe una realidad que refleja el arduo y dedicado trabajo de las fuerzas policiales alrededor del mundo en la lucha contra la criminalidad organizada. En este contexto, destaca el Federal Bureau of Investigation (FBI, por sus siglas en inglés), la agencia federal de investigación criminal del Departamento de Justicia de los Estados Unidos, que ha alcanzado un prestigio internacional a lo largo de sus 116 años de existencia.

La misión del FBI es "Proteger al pueblo estadounidense y defender la Constitución de los Estados Unidos". Con jurisdicción sobre más de 200 delitos federales, sus áreas de investigación abarcan desde asuntos de seguridad nacional y crimen organizado hasta corrupción pública y delitos cibernéticos, entre otros delitos complejos.

Es importante señalar que el trabajo del FBI no se limita a las fronteras de los Estados Unidos; su presencia también se ha expandido a Latinoamérica y el Caribe. En este sentido, el FBI ha establecido una importante cooperación en Perú, donde brinda asesoramiento en materia de investigación criminal y ciencias forenses a la policía peruana y a los operadores de justicia nacionales.

EL PROGAMA DE AGREGADOS LEGALES

El FBI cuenta con un programa de Agregados Legales y tiene "63 oficinas de agregados legales, comúnmente conocidas como "legats", y 30 suboficinas más pequeñas en ciudades clave de todo el mundo, que brindan cobertura a más de 180 países, territorios e islas". "Cada oficina se establece mediante acuerdo mutuo con el país anfitrión y está ubicada en la embajada o consulado de Estados Unidos en esa nación. El programa de agregados legales "es administrado por la División de Operaciones Internacionales en la sede del FBI en Washington, DC. Esta oficina se mantiene en estrecho contacto con otras agencias federales, Interpol, policías extranjeros y oficiales de seguridad en Washington y asociaciones nacionales e internacionales de aplicación de la ley."
EL programa permite el enlace internacional e intercambio de información con las agencias del cumplimiento de la ley en el extranjero, conforme a las leyes, tratados y acuerdos entre estas agencias, para coordinar pedidos de asistencia mutua e investigaciones criminales de interés común.

LA PRESENCIA DEL FBI EN PERÚ

Durante varios años el Perú recibió visitas temporales de agentes del FBI para coordinar con la Policía Nacional del Perú, Ministerio Público y entidades afines, la investigación de hechos delictivos con vínculos comunes entre Perú y los Estados Unidos.

En el año 2016 se iniciaron las primeras conversaciones entre el gobierno del Perú y los Estados Unidos para la instalación de una sede del FBI en Lima, Perú, con la finalidad de profundizar temas en los que ya se venía trabajando, incluyendo el importante aporte que podría brindar el FBI en el entrenamiento de los policías peruanos en temas especializados de investigación criminal, operaciones tácticas y la implementación de adelantos de la ciencia forense como característica de una policía científica.

LA CONSOLIDACIÓN DEL PROCESO

Luego de un largo proceso de evaluación y autorizaciones gestionadas por ambos países, en noviembre del 2020 se concretó la instalación de una oficina de Agregado Legal del FBI en la Embajada de los Estados Unidos en Perú. Esta oficina depende de la sede regional del Agregado Legal del FBI ubicada en Santiago de Chile. Asimismo, se nombró Agregado Legal Adjunto al agente especial del FBI Norman Quilichini, abogado de profesión, con una importante experiencia en investigación criminal, operaciones tácticas e investigación de delitos de corrupción de funcionarios públicos.

Asimismo, se habilitó una plaza para un investigador nacional, que el autor de este artículo, graduado en la sesión 136 del FBINAA, tiene el honor de ocupar en la actualidad.

LOS GRADUADOS DEL FBINAA EN PERÚ

El Perú cuenta con 11 oficiales de la Policía Nacional que se han graduado en el prestigioso programa internacional de la Academia del FBI. A la fecha, este programa ha realizado 291 sesiones de 10 semanas cada una, capacitando a miles de policías de los 50 estados de los Estados Unidos, así como 10,200 organismos encargados de la aplicación de la ley, y 174 países de todo el mundo.

Los graduados forman parte de la asociación FBI National Academy Associates, Inc. (FBINAA, por sus siglas en inglés), una organización internacional sin fines de lucro cuyo objetivo es "inspirar a los miembros del FBINAA a continuar sirviendo a la comunidad, fomentar redes, promover la educación y el desarrollo profesional durante su carrera policial y más allá".

El primer policía peruano en graduarse de la Academia del FBI fue el Inspector Mayor Alfonso Rivera Santander Herrera, quien luego se convirtió en Director de la antigua Policía de Investigaciones del Perú. Rivera Santander participó en la sesión 71 de la Academia el 19 de junio de 1963 y es reconocido por haber aplicado los conocimientos adquiridos para mejorar los métodos de investigación y desarrollar la ciencia criminalística en la policía peruana, estableciendo una nueva estructura técnica y científica. Los graduados posteriores también han realizado contribuciones significativas al desarrollo institucional.

LA PRIMERA SESIÓN DE REENTRENAMIENTO EN PERÚ

Del 21 al 23 de mayo del presente año, Lima fue el escenario de la Conferencia Internacional de Reentrenamiento para los Oficiales de Policía graduados de la Academia del FBI, Capítulo de Latinoamérica y el Caribe. El tema central de esta conferencia fue "Lucha Contra la Criminalidad Organizada Transnacional". Durante el evento, se llevaron a cabo exposiciones interesantes a cargo de agentes

especializados del FBI, quienes abordaron temas actuales como la ciberdelincuencia, el lavado de activos, la lucha contra la corrupción y los delitos contra el patrimonio cultural, entre otros tópicos de gran relevancia.

Además, se contó con la participación de un alto representante de la Policía Nacional del Perú, quien presentó un análisis sobre los antecedentes y la coyuntura actual del terrorismo internacional. El sector privado también tuvo una destacada presencia, con representantes de las empresas Meta y Uber, que discutieron sobre seguridad tecnológica y su colaboración con las fuerzas del orden.

Es importante resaltar que esta fue la primera vez en la historia de la Asociación de Graduados del FBI (FBINAA) que se llevó a cabo un evento de tal magnitud en Perú. La conferencia fue un éxito rotundo, superando las expectativas gracias al trabajo en equipo de la División de Asuntos Internacionales del FBI, la Asociación de Graduados del FBI, la Oficina Regional del FBI en Santiago de Chile, la Oficina Legal del FBI en Lima, y la valiosa colaboración de la Policía Nacional del Perú a través de su Dirección de Asuntos Internacionales, que intervino tanto en la organización y seguridad del evento.

Participaron oficiales de policía de más de 14 países de la región, así como altos funcionarios del FBI, incluyendo al Director Adjunto de la División de Investigación Criminal, José Pérez, junto con Jefes Regionales y Agregados Legales Adjuntos del FBI.

LA IMPORTANTE CONTRIBUCIÓN DEL FBI EN PERÚ

Desde la creación de la oficina del FBI en el Perú a la fecha, la agencia ha desarrollado una importante labor de enlace con la Policía Nacional del Peru, el Ministerio Publico, el Poder Judicial y otras importantes entidades comprometidas con la seguridad nacional.

Gracias a una permanente labor de asesoramiento y cooperación técnica en investigaciones criminales, se han logrado realizar exitosas operaciones en apoyo a la Policía Nacional y operadores de justicia, para combatir el crimen organizado transnacional. Se suma a ello el enlace internacional con los diferentes países de la región de Latinoamérica y el Caribe para el logro de objetivos comunes en esta línea de acción.

Cabe destacar la importante gestión para la capacitación de un número significativo de operadores de justicia mediante cursos y talleres en temas especializados, como escena del crimen, formación de negociadores, cibercrimen y el programa anticorrupción, entre otros. Estos cursos han sido impartidos por instructores especialistas del FBI en Perú, Estados Unidos y otros países de la región.

COMENTARIO FINAL

El FBI, bajo su lema de “Fidelidad, Valentía e Integridad”, ha establecido una sólida presencia en la región, especialmente en Perú. Esta colaboración no sólo representa una oportunidad única para la Policía Nacional del Perú, sino también para los operadores de justicia locales, quienes podrán desarrollar una relación profesional de cooperación mutua con esta prestigiosa agencia.

Esta alianza con el FBI busca no solo desarticular redes criminales, sino también fomentar la justicia y la paz social en nuestras naciones. Al trabajar juntos, se espera construir un entorno más seguro para todos los ciudadanos, donde se respeten los derechos humanos y se promueva el desarrollo sostenible. Esta alianza es un paso importante hacia la consolidación de un enfoque integral en la lucha contra el crimen, que incluye la prevención, la investigación y la persecución efectiva de los delitos.

THE PRESENCE OF THE FBI IN PERU: A STRATEGIC ALLIANCE IN LATIN AMERICA AND THE CARIBBEAN IN THE FIGHT AGAINST TRANSNATIONAL ORGANIZED CRIME

For decades, impressive police chronicles have served as a source of inspiration for unforgettable Hollywood movies and American television shows. These portrayals have showcased complex criminal cases where investigators demonstrate their expertise in criminology and forensic sciences, gathering crucial evidence to uncover motives and identify the perpetrators.

However, beyond the fictional or imaginative elements in these stories, there exists a reality that reflects the arduous and dedicated work of police forces worldwide in combating organized crime. In this context, the Federal Bureau of Investigation (FBI), the criminal investigation agency of the U.S. Department of Justice, stands out for having earned international prestige over its 116 years of existence.

The mission of the FBI is to "protect the American people and uphold the Constitution of the United States." With jurisdiction over more than 200 federal crimes, its investigative areas range from national security and organized crime to public corruption and cybercrime, among other complex crimes.

It is important to note that the FBI's work is not confined to U.S. borders; its presence has also expanded to Latin America and the Caribbean. In this regard, the FBI has established significant cooperation in Peru, providing advice on criminal investigation and forensic science to the Peruvian police and national justice operators.

THE LEGAL ATTACHÉ PROGRAM

The FBI has a Legal Attaché program and maintains "63 Legal Attaché offices, commonly known as 'Legats,' and 30 smaller sub-offices in key cities worldwide, covering more than 180 countries, territories, and islands." "Each office is established through mutual agreement with the host country and is located in the U.S. embassy or consulate in that nation. The Legal Attaché program is managed by the International Operations Division at FBI headquarters in Washington, D.C. This office maintains close contact with other federal agencies, Interpol, foreign police forces, and security officials in Washington, as well as national and international law enforcement associations.

The program allows for international liaison and information exchange with foreign law enforcement agencies, in accordance with laws, treaties, and agreements between these agencies, to coordinate requests for mutual assistance and criminal investigations of common interest.

THE PRESENCE OF THE FBI IN PERU

For several years, Peru received temporary visits from FBI agents to coordinate with the Peruvian National Police, the Public Ministry, and related entities on the investigation of criminal acts with common links between Peru and the United States.

In 2016, the first talks began between the governments of Peru and the United States to establish an FBI office in Lima, Peru, to deepen areas already under collaboration, including the significant contribution that the FBI could provide in training Peruvian police in specialized criminal investigation topics, tactical operations, and advancements in forensic science as a hallmark of scientific policing.

THE CONSOLIDATION OF THE PROCESS

After a lengthy evaluation and authorization process managed by both countries, in November 2020, the FBI's Legal Attaché office was established at the U.S. Embassy in Peru. This office is under the regional jurisdiction of the FBI Legal Attaché office located in Santiago, Chile. Special Agent Norman Quilichini, an attorney with significant experience in criminal investigation, tactical operations, and the investigation of public official corruption crimes, was appointed as the Deputy Legal Attaché.

In addition, a position for a national investigator was created, which the author of this article, a graduate of FBINAA Session 136, currently occupies with honor.

FBINAA GRADUATES IN PERU

Perú has 11 officers from the Peruvian National Police who have graduated from the prestigious FBI Academy's international program. To date, this program has conducted 291 sessions, each lasting 10 weeks, training thousands of police officers from all 50 U.S. states, as well as 10,200 law enforcement agencies and 174 countries worldwide.

The graduates are part of the FBI National Academy Associates, Inc. (FBINAA), an international non-profit organization whose mission is "to inspire FBINAA members to continue serving the community, foster networks, and promote education and professional development throughout their policing careers and beyond.

The first Peruvian police officer to graduate from the FBI Academy was Major Inspector Alfonso Rivera Santander Herrera, who later became Director of the former Peruvian Investigative Police. Rivera Santander participated in the 71st session of the Academy on June 19, 1963, and is recognized for applying the knowledge acquired to improve investigation methods and develop forensic science in the Peruvian police, establishing a new technical and scientific structure.

Subsequent graduates have also made significant contributions to institutional development.

THE FIRST RETRAINING SESSION IN PERU

From May 21 to 23 of this year, Lima hosted the International Retraining Conference for Police Officers who graduated from the FBI Academy, Latin American and Caribbean Chapter. The main theme of this conference was "The Fight Against Transnational Organized Crime." During the event, specialized FBI agents gave insightful presentations on current topics such as cybercrime, money laundering, anti-corruption efforts, and crimes against cultural heritage, among other highly relevant subjects.

Additionally, a high-ranking representative of the Peruvian National Police presented an analysis of the background and current situation of international terrorism. The private sector also had a notable presence, with representatives from Meta and Uber discussing technological security and their collaboration with law enforcement agencies.

It is important to note that this was the first time in FBINAA history that an event of this magnitude was held in Peru. The conference was an outstanding success, exceeding expectations due to the teamwork of the FBI's International Affairs Division, the FBI Graduates Association, the FBI Regional Office in Santiago, Chile, the FBI Legal Attaché Office in Lima, and the valuable collaboration of the Peruvian National Police through its Directorate of International Affairs, which was involved in both organizing and securing the event.

Police officers from more than 14 countries in the region participated, as well as high-ranking FBI officials, including the Deputy Director of the Criminal Investigation Division, José Pérez, along with Regional Chiefs and Deputy Legal Attachés from the FBI.

THE SIGNIFICANT CONTRIBUTION OF THE FBI IN PERU

Since the establishment of the FBI office in Peru, the agency has developed a significant liaison role with the Peruvian National Police, the Public Ministry, the Judiciary, and other important entities committed to national security.

Thanks to ongoing advisory and technical cooperation efforts in criminal investigations, successful operations have been conducted in support of the National Police and justice operators to combat transnational organized crime. This is complemented by international cooperation with various countries in the Latin American and Caribbean region to achieve common objectives in this area.

It is worth noting the important initiatives to train a significant number of justice operators through specialized courses and workshops on topics such as crime scene management, negotiator training, cybercrime, and the anti-corruption program, among others. These courses have been taught by specialized FBI instructors in Peru, the United States

FINAL COMENT

The FBI, under its motto of "Fidelity, Bravery, and Integrity," has established a strong presence in the region, especially in Peru. This collaboration represents not only a unique opportunity for the Peruvian National Police but also for local justice operators, who will be able to develop a professional relationship of mutual cooperation with this prestigious agency.

This alliance with the FBI aims not only to dismantle criminal networks but also to foster justice and social peace in our nations. By working together, we hope to build a safer environment for all citizens, where human rights are respected, and sustainable development is promoted. This alliance is an important step toward consolidating a comprehensive approach to fighting crime, including prevention, investigation, and effective prosecution of offenses.

JULIO G. BERNAL CAVERO

Attorney

Attorney
Master of Law in Criminal Sciences
FBI Foreign Service National Investigator

National Investigator of the FBI Foreign Service, U.S. Embassy, Lima, Peru. Retired Senior Officer of the National Police of Peru, Lawyer, Master in Law with a specialization in Criminal Sciences.

References

1 “Oficinas en el extranjero”, FBI web page, https://www.fbi.gov/
2 El Perú propone a EEUU abrir una oficina del FBI en Lima”, RRPP Redacción https://rpp.pe/lima/seguridad/peru-plantea-a-eeuu-abrir-una-oficina-del-fbi-en-lima-noticia-01 de marzo de 2016
3 “FBINAA News Release September 12, 2024”
4 https://www.fbinaa.org/about-us/about-the-fbinaa/

MI EXPERIENCIA EN FBINAA YLP
POR SOFÍA ARAYA BUSTAMANTE

Este programa cambió mi vida, transformando mi percepción respecto al mundo y a mis propios límites. YLP me ayudó a conocerme, a mi formación como persona y a definir quién quiero ser y cómo voy a aportar a nuestra sociedad.

El proceso de selección me asustó bastante, tener que escribir un ensayo respecto a una temática tan amplia como lo es "cuál es el factor más importante al que se enfrentan los adolescentes en la sociedad actual" fue un reto complicado de asumir.

Tuve muchas ideas y diferentes problemáticas para plantear, pero nuestros entornos son distintos, por lo que en otras partes del mundo seguramente deben enfrentarse a otras cosas iguales de importantes. Por otro lado, la entrevista en un idioma que no es mi lengua materna me mantuvo expectante y nerviosa semanas completas. A pesar de lo aterrador que suene esto, puedo afirmar que todo valió la pena.

En medio de mi clase de argumentación llegó el correo electrónico que más esperaba: la respuesta de la Academia. Antes de que pudiese abrir la carta, mi coordinadora del programa ya estaba felicitándome por la aceptación, esto me hizo mucha gracia, puesto que me ahorró los nervios de leer la carta y la expectación de esta.

"Buenos días Sofía. Por favor revisa tu correo, ha llegado la carta de aceptación de la academia" o "¡¡¡Felicidades!!! Es una experiencia única en la vida".

Ya en el Aeropuerto Nacional Ronald Reagan me recibieron con mucho cariño y amabilidad, mi consejera y algunos jóvenes estaban esperando a los demás chicos que faltaban, mis nervios se esfumaron y me relacioné con todos, compartimos nuestros gustos e intereses, de donde veníamos y como era nuestra realidad.

Lily (la chica de la izquierda) me acompañó durante todo el viaje, nos conocimos en el aeropuerto y prácticamente me cuidó durante mi estadía en Estados Unidos, ayudándome a escoger mis almuerzos, compartiendo sus apuntes y explicando cosas que se me dificultaban entender, cómo en nuestro paseo por Fredericksburg Battlefield o algunas de las atracciones en Washington D.C.

Cada día fue una aventura diferente, Hollie (mi roommate) y yo nos levantamos una semana entera alrededor de las 5 a.m. dado que el entrenamiento físico empezaba a las 6:00 a.m. hasta las 7:15 a.m., donde hacíamos distintas actividades como juegos o que incluían correr, trabajar en equipo y motivarnos entre compañeros.

Las clases teóricas fueron muy entretenidas y variadas, algunas de ellas son Fitness and Nutrition; Understanding Self; Time Management; Leadership Fundamentals; Situational Leadership; Decision Making; Public Speaking and Interviewing; Perseverance Through Adversity; Ethics, Values and Integrity y más. La clase que más me gustó fue Perseverance Through Adversity, donde nos enseñaron cómo avanzar junto al cambio, adaptarnos a distintas situaciones y que nada es un impedimento.

Partimos la clase con la pregunta de qué nos podría impedir cumplir nuestros objetivos, muchos jóvenes hicieron referencias a discapacidades físicas como la falta de alguna extremidad, pero después de ver ejemplos de personas que enfrentan adversidades y cumplieron objetivos a pesar de tener discapacidades físicas como no poder caminar, logramos entender que las limitaciones las creamos nosotros mismos y que estamos a cargo de cambiar nuestra mentalidad para poder cumplir desafíos u objetivos.

Visitamos Washington D.C., donde compartí junto a mis amigos increíbles experiencias y conocí muchas cosas nuevas respecto a la historia de EE.UU. También fuimos a Fredericksburg, donde nos enseñaron sobre la batalla ocurrida en el contexto de la Guerra de Secesión. Visitamos el cementerio de Arlington, donde vimos la tumba de John F. Kennedy. ¡Fuimos al Capitolio! ¡Mi parte favorita del viaje a Washington, sin dudas! Aunque también amé ver the Sunset Parade, todo fue increíble.

¡Una de las cosas que me impresionó fue ver ciervos y ardillas! Me encantan los animales por lo que tomé muchas fotos de estos.

Una de las cosas que más amé durante esta experiencia fue the Yellow Brick Road, donde todos nos unimos para poder superar esta gran prueba, apoyándonos en el camino mientras corríamos alrededor de 5km en un bosque. Creo que no hay algo más satisfactorio que llegar a la meta junto a tus amigos y ver el arduo esfuerzo de una semana completa, a día de hoy es uno de mis mayores orgullos.

Este programa me enseñó y me mostró muchas cosas positivas que puedo comentar respecto a mis vivencias de este.

Las personas que conocí en este, los valores aprendidos, como poder ser grandes líderes en nuestro entorno.

Durante ese tiempo no solo adquirí herramientas que me ayudaron a mejorar mis habilidades de liderazgo, sino que también aprendí a poner en práctica lo aprendido a través de diversas actividades grupales y desafíos que me hicieron desplazarme fuera de mi zona de confort. Además, el ambiente de compañerismo y apoyo mutuo que se creó entre todos los participantes de este programa fue increíblemente enriquecedor.

La oportunidad que se me otorgo de intercambiar experiencias con jóvenes de diferentes partes del mundo con diferentes culturas fue una experiencia invaluable, gracias a esto pude ampliar mi visión del mundo. Cada día en el programa fue una oportunidad distinta y nueva para crecer tanto como personal como profesionalmente. Sin lugar a dudas, esta experiencia me dejó muchos recuerdos imborrables y una gran motivación para seguir trabajando y esforzándome por un futuro mejor. ¡No me quedan palabras suficientes para describir la gran experiencia que el programa YLP me otorgó!

MY EXPERIENCE AT FBINAA YLP
BY SOFÍA ARAYA BUSTAMANTE

This program changed my life, transforming my perception of the world and my own limits. YLP helped me to know myself, to develop myself as a person and to define who I want to be and how I am going to contribute to our society.

The selection process scared me quite a bit; having to write an essay on a topic as broad as "what is the most important factor that teenagers face in today's society" was a difficult challenge to take on.

I had many ideas and different problems to raise, but our environments are different, so in other parts of the world they must surely face other equally important things. On the other hand, the interview in a language that is not my mother tongue kept me expectant and nervous for weeks. Despite how scary this sounds; I can say that it was all worth it.

In the middle of my argumentation class, the email I was most looking forward to arrive: the response from the Academy. Before I could open the letter, my program coordinator was already congratulating me on my acceptance. This made me laugh a lot, since it saved me the nerves of reading the letter and the anticipation of it.

"Good morning, Sofia. Please check your mail, the acceptance letter from the academy has arrived" or "Congratulations!!! It is a once in a lifetime experience."

Already at Ronald Reagan National Airport I was greeted with much love and kindness.
My counselor and some young people were waiting for the other students who were missing. My nerves vanished and I interacted with everyone, we shared our tastes and interests, where we came from and what our reality was like.

Lily (the girl on the left) accompanied me throughout the trip. We met at the airport and she practically took care of me during my stay in the United States, helping me choose my lunches, sharing her notes and explaining things that were difficult for me to understand, such as our walk-through Fredericksburg Battlefield or some of the attractions in Washington D.C.

Every day was a different adventure. Hollie (my roommate) and I got up around 5 a.m. for a whole week since physical training started at 6:00 a.m. until 7:15 a.m., where we did different activities such as games or that included running, teamwork and motivating each other.

The theoretical classes were very entertaining and varied. Some of them are Fitness and Nutrition; Understanding Self; Time Management; Leadership Fundamentals; Situational Leadership; Decision Making; Public Speaking and Interviewing; Perseverance Through Adversity; Ethics, Values and Integrity and more. The class I liked the most was Perseverance Through Adversity, where they taught us how to move forward with change, adapt to different situations and that nothing is an impediment.

We started the class with the question of what could prevent us from achieving our goals. Many young people made references to physical disabilities such as the lack of a limb, but after seeing examples of people who face adversity and achieved goals despite having physical disabilities such as not being able to walk, we came to understand that we create limitations ourselves and that we are in charge of changing our mindset in order to meet challenges or goals.

We visited Washington D.C., where I shared incredible experiences with my friends and learned many new things about U.S. history. We also went to Fredericksburg, where they taught us about the battle that occurred in the context of the Civil War. We visited Arlington Cemetery, where we saw John F. Kennedy's grave. We went to the Capitol! My favorite part of the trip to Washington, without a doubt! Although I also loved watching the Sunset Parade, everything was amazing.

One of the things that impressed me was seeing deer and squirrels! I love animals so I took a lot of photos of them.

One of the things I loved the most during this experience was the Yellow Brick Road, where we all came together to overcome this great test, supporting each other along the way while we ran around 5km in a forest. I think there is nothing more satisfying than reaching the finish line with your friends and seeing the arduous effort of a whole week, today it is one of my greatest prides.

This program taught me and showed me many positive things that I can comment on regarding my experiences of it.

The people I met in it, the values learned, how to be great leaders in our environment.

During that time, I not only acquired tools that helped me improve my leadership skills, but I also learned to put into practice what I learned through various group activities and challenges that made me move outside my comfort zone. Furthermore, the atmosphere of camaraderie and mutual support that was created among all the participants of this program was incredibly enriching.

The opportunity I was given to exchange experiences with young people from different parts of the world with different cultures was an invaluable experience, thanks to which I was able to broaden my vision of the world. Every day in the program was a different and new opportunity to grow both personally and professionally. Without a doubt, this experience left me with many indelible memories and a great motivation to continue working and striving for a better future. I do not have enough words to describe the great experience that the YLP program gave me!

Sofía Araya Bustamante

Tengo 16 años y voy en III° medio en el colegio de los Sagrados Corazones de Providencia, en Santiago, Chile.

Disfruto de actividades como tejer, pintar con lápices pasteles, ver deportes y jugar videojuegos. Me gusta mucho compartir tiempo de calidad junto a mis amigos, siempre vamos a parques o jugamos partidos de fútbol.

Uno de mis mayores sueños es poder estudiar economía en el extranjero, específicamente en alguna universidad de Estados Unidos ¡por lo que planeo postular para el año 2025!

LA INTELIGENCIA EN LOS ESCALONES DE LA LUCHA POLICIAL

Con base en las experiencias de las operaciones policiales y el ejercicio real táctico vivido en campo, así como de la academia e investigaciones desarrolladas, apartándonos del uso de estadísticas, o de cifras e informes, dada su trascendental relevancia, aquí se evidencia lo que no se ha podido apreciar en su dimensión real y necesaria con relación a la inteligencia del primer escalón de la lucha policial, no solamente como proceso destinado a recopilar, organizar, analizar y utilizar sistemáticamente la información para la toma de decisiones de la operación policial de las fuerzas del orden, pues resulta necesario que se reconozca e identifique la ausencia de planeación operacional destinada a garantizar la máxima seguridad posible de todo elemento que participe en la función policial, den cualquiera de sus fracciones operacionales y tácticas o escalones, que, quizá sin mala fe, pero eso sí, por causas ajenas a los integrantes de los cuerpos policiales, por descuido o desconocimiento profesional en la materia, no en la teoría, sino en la realidad.

La carencia que se registra en el trabajo de campo de las operaciones policiales se ha perdido en el olvido de los hechos y de los informes carentes de análisis y registro que sirva a la lucha policial; es así que debe advertirse que no obstante la teoría, el desconocimiento de la inteligencia del primer escalón de la lucha policial se constituye en una vulnerabilidad de relevante trascendencia, porque regularmente se substituye por el inadecuado uso de un algoritmo que altera la realidad y la verdad de las cosas, que pende solamente del ánimo de justificar otras cuestiones ajenas a la lucha policial; evidencia de ello es apreciable en la publicación de la investigación científica policial mediante la cual demostré la existencia del "fenómeno de la inseguridad pública objetiva que surge cuando la sociedad se encuentra verdaderamente convencida de la existencia de la inseguridad" (Luna-Alatorre B. página 93, 1998), como resultado de la ausencia de seguridad en el entorno social y personal de la población en general, no solamente de la sociedad, sino también de los mismos integrantes de los cuerpos policiales, fundamentalmente en el desarrollo de su actuación en campo, pues en la citada investigación se evidenció que "regularmente en los enfrentamientos armados entre policías y delincuentes, el servidor público resulta con mayores lesiones provocadas por arma de fuego que el delincuente" (op.cit),

Enfrentamiento que se desarrolla en lugares o procesos críticos, variables y múltiples, regularmente "en reacción" o en respuesta a actos ofensivos de los delincuentes, que suceden en un intervalo corto de tiempo y espacio reducido, del que suele desconocerse el terreno, además que para ello no existe un plan de actuación sostenido en la información vinculada a la capacidad de fuego y numero de los atacantes, lo que interfiere en la consecución de las finalidades tácticas policiales, sobre todo, en las técnicas utilizadas para las acciones que se desarrollan en campo, y otras, que de manera global pueden afectar el funcionamiento policial, puesto que a sus integrantes, los de los cuerpos policiales, ni siquiera se les permite apegarse al principio que garantiza el derecho inminente a la legitima "defensa individual o colectiva" que se encuentra reconocido desde 26 de junio del año 1945, en el artículo 51 de la Carta de las Naciones Unidas, lo que se suma a la incertidumbre sobre el intervalo de tiempo en el que acudirán las células de refuerzos del punto de control policial más próximo al lugar del enfrentamiento, lo que también suele pasar en persecución, localización y presentación de delincuentes.

Es lamentable que la inteligencia del primer escalón de la lucha policial, es decir, la inteligencia que se encuentra en forma directa y estrecha con el fin, misión y objetivo de garantizar la seguridad de todos los integrantes de los cuerpos e instituciones que participan en la lucha policial, ni antes ni ahora se registra en América Latina y el Caribe, no obstante que es una región geopolítica que comprende más de 40 países y territorios desde México hasta el Cabo de Hornos, como si lo expuesto por Manfred Kossok respecto a "la falta de escritos serios acerca de la militarización latinoamericana" ("Nuestras Metas y Supuestos", Compendio de Lecturas requeridas, Colegio de Defensa Nacional, Décimo Tercera Antigüedad, pagina 171, México 1994) fuese el único fenómeno que ha sido registrado, puesto que las cuestiones conceptuales, semánticas y metodológicas utilizadas en la realidad confunden la operación policial con la investigación policial, y la inteligencia policial con la inteligencia criminal y en otros casos se pierden no obstante que su objetivo se generar inteligencia estratégica que sirva a la toma de decisiones, por un ciclo de acciones de recolección, procesamiento y análisis de información, en la que se excluye la destinada a la seguridad del elemento que participa en la lucha policial.

INTELLIGENCE IN THE STEPS OF THE POLICE STRUGGLE

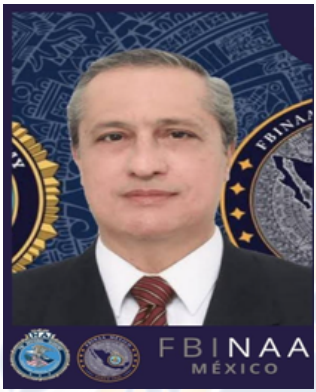
Based on the experiences of police operations and the real tactical exercise lived in the field, as well as the academy and research developed, moving away from the use of statistics, or figures and reports, given their transcendental relevance, here is evidenced what has not been able to be appreciated in its real and necessary dimension in relation to the intelligence of the first echelon of the police struggle, not only as a process destined to collect, organize, analyze and systematically use information for decision making in the police operation of the forces of order, since it is necessary to recognize and identify the absence of operational planning destined to guarantee the maximum possible security of all elements that participate in the police function, in any of its operational and tactical fractions or echelons, which, perhaps without bad faith, but that's right, for reasons beyond the control of the members of law enforcement, due to carelessness or professional ignorance of the matter, not in theory, but in reality

The lack that is recorded in the field work of police operations has been lost in the oblivion of the facts and reports lacking analysis and registration that serve the police fight; thus, it must be noted that despite the theory, the ignorance of the intelligence of the first echelon of the police fight constitutes a vulnerability of relevant importance, because it is regularly replaced by the inappropriate use of an algorithm that alters reality and the truth of things, which depends only on the desire to justify other issues outside the police fight; Evidence of this is noticeable in the publication of the scientific police research through which it demonstrated the existence of the "phenomenon of objective public insecurity that arises when society is truly convinced of the existence of insecurity" (Luna-Alatorre B. page 93, 1998), as a result of the absence of security in the social and personal environment of the population in general not only of society, but also of the members of the police forces themselves, mainly in the development of their performance in the field, since in the cited research it is evident that "regularly in armed confrontations between police and criminals, the public servant ends up with greater injuries caused by firearms than the criminal" (op. cit)

Confrontation that takes place in critical, variable and multiple places or processes, regularly "in reaction" or in response to offensive acts by criminals, which occur in a short interval of time and reduced space, of which the terrain is usually unknown, in addition to the fact that there is no action plan sustained in the information linked to the fire capacity and number of the attackers, which interferes with the achievement of tactical police objectives, especially in the techniques used for actions carried out in the field, and others, which globally can affect police operations, since its members, those of the police forces, are not even allowed to adhere to the principle that guarantees the imminent right to legitimate "individual or collective defense" that has been recognized since June 26, 1945, in Article 51 of the United Nations Charter,

Which adds to the uncertainty about the time interval in which reinforcement cells will arrive from the police checkpoint closest to the scene of the confrontation, which also usually happens in the pursuit, location and presentation of criminals.

It is regrettable that the intelligence of the first echelon of the police struggle, that is, the intelligence that is directly and closely related to the purpose, mission and objective of guaranteeing the security of all members of the bodies and institutions that participate in the police struggle, is neither before nor now recorded in Latin America and the Caribbean despite the fact that it is a geopolitical region that includes more than 40 countries and territories from Mexico to Cape Horn, as if what Manfred Kossok stated regarding "the lack of serious writings about Latin American militarization" ("Our Goals and Assumptions", Compendium of Required Readings, National Defense College, Thirteenth Antiquity, page 171, Mexico 1994) was the only phenomenon that has been recorded, since the conceptual, semantic and methodological issues used in reality confuse the police operation with the police investigation, and police intelligence with criminal intelligence and in other cases they are lost despite the fact that their objective is to generate strategic intelligence that serves the decision-making process.



Benjamín Luna-Alatorre

Professional profile

Benjamín Luna-Alatorre is a graduate of the FBI National Academy Session 198, and a founding member of the FBI NAA Group Mexico, and he studied "Criminal Justice Education" at the University of Virginia, USA; since 1986 he has a Bachelor's Degree in Law from the National Autonomous University of Mexico UNAM; in 1994 he obtained by "Acclamation" the Master's Degree in Military Administration for National Security and Defense, National Defense College - University of the Mexican Army and Air Force, UDEFAM-Thirteenth Seniority, in which Military Educational Institution he was a Lecturer in several seniorities; he has a Doctorate in Law from the UNITECH University; he has a Doctorate in Education and Educational Administration from the UNIDEP University; In 1988 he was promoted from the rank of Captain to Major of Military Justice, where he served as Agent of the Military Public Ministry of the Seventh Army Corps, VII Region and 31st Military Zone; 1992- April 1995, he was Administrator of Prevention of Tax Crimes (Intelligence) and Deputy Administrator of the Federal Fiscal Police; 1995: Director of Political Coordination of the Government of the State of Mexico (Intelligence); 1995 Member of the Anti-Terrorism Cabinet GAT-CISEN; December 23, 1997: General Director of Criminal Policy and Fight against Crime of the Attorney General's Office of the State of Mexico; May 1, 1999: General Director of Homicide Investigation of the Attorney General's Office of the Federal District, today Mexico City; 2005 to 2007: Manager and Legal Director and Head of the Transparency Liaison Unit of the parastatal called Administración Portuaria Integral de Manzanillo, S.A. de C.V.; March 2016-March 2019, Counselor of the Human Rights Commission of the State of Colima; July 2019-2021, Alternate Commissioner of the General Commission for the Comprehensive Protection of the Practice of Journalism of the State of Colima "COPIP", March 2017- August 2020, President of the Advisory Council of the Institute for Transparency, Access to Public Information and Data Protection of the State of Colima.

ARMAS FANTASMAS EN EL CARIBE: LA AMENAZA EMERGENTE DE LAS ARMAS DE FUEGO IMPRESAS EN 3D

Una de las principales preocupaciones en el Caribe en los últimos años son las armas de fuego de fabricación privada (PMF), también conocidas como "armas fantasma" fabricadas mediante tecnología de impresión 3D. Las armas de fuego y sus componentes se fabrican de forma sencilla mediante impresoras 3D importadas, como se muestra en la Figura 1, con planos descargables y materiales de fácil acceso (Small Arms Survey, 2024). La falta de un marco regulatorio que regule la importación de impresoras 3D y el fácil acceso a esta tecnología plantea serias preocupaciones en relación con la seguridad pública y la seguridad nacional en toda la región.

Este artículo examina los desafíos que plantean las armas de fuego y los componentes impresos en 3D ilegales en el Caribe, las dificultades para la aplicación de la ley y las deficiencias de la legislación actual.

EL SURGIMIENTO DE LAS ARMAS DE FUEGO IMPRESAS EN 3D

El Caribe refleja la tendencia mundial de aumento de la producción de PMF. La primera incautación importante de componentes para armas impresas en 3D en el Caribe ocurrió en Trinidad y Tobago en 2023.

Tras ese suceso, varias otras islas del Caribe, como Barbados, Antigua y Jamaica, también han visto un repunte en la incautación de componentes de armas de fuego impresos en 3D; en particular, receptores de armas de fuego (Loop News, 2023). La Oficina de Aduanas y Protección Fronteriza de los Estados Unidos informó que las tasas mensuales de interceptación de receptores y kits de armas de fuego impresos en 3D con destino al Caribe experimentaron un asombroso aumento del 600% en 2023 en comparación con el período de 2016 a 2021 (Small Arms Survey, 2024).

El 4 de septiembre de 2024 se produjo una incautación especialmente notable en Barbados: agentes de policía de la Unidad Anti-Armas y Pandillas incautaron doce (12) receptores de pistola impresos en 3D (véase la Figura 2). Esta incautación puso de relieve la facilidad con la que los particulares, sin antecedentes penales y sin experiencia aparente con armas de fuego, pueden adquirir las habilidades técnicas necesarias para fabricar un arma de fuego en su totalidad o en parte (Wenzinger et al, 2024).

DESAFÍOS PARA LAS FUERZAS DEL ORDEN

La proliferación de armas de fuego impresas en 3D presenta un desafío multifacético para las fuerzas del orden en todo el Caribe. Principalmente, los materiales utilizados para construirlas (filamentos, polímeros plásticos y termoplásticos) no son fácilmente detectados por las medidas de seguridad convencionales. Por lo tanto, es probable que los espacios más seguros de la sociedad, como los juzgados, los aeropuertos y los puertos marítimos, se vean comprometidos (BBC News, 2018).

La naturaleza digital de las armas de fuego aumenta la complejidad. Los planos de las armas se pueden descargar de Internet y luego compartir sin necesidad de permiso de una autoridad internacional. Este tipo de descentralización de la fabricación de armas de fuego hace que los viejos métodos de

seguimiento de las ventas y transferencias de armas sean prácticamente inútiles, lo que es una capa crucial de monitoreo de las fuerzas del orden.

Las fuerzas del orden del Caribe a menudo carecen de los recursos financieros y la capacitación para analizar las armas de fuego impresas en 3D de manera efectiva. Mientras que las armas de fuego tradicionales tienen marcas balísticas distintivas, las armas producidas por impresoras 3D pueden alterarse de tal manera que eludan por completo el análisis balístico. Esto presenta un obstáculo importante para los expertos forenses que intentan vincular estas armas a delitos específicos, lo que obstaculiza los esfuerzos de investigación (Daly et al., 2021).

LA NECESIDAD DE SOLUCIONES LEGISLATIVAS Y REGULATORIAS

La falta de legislación permite a las personas fabricar estas armas o parte de ellas sin riesgo de procesamiento. Es necesaria la introducción de un marco regulatorio para la importación y compra de impresoras 3D. Esto no solo requeriría leyes, sino también mecanismos para su aplicación. Un sistema de licencias que se aplique a las impresoras 3D, las personas y las empresas que tengan la intención de utilizarlas otorgaría a las fuerzas del orden una mayor capacidad de supervisión y regulación (Guardian, 2023).

Además, existe una necesidad urgente de monitorear las plataformas en línea que difunden planes e instrucciones paso a paso para fabricar armas impresas en 3D. Por lo tanto, se alienta firmemente a los organismos encargados de hacer cumplir la ley del Caribe a que colaboren con sus homólogos internacionales, como la Oficina Federal de Investigaciones (FBI), la Oficina de Alcohol, Tabaco, Armas de Fuego y Explosivos (ATF), Interpol y Europol, para identificar, atacar y desmantelar los sitios web que promueven la producción ilegal de armas de fuego (Daly et al., 2021).

CONCLUSIÓN

El aumento de las armas fantasma y las armas de fuego impresas en 3D presenta un desafío importante para la seguridad del Caribe. La accesibilidad de las impresoras 3D y la ausencia de cualquier legislación crean un problema importante. Se puede esperar una mayor escalada si no se toman medidas regulatorias inmediatas, lo que podría socavar los esfuerzos de seguridad y protección nacional de la región.

Las naciones caribeñas deben implementar rápidamente marcos regulatorios para las impresoras 3D, al tiempo que mejoran las capacidades forenses y fomentan la cooperación internacional para combatir la propagación de las armas fantasma en toda la región.

GHOST GUNS IN THE CARIBBEAN: THE EMERGING THREAT OF 3D-PRINTED FIREARMS

A major concern in the Caribbean in recent years are privately manufactured firearms (PMFs), also known as "ghost guns" manufactured using 3D printing technology. Firearms and firearm components are being made straightforwardly using imported 3D printers, as shown in Figure 1, with downloadable blueprints and easily accessible materials (Small Arms Survey, 2024). The lack of a regulatory framework governing the importation of 3D printers and easy access to this technology raises serious concerns regarding public safety and national security across the region.

This article examines the challenges posed by illegal 3D-printed firearms and components in the Caribbean, the difficulties for law enforcement, and the shortcomings in current legislation.

THE EMERGENCE OF 3D-PRINTED FIREARMS

The Caribbean mirrors the global trend of increasing production of PMFs. The first major seizure of components for 3D-printed guns in the Caribbean occurred in Trinidad and Tobago in 2023.

Following that occurrence, several other Caribbean islands such as Barbados, Antigua and Jamaica have also seen an uptick in the seizure of 3D printed firearm components; particularly firearm receivers (Loop News, 2023). U.S. Customs and Border Protection reported that the monthly interception rates of Caribbean-bound 3D-printed firearm receivers and kits saw a staggering 600% increase in 2023 compared to the period from 2016 to 2021 (Small Arms Survey, 2024).

A particularly notable seizure occurred in Barbados on September 4, 2024, police officers from the Anti-Gun and Gangs Unit seized twelve (12) 3D printed pistol receivers (see Figure 2). This seizure highlighted the ease with which private individuals; with no criminal record and no apparent experience with firearms, can acquire the necessary technical skills to manufacture a firearm in whole or in part (Wenzinger et al, 2024).

CHALLENGES FOR LAW ENFORCEMENT

The proliferation of 3D-printed firearms presents a multifaceted challenge for law enforcement agencies across the Caribbean. Chiefly, the materials used to construct them (filament, plastic polymers and thermoplastics) are not easily detected by conventional security measures. Therefore, society's most secure spaces; such as courthouses, airports, and seaports, is likely to be compromised (BBC News, 2018).

The digital nature of firearms adds to the complexity. The plans for the weapons can be downloaded from the internet and subsequently shared with no permission needed from international authority. This sort of decentralisation of firearm manufacturing makes the old methods of keeping track of gun sales and transfers all but impotent, which is a crucial layer of law enforcement monitoring.

Caribbean law enforcement agencies often lack the financial resources and training to analyse 3D-printed firearms effectively. Whereas traditional firearms bear distinctive ballistic markings, guns produced by 3D printers can be altered in such a manner as to elude ballistic analysis altogether.This presents a significant hurdle for forensic experts attempting to link these weapons to specific crimes, thereby stymieing investigative efforts (Daly et al., 2021).

THE NEED FOR LEGISLATIVE AND REGULATORY SOLUTIONS

The lack of legislation allows individuals to manufacture these weapons or part thereof without the risk of prosecution. The introduction of a regulatory framework for the importation and purchase of 3D printers is necessary. This would not only necessitate laws but also the mechanisms for their enforcement. A licensing system that applies to 3D printers, people and businesses that intend to utilize them would position law enforcement with more oversight and regulatory capabilities (Guardian, 2023).

In addition, there is an urgent need to monitor online platforms that disseminate plans and step-by-step instructions for making 3D-printed guns. Therefore, Caribbean law enforcement agencies are strongly encouraged to collaborate with their international counterparts, such as the Federal Bureau of Investigations (F.B.I), the Bureau of Alcohol, Tobacco, Firearms and Explosives (A.T.F), Interpol and Europol, to identify, target and dismantle websites that promote the illegal production of firearms (Daly et al., 2021).

CONCLUSION

The rise of ghost guns and 3D-printed firearms presents a significant challenge to the security of the Caribbean. The accessibility of 3D printers and the absence of any legislation creates a major problem. Further escalation can be expected without immediate regulatory action, potentially undermining the region's safety and national security efforts.

Caribbean nations must swiftly implement regulatory frameworks for 3D printers while enhancing forensic capabilities and fostering international cooperation to combat the spread of ghost guns throughout region.

DWAYNE S. CUMBERBATCH

Member of the FBI National Academy Associates and represents the Latin America and Caribbean Chapter. He attended the F.B.I National Academy at Session 289. He is from the country Barbados and he is the Inspector i/c of the Serious Organized Crime Unit (S.O.C.U) of the Barbados Police Service. He has been a police officer for 22 years and spent majority of his career as a detective in the Criminal Investigations Department. He is an Attorney at law, and was called to the Bar in Barbados in 2018. In 2021, he was placed in charge of the Anti-Gun and Gangs Unit (A.G.G.U), which is responsible for firearm interdiction and gang infiltration. In 2024, the Anti-Gun and Gangs Unit was renamed the Serious Organized Crime Unit, to assist with organized crime, gang violence and firearm interdiction.

References

- BBC News.(2018, July 31).US issues blueprints for 3D-printed guns despite injunction.https://www.bbc.co.uk/news/world-us-canada-45011351
- Cayman Compass.(2024, May 28).Changes to firearms legislation to outlaw 3D-printed guns.https://www.caymancompass.com/2024/05/28/changes-to-firearms-legislation-to-outlaw-3d-printed-guns/
- Daly, A., Mann, M., Squires, P., & Walters, R. (2021).3D printing, policing and crime.Policing and Society: An International Journal of Research, 31(1), 37-51.https://doi.org/10.1080/10439463.2020.1730835
- Guardian.(2023, October 10).Experts: 3D-printed guns not worth criminals' effort.https://www.guardian.co.tt/news/experts-3dprinted-guns-not-worth-criminals-effort-6.2.1693115.9627c91ed1
- Loop News.(2023, October 8).Police seize ghost guns being manufactured in Trinidad.https://caribbean.loopnews.com/content/police-seize-ghost-guns-being-manufactured-trinidad
- Small Arms Survey.(2024).Dangerous devices: Privately made firearms in the Caribbean.https://www.smallarmssurvey.org/dangerous-devices-privately-made-firearms-caribbean/developments-since-april-2023
- Wenzinger, Z. E., Wetzel, S., Bernarding, B., Viator, J., Kohlhepp, B., & Marshall, P. (2024). The relevance of current forensic firearms examination techniques when applied to 3D-printed firearms.Journal of Forensic Sciences, 69(2), 659–668.https://doi.org/10.1111/1556-4029.15467

En la era digital actual, donde la información es un activo invaluable y la conectividad es omnipresente, la ciberseguridad se ha convertido en una preocupación crítica para individuos, empresas y gobiernos por igual. Frente a la creciente sofisticación y diversidad de las amenazas cibernéticas, es imperativo adoptar estrategias y medidas efectivas para proteger nuestros activos digitales y garantizar la integridad y la confidencialidad de nuestros datos (Accinelli, 2024).

1.Concientización y Educación: Una de las primeras líneas de defensa en ciberseguridad es la concientización y la educación de los usuarios. Es fundamental que tanto individuos como empleados de empresas comprendan los riesgos asociados con el uso de tecnologías digitales y estén al tanto de las mejores prácticas de seguridad cibernética. Esto incluye la capacitación regular sobre cómo identificar y evitar ataques de phishing, cómo crear contraseñas seguras, cómo proteger la información confidencial y cómo utilizar de manera segura los dispositivos y las redes (Accinelli, 2024).

2. Implementación de Medidas de Seguridad Técnicas: Adem·s de la concientización, es crucial implementar medidas técnicas de seguridad para proteger sistemas, redes y datos contra amenazas cibernéticas. Esto incluye la instalación y actualización regular de software antivirus y antispyware, la configuración de firewalls para controlar el tráfico de red, la implementación de autenticación multifactor para acceder a sistemas y datos sensibles, y el cifrado de datos tanto en reposo como en tránsito para proteger la confidencialidad de la información. (Reuters, 2019)

3. Monitoreo y Detección de Amenazas: Otra estrategia importante en ciberseguridad es la implementación de sistemas de monitoreo y detección de amenazas. Esto implica el uso de herramientas de seguridad de red y de sistemas que puedan identificar actividades sospechosas o anomalías en el tráfico de datos y alertar a los administradores de seguridad para que puedan responder rápidamente a posibles incidentes. El monitoreo continuo y la respuesta proactiva son fundamentales para minimizar el impacto de las brechas de seguridad y las violaciones de datos.

4. Gestión de Vulnerabilidades y Parches: La gestión de vulnerabilidades es una parte integral de cualquier estrategia de ciberseguridad efectiva. Esto implica identificar y remediar activamente las vulnerabilidades en sistemas y aplicaciones mediante la implementación oportuna de parches de seguridad y actualizaciones de software. Las organizaciones deben establecer procesos y políticas claras para la evaluación y la gestión de riesgos, así como para la aplicación de parches de seguridad de manera regular y sistemática (Reuters, 2019).

5. Planificación de Respuesta a Incidentes: Por último, pero no menos importante, las organizaciones deben desarrollar y poner en práctica planes de respuesta a incidentes para gestionar de manera efectiva las brechas de seguridad y los ataques cibernéticos. Esto incluye la designación de un equipo de respuesta a incidentes, la definición de roles y responsabilidades, la creación de protocolos de comunicación y coordinación, y la realización de simulacros periódicos para poner a prueba la efectividad del plan y garantizar una respuesta rápida y coordinada en caso de emergencia (Reuters, 2019).

La ciberseguridad es un desafío continuo y en constante evolución en la era digital actual. Adoptar estrategias y medidas efectivas de ciberseguridad es fundamental para proteger nuestros activos digitales, preservar la confidencialidad y la integridad de nuestros datos y garantizar la continuidad de nuestras operaciones en un mundo cada vez más conectado. Mediante la concientización, la educación, la implementación de medidas técnicas de seguridad, el monitoreo y la detección de amenazas, la gestión de vulnerabilidades y la planificación de respuesta a incidentes, podemos fortalecer nuestras defensas cibernéticas y enfrentar los desafíos de seguridad digital con confianza y resiliencia.

In the current digital era, where information is an invaluable asset and connectivity is ubiquitous, cybersecurity has become a critical concern for individuals, businesses, and governments alike. In the face of the growing sophistication and diversity of cyber threats, it is imperative to adopt effective strategies and measures to protect our digital assets and ensure the integrity and confidentiality of our data (Accinelli, 2024).

1.Awareness and Education: One of the first lines of defense in cybersecurity is user awareness and education. It is essential that both individuals and company employees understand the risks associated with the use of digital technologies and are aware of best cybersecurity practices. This includes regular training on how to identify and avoid phishing attacks, how to create secure passwords, how to protect confidential information, and how to safely use devices and networks (Accinelli, 2024).

2.Implementation of Technical Security Measures: In addition to awareness, it is crucial to implement technical security measures to protect systems, networks, and data from cyber threats. This includes installing and regularly updating antivirus and antispyware software, configuring firewalls to control network traffic, implementing multi-factor authentication to access sensitive systems and data, and encrypting data both at rest and in transit to protect the confidentiality of information (Reuters, 2019).

3.Threat Monitoring and Detection: Another important cybersecurity strategy is the implementation of monitoring and threat detection systems. This involves the use of network and system security tools that can identify suspicious activities or anomalies in data traffic and alert security administrators to quickly respond to potential incidents. Continuous monitoring and proactive response are fundamental to minimizing the impact of security breaches and data violations.

4.Vulnerability and Patch Management: Vulnerability management is an integral part of any effective cybersecurity strategy. This involves actively identifying and remediating vulnerabilities in systems and applications by timely implementing security patches and software updates. Organizations should establish clear processes and policies for risk assessment and management, as well as for systematically applying security patches (Reuters, 2019).

5.Incident Response Planning: Last but not least, organizations must develop and implement incident response plans to effectively manage security breaches and cyberattacks. This includes designating an incident response team, defining roles and responsibilities, creating communication and coordination protocols, and conducting regular drills to test the effectiveness of the plan and ensure a quick and coordinated response in an emergency (Reuters, 2019).

Cybersecurity is a continuous and ever-evolving challenge in today's digital era. Adopting effective cybersecurity strategies and measures is essential to protect our digital assets, preserve the confidentiality and integrity of our data, and ensure the continuity of our operations in an increasingly connected world. Through awareness, education, implementation of technical security measures, threat monitoring and detection, vulnerability management, and incident response planning, we can strengthen our cyber defenses and face digital security challenges with confidence and resilience.

PhD Juan Raúl Gutiérrez Zaragoza

Life Member of the FBI National Academy, graduated from that Academy in Session 184, President of the Latin America and Caribbean Chapter of the FBINAA, 2021-2023.

He is the only associate in Latin America and the Caribbean of the FBI National Academy who has completed the full cycle of three courses in person to obtain the only leadership certificate awarded by the FBINAA, consisting of the following program: "Meeting the Leadership Challenges of Law Enforcement 'First Line Supervision'," "Mastering the Leadership Challenges of Law Enforcement," and the "Officer Resiliency, Safety, & Wellness Leadership Forum."

He is a professor in Public Security, Citizen Security, Human Security, Administrative Law, Criminal Law in both the traditional system and the accusatory criminal system, Philosophy of Law, Political Science, Theory of the State, Constitutional Law, and Public Administration. He is the author of several academic articles, among which are: "Ethics and Integrity in Public Service," published in the journal Tiempo de Derechos (December 2020), and "Towards a Comprehensive Criminal Policy in Mexico: Challeng...

Due to his experience in justice institutions, he planned, executed, and coordinated the transition of the defunct Specialized Unit for Organized Crime Investigation to the level of Subprocuraduría (Assistant Attorney General's Office) at the Office of the Attorney General of the Republic, now the Office of the Prosecutor General of the Republic (FGR). This led to the formation of what is now known as SEIDO, where all the units that make up the Specialized Assistant Attorney General's Office for Organize...

He coordinated the implementation of the New Criminal Justice System in the State of Jalisco, collaborating with the Security and Justice Commission of the Jalisco State Congress to harmonize thirteen State Laws. He also participated in the structural reform of the Organic Law of the Executive Branch of the State of Jalisco, among other academic and research contributions, as well as many other endeavors.

He has vast experience in Public Administration at the federal, state, and municipal levels. In 2024, he will complete forty years of service to the Government of Mexico in one of its three branches.

EVOLUCIÓN DE LA VIDEO VIGILANCIA Y SUS TENDENCIAS ACTUALES

En la actualidad damos por sentada, la videovigilancia, "locales, calles e incluso hogares están equipados con esta tecnología y es algo que hemos llegado a aceptar y esperar" (Historia de la Vigilancia), sin embargo, no debemos olvidar que la videovigilancia, es la lógica evolución de la vigilancia u observancia, tradicional.

Cuando hablamos de un sistema de videovigilancia, nos referimos a un conjunto de aparatos instalados en cascada, para proporcionar "servicios de seguridad y supervisión" (...) "Cada componente desempeña un papel fundamental a la hora de garantizar que un sistema de videovigilancia funcione de forma eficaz y segura" (Senstar).

Hace aproximadamente 200,000 años, los primeros homos sapiens, recorrían las llanuras africanas en su travesía épica para expandirse a través de los continentes, (National Geografic) hasta la actualidad donde la inteligencia artificial, está cambiando la forma y velocidad en que los seres humanos trabajamos y en general vivimos, desvaneciendo nuestros humildes y precarios orígenes. Las actividades de vigilancia son y serán esenciales para mantener la vida y bienestar de las sociedades; caza, pesca, producción de bienes, prestación de servicios, seguridad y la guerra, ayer como hoy son simplemente impensables e inviables sin vigilancia.

La videovigilancia y su actividad antecesora la vigilancia propiamente dicha, como toda actividad humana, se realizaba únicamente en las capacidad humanas propias y las limitaciones cognitivas y físicas. Fatiga, distracción, malas interpretaciones, prejuicios e intereses personales, la limitada memoria, la baja fiabilidad en la reproducción de lo captado y las fortalezas como la propia inteligencia humana, virtud, responsabilidad, compromiso y su capacidad poder evaluar información, crear conclusiones y recomendaciones, fueron denominadores comunes.

Adicionándole otras limitaciones que condicionaban la continuidad de la actividad, condiciones ambientales adversas y la incapacidad de transmitir los productos de la vigilancia a distancia rápida y fielmente.

Desde esas tempranas épocas se identificó la necesidad de superar estas limitaciones y potenciar las fortalezas, desde un enfoque tecnológico y organizativo, mediante la progresiva introducción de artilugios y procesos sistémicos, mejorando el procesamiento de la información.

Algunos de los más sobresalientes e ingeniosos, son telescopios, rudimentarios sistemas de encriptamiento, primitivos sistemas de señales, transmisión de información y datos (como el uso de animales, perros y aves entrenadas), la transmisión eléctrica de mensajes (telégrafo, teléfono) y la aparición de sistemas tratamiento y fijación de imágenes (Daguerrotipia, fotografía y el video análogo) y sonido (discos, cintas magnéticas) y por último el análisis de información, y sus metodologías. Todo para poder dar seguimiento al desarrollo de un fenómeno o situación en concreto en un tiempo determinado, realizando un "monitoreo en vivo", es decir ver las cosas en el sitio y momento en que se están sucediendo para así tomar acciones, para tratar de minimizarlo, potenciarlo u orientarlo.

Los anterior nos pueden dar un bosquejo del largo camino recorrido hasta nuestros días. Pero ¿Dónde comienza la videovigilancia como la conocemos? Metodológicamente es cuando la tecnología tiene suficiente madurez, para integrar los elementos aislados, como la captación de imágenes en video mediante el uso de cámaras, el almacenamiento, la administración y manejo de imágenes y la transmisión de estas un centro de análisis y operaciones. Con lo que considero que la superación del "monitoreo en vivo", es el punto de inflexión, que marca el inicio de la moderna Videovigilancia.

El antecedente documentado más antiguo se sitúa “en 1927, cuando el Ingeniero Alemán de nombre Walter Bruch creo el primer sistema de CCTV, que se conoció como “ojos televisivos” (Television-Eyes). Este sistema utilizaba la última tecnología del momento pantallas de Rayos Catódicos (CRTs) y cámaras filmadoras de formato de 8 mm para capturar imágenes, aunque significaba un enorme avances estaba limitado a las tecnologías disponibles en ese momento. (traducción libre de The birth of Surviellance), siendo su primer uso en gran escala en las investigaciones asociadas al desarrollo del Bombas V2 en Alemania durante la Segunda Guerra Mundial. Y su primero uso comercial documentado se le atribuye la empresa Vericon en los Estados Unidos. (la historia de la Videovigilancia)

Según la consultora en Seguridad SENSTAR, con sede en Ontario, Canadá, un moderno sistema de video vigilancia, deberá contar con lo siguiente:
Cámaras: Son el componente principal de cualquier sistema de videovigilancia, con diferentes capacidades y especificaciones técnicas. **Dispositivos de grabación:** Son los dispositivos para almacenar imágenes durante un periodo determinado, su capacidad depende de su memoria interna y la calidad de las imágenes grabadas. **Monitores de visualización:** Los monitores permiten ver en tiempo real las imágenes captadas por las cámaras. **Equipos de red:** Son los Dispositivos IP, routers, conmutadores y cableado **Software:** Proporciona la interfaz para interactuar con el sistema de vigilancia. configurar las cámaras, ajustes de grabación y la visualización de imágenes en directo y grabadas. Los más avanzados ofrecen capacidades de análisis e inteligencia artificial para identificar y alertar sobre eventos o anomalías específicos. **Accesorios:** Aparatos tales como soportes, carcasas y fuentes de alimentación, esenciales para instalar y utilizar un sistema de vigilancia. **Servicios en la nube:** Algunos sistemas de vigilancia se integran con servicios en la nube para el almacenamiento de datos y la supervisión remota. **Medidas de ciberseguridad:** Protegen el sistema de accesos no autorizados y amenazas cibernéticas.

La construcción de un efectivo sistema de Videovigilancia requiere una cuidadosa planificación e identificar las necesidades de seguridad específicas de una instalación, al tiempo que se cumplen las directrices legales y éticas.

De lo anterior y el entorno actual, permite identificar las más notables tendencias en el desarrollo de esta industria, la sustitución total de los sistemas analógicos, las soluciones de video impulsadas por inteligencia artificial (reconocimiento facial y de lenguaje corporal, conteos, métricas y patrones), servicios de almacenamiento en la nube, la utilización de dispositivos multifunción y multitarea y la democratización del servicio al ser las tecnología de mas bajo costo y fácil interface. Todo lo cual nos hace pensar que la videovigilancia esta más vigente que nunca y tiene un espacio en todos los campos de la seguridad.

EVOLUTION OF VIDEO SURVEILLANCE AND ITS CURRENT TRENDS

Nowadays we take video surveillance for granted, “premises, streets and even homes are equipped with this technology and it is something we have come to accept and expect” (History of Surveillance), however, we must not forget that video surveillance is the logical evolution of traditional surveillance or enforcement.

When we talk about a video surveillance system, we refer to a set of devices installed in cascade, to provide “security and monitoring services” (...) “Each component plays a fundamental role in ensuring that a video surveillance system works effectively and safely” (Senstar).

Approximately 200,000 years ago, the first homo sapiens roamed the African plains on their epic journey to expand across the continents (National Geographic) until today, where artificial intelligence is changing the way and speed at which human beings work and generally live, obliterating our humble and precarious origins. Surveillance activities are and will be essential to maintain the life and well-being of societies; hunting, fishing, production of goods, provision of services, security and war, yesterday as today are simply unthinkable and unviable without surveillance.

Video surveillance and its predecessor, surveillance itself, like all human activity, was carried out solely within human capacities and cognitive and physical limitations. Fatigue, distraction, misinterpretations, prejudices and personal interests, limited memory, low reliability in the reproduction of what was captured and strengths such as human intelligence itself, virtue, responsibility, commitment and its ability to evaluate information, create conclusions and recommendations, were common denominators.

Adding to this were other limitations that conditioned the continuity of the activity, adverse environmental conditions and the inability to transmit the products of remote surveillance quickly and faithfully.

From those early times, the need to overcome these limitations and enhance the strengths was identified, from a technological and organizational approach, through the progressive introduction of gadgets and systemic processes, improving the processing of information.

Some of the most outstanding and ingenious are telescopes, rudimentary encryption systems, primitive signal systems, transmission of information and data (such as the use of trained animals, dogs and birds), the electrical transmission of messages (telegraph, telephone) and the appearance of systems for processing and fixing images (Daguerreotype, photography and analog video) and sound (disks, magnetic tapes) and finally the analysis of information, and its methodologies. All this in order to be able to monitor the development of a specific phenomenon or situation at a given time, carrying out “live monitoring”, that is, seeing things in the place and at the time they are happening in order to take action to try to minimize, enhance or guide them.

The above can give us an outline of the long road traveled to this day. But where does video surveillance as we know it begin? Methodologically, it is when the technology is mature enough to integrate isolated elements, such as the capture of video images using cameras, storage, management and handling of images and their transmission to an analysis and operations center. Therefore, I consider that the overcoming of “live monitoring” is the turning point, which marks the beginning of modern video surveillance.

The oldest documented antecedent is located "in 1927, when the German engineer named Walter Bruch created the first CCTV system, which was known as "television eyes" (Television-Eyes). This system used the latest technology of the time: Cathode Ray Screens (CRTs) and 8 mm format film cameras to capture images, although it meant enormous progress, it was limited to the technologies available at that time. (free translation of The birth of Surveillance), its first large-scale use being in the research associated with the development of the V2 Bomb in Germany during World War II. And its first documented commercial use is attributed to the company Vericon in the United States. (the history of Video Surveillance)

According to the security consultancy SENSTAR, based in Ontario, Canada, a modern video surveillance system must have the following:

Cameras: They are the main component of any video surveillance system, with different capacities and technical specifications. Recording devices: They are the devices to store images for a certain period, their capacity depends on their internal memory and the quality of the recorded images. Display monitors: The monitors allow you to see the images captured by the cameras in real time. Network equipment: These are IP devices, routers, switches and cabling Software: Provides the interface to interact with the surveillance system, configure the cameras, recording settings and the display of live and recorded images. The most advanced ones offer analysis and artificial intelligence capabilities to identify and alert on specific events or anomalies. Accessories: Devices such as supports, housings and power supplies, essential to install and use a surveillance system. Cloud services: Some surveillance systems integrate with cloud services for data storage and remote monitoring. Cybersecurity measures: Protect the system from unauthorized access and cyber threats.

Building an effective video surveillance system requires careful planning and identifying the specific security needs of a facility, while complying with legal and ethical guidelines.

From the above and the current environment, it is possible to identify the most notable trends in the development of this industry, the total replacement of analog systems, video solutions driven by artificial intelligence (facial and body language recognition, counts, metrics and patterns), cloud storage services, the use of multifunction and multitasking devices and the democratization of the service as the technology is the lowest cost and easiest to interface. All of which makes us think that video surveillance is more relevant than ever and has a place in all fields of security.

FELIX ALEJANDRO MALDONADO JIMENEZ

Retired Commissioner General of the National Police of Honduras.

Graduated from the National Police Academy General Jose Trinidad Cabañas in 1993, as a Police Officer in the rank of Second Lieutenant of Police, Graduated in Police Sciences from the National Police University of Honduras, Lawyer Graduated from the Autonomous University of Honduras and with studies in Electrical Engineering. In addition to courses at the Interministerial Anti-Drug Center of France (CIFAD), Criminal Investigation University of Korea and Graduate of Session 234 of the National Academy of the FBI.

During my professional career of almost 30 years, I have held a wide variety of positions and responsibilities, such as Anti-Drug Investigator, Information Analyst, Municipal Police Chief, Head of the Anti-Kidnapping Group, Rector and Professor at the National Police University of Honduras, Liaison Officer to the National Congress, Departmental Chief, Chief of the Ministerial Cabinet, Administrative Director and Head of External Cooperation and International Relations. I am currently working in the private sector of Honduras.

References

- La historia de la vídeovigilancia - desde 1942 hasta la actualidad - PCR | Digital Travel (digitltravel.com)
- Tendencias en videovigilancia para 2024 (atlas.com.co)
- Componentes de los sistemas de videovigilancia - Senstar: protegiendo a personas, lugares y bienes
- ¿Cuál es el origen de la humanidad según la ciencia? | National Geographic (nationalgeographicla.com)
- The Birth Of Surveillance: When Were Security Cameras Invented? - TechSynchron

TERRORISMO INTERNACIONAL. SU IMPLICANCIA EN LA CIUDAD DE BUENOS AIRES

El Terrorismo, como fenómeno en el cual se destaca la violencia extrema, ha sufrido mutaciones a lo largo del tiempo, siendo característico por sus distintos métodos de ejercer el terror, ya sea a través de ataques contra la vida, como así también la amenaza de cometerlos. Si bien estas acciones que sólo representan un grupo de tipos de ataques, han variado en su forma, lo que ha sufrido mayor modificación es la geografía y el espacio del fenómeno, que de ser anteriormente circunscripto a un país o una zona fronteriza, pasó a ser internacional, o como a veces se lo conoce: "global", término atribuido al filósofo y sociólogo de la comunicación canadiense, Marshal McLuhan (1911-1980).

Esto significó un enorme desafío para las autoridades de cada país, ya que un delito localizado pasaba a desarrollarse con las cualidades de las Organizaciones Criminales Transnacionales, generando una necesidad imperiosa de coordinación entre los distintos países parte y sus fuerzas encargadas de hacer cumplir la ley, lo que hasta la actualidad no ha alcanzado el nivel necesario para derrotar a las Organizaciones Terroristas y sus cómplices, vinculados a los denominados Delitos Conexos.

En el marco teórico argentino, hay ausencia de definiciones. Por tal motivo, los integrantes de las distintas instituciones dedicados a investigar y combatir el Terrorismo, se ven en la obligación de realizar extractos y conclusiones de diferentes escritos legales y manuales, a fin de encontrar términos que permitan delimitar y comprender el delito para luego abordarlo.

Con respecto al marco legal de la República Argentina, hay escasez de lineamientos precisos sobre procedimientos, y sólo se cuenta con el artículo 41 quinquies del Código Penal Argentino, que establece:

"Cuando alguno de los delitos previstos en este Código, en leyes especiales o en las leyes que incorporen al derecho interno tipos penales previstos en convenciones internacionales vigentes ratificadas en la República Argentina, hubiere sido cometido con la finalidad de aterrorizar a la población u obligar a las autoridades públicas nacionales o gobiernos extranjeros o agentes de una organización internacional a realizar un acto o abstenerse de hacerlo, la escala se incrementará en el doble del mínimo y el máximo".

Para una mejor comprensión del contexto del Terrorismo a nivel mundial y la correspondiente ubicación de la República Argentina, a continuación se incorpora una imagen extraída del Índice Global del Terrorismo 2024 (Global Terrorism Index 2024), publicada por el Instituto de Economía y Paz (Institute for Economics & Peace), donde se aprecia la métrica del impacto del terrorismo, posicionando a la Argentina en un nivel "Muy Bajo".

El 17 de Marzo de 1992, se perpetró en la Ciudad de Buenos Aires el atentado suicida contra la Embajada de Israel, donde fallecieron 22 personas y otras 242 quedaron heridas. Fue un atentado contra la comunidad judía, que afectó a toda la sociedad sin distinguir religiones ni nacionalidades. Dos años después, el 18 de Julio de 1994, se llevaba adelante el atentado suicida contra la Asociación Mutual Israelita Argentina (AMIA), provocando la muerte de 85 personas y 300 heridos. También se trató de un atentado contra la comunidad judía, que una vez más recayó sobre toda la ciudadanía, sin distinciones. En ambos casos, la investigación judicial y policial se encontró con una realidad que no permitió un avance certero que lograra la identificación de los autores ideológicos y su correspondiente detención para su posterior enjuiciamiento.

Luego de 30 y 32 años de sucedido cada atentado respectivamente, este año 2024 se obtuvo la desclasificación del denominado "Informe Toma", en referencia al ex titular de la Secretaría de Inteligencia del Estado (SIDE), Miguel Ángel Toma, quien en el año 2003 entrega al Juez Galeano el reporte con la información suficiente para comprender el entretejido del atentado a la AMIA y sus autores.

Este informe, en coincidencia con agencias de Inteligencia extranjeras como la CIA (Estados Unidos) y el Mossad (Israel), establece que las autoridades máximas de la República de Irán y de la Organización Terrorista Hezbollah, dieron la orden para que se concretara el ataque. Confirma que el atentado fue dirigido y ejecutado en el terreno por Hezbollah, con preparación desde la Triple Frontera (Brasil, Paraguay y Argentina) desde el año 1988. Ratifica que menos el suicida, todos los partícipes se fueron del país días y hasta horas antes de la explosión. También aclara que no hubo argentinos involucrados, y que aquellos que tuvieron participación fue en forma indirecta y desconociendo el objetivo. En otro orden de cosas, el informe certifica que los autores fueron reclutados y entrenados en el Líbano, en los cuarteles "Yihad Islámica", y que algunos de ellos lograron ascensos dentro del régimen iraní y de la Unidad de Atentados. Finalmente, enfatiza en que la Inteligencia iraní en Buenos Aires, ubicada en su propia Embajada, supo de los preparativos finales y de la materialización del atentado a la AMIA, unos días antes.

Cabe hacer una pequeña introducción de las áreas policiales destinadas a la Investigación del Terrorismo, y en esta circunstancia, focalizando en la Ciudad de Buenos Aires y su División Antiterrorismo. Como bien se dijo en un principio, el fenómeno del Terrorismo se manifiesta a nivel global, por lo que acertadamente, cada Fuerza Federal de Seguridad y Policía Provincial de un Estado de gran desarrollo, posee su Unidad Antiterrorista, de modo de llevar a cabo las tareas de reunión y análisis de información, como así también las inherentes a investigación, todo en procura de una oportuna prevención.

A partir de contarse con diversas estructuras dedicadas a la misma especialidad, desde el año en curso la Dirección Nacional de Inteligencia Criminal ha tomado la iniciativa de crear el Centro de Misión Antiterrorista (CMA), del cual participan miembros de cada Institución vinculados a la temática, asistiendo de manera diaria y presencial para desarrollar sus labores, trabajando en conjunto cada tema considerado relevante. Luego, al confeccionarse un documento producido, el mismo se distribuye a cada organización parte, manteniendo un fluido y actualizado intercambio de información para la correcta toma de decisiones.

Profundizando las funciones específicas de la División Antiterrorismo de la Ciudad de Buenos Aires (Prevención, Detección, Investigación), las tareas inherentes a la Prevención, son aquellas que procuran que los hechos no sucedan, y para tal fin es fundamental el generar conciencia sobre las acciones violentas y sus consecuencias. Abarcando el concepto de Detección, se hace referencia a la importancia de buscar y reunir información en todos los medios existentes, sean físicos (terreno) o tecnológicos (internet), con la firme idea de observar personas, grupos de personas, expresiones, manifiestos, maniobras, etc., que por el contenido puedan ser considerados elementos de suficiente sospecha para solicitar al Juzgado de turno la intervención investigativa. Con respecto al término Investigación, se inicia cuando se toma conocimiento de un hecho consumado o sus actos preparatorios, implementando las labores típicas del investigador policial.

INTERNATIONAL TERRORISM. ITS IMPLICATION IN THE CITY OF BUENOS AIRES

Terrorism, as a phenomenon in which extreme violence stands out, has undergone mutations over time, being characterized by its different methods of exercising terror, either through attacks against life, as well as the threat of committing them. Although these actions, which only represent a group of types of attacks, have varied in their form, what has undergone greater modification is the geography and space of the phenomenon, which from being previously limited to a country or a border area, became international, or as it is sometimes known: "global", a term attributed to the Canadian philosopher and sociologist of communication, Marshal McLuhan (1911-1980).

This meant an enormous challenge for the authorities of each country, since a localized crime began to develop with the qualities of Transnational Criminal Organizations, generating an urgent need for coordination between the different participating countries and their forces in charge of enforcing the law, which to date has not reached the level necessary to defeat the Terrorist Organizations and their accomplices, linked to the so-called Related Crimes.

In the Argentine theoretical framework, there is a lack of definitions. For this reason, the members of the different institutions dedicated to investigating and combating Terrorism, are forced to make extracts and conclusions from different legal documents and manuals, in order to find terms that allow them to delimit and understand the crime and then address it. Regarding the legal framework of the Argentine Republic, there is a lack of precise guidelines on procedures, and there is only article 41 quinquies of the Argentine Penal Code, which states:

"When any of the crimes provided for in this Code, in special laws or in the laws that incorporate into domestic law criminal types provided for in international conventions in force ratified in the Argentine Republic, has been committed with the purpose of terrorizing the population or forcing national public authorities or foreign governments or agents of an international organization to carry out an act or refrain from doing so, the scale will be increased by twice the minimum and the maximum.

For a better understanding of the context of Terrorism worldwide and the corresponding location of the Argentine Republic, below is an image taken from the Global Terrorism Index 2024, published by the Institute for Economics & Peace, where the metric of the impact of terrorism can be seen, positioning Argentina at a "Very Low" level.

On March 17, 1992, a suicide attack against the Israeli Embassy was perpetrated in the City of Buenos Aires, where 22 people died and another 242 were injured. It was an attack against the Jewish community, which affected the entire society without distinguishing between religions or nationalities. Two years later, on July 18, 1994, a suicide attack was carried out against the Argentine Israelite Mutual Association (AMIA), causing the death of 85 people and 300 injured. This was also an attack against the Jewish community, which once again fell on all citizens, without distinction. In both cases, the judicial and police investigations were faced with a reality that did not allow for any certain progress that would lead to the identification of the ideological authors and their corresponding arrest for subsequent prosecution.

After 30 and 32 years of each attack, respectively, this year 2024 the declassification of the so-called "Toma Report" was obtained, in reference to the former head of the State Intelligence Secretariat (SIDE), Miguel Ángel Toma, who in 2003 gave Judge Galeano the report with sufficient information to understand the intricacies of the AMIA attack and its authors.

This report, in agreement with foreign intelligence agencies such as the CIA (United States) and the Mossad (Israel), establishes that the highest authorities of the Republic of Iran and the Terrorist Organization Hezbollah gave the order for the attack to be carried out. It confirms that the attack was directed and executed on the ground by Hezbollah, with preparation from the Triple Frontier (Brazil, Paraguay and Argentina) since 1988. It confirms that except for the suicide bomber, all the participants left the country days and even hours before the explosion. It also clarifies that there were no Argentines involved, and that those who did participate did so indirectly and without knowing the objective. In another order of things, the report certifies that the authors were recruited and trained in Lebanon, in the "Islamic Jihad" barracks, and that some of them achieved promotions within the Iranian regime and the Attack Unit. Finally, it emphasizes that Iranian Intelligence in Buenos Aires, located in its own Embassy, knew of the final preparations and the materialization of the attack on the AMIA, a few days before.

A brief introduction of the police areas assigned to the Investigation of Terrorism is worth making, and in this circumstance, focusing on the City of Buenos Aires and its Anti-Terrorism Division. As was said at the beginning, the phenomenon of Terrorism is manifested at a global level, so each Federal Security Force and Provincial Police of a highly developed State, rightly has its Anti-Terrorist Unit, in order to carry out the tasks of gathering and analyzing information, as well as those inherent to investigation, all in pursuit of timely prevention.

Since having various structures dedicated to the same specialty, since this year the National Directorate of Criminal Intelligence has taken the initiative to create the Anti-Terrorist Mission Center (CMA), in which members of each Institution linked to the subject participate, attending daily and in person to develop their work, working together on each topic considered relevant. Then, when a document is produced, it is distributed to each participating organization, maintaining a fluid and updated exchange of information for correct decision-making.

Going deeper into the specific functions of the Anti-Terrorism Division of the City of Buenos Aires (Prevention, Detection, Investigation), the tasks inherent to Prevention are those that ensure that events do not occur, and to this end it is essential to raise awareness about violent actions and their consequences. Covering the concept of Detection, reference is made to the importance of seeking and gathering information in all existing media, whether physical (field) or technological (internet), with the firm idea of observing people, groups of people, expressions, manifestos, maneuvers, etc., that due to their content can be considered elements of sufficient suspicion to request investigative intervention from the Court on duty. Regarding the term Investigation, it begins when knowledge is gained of a completed event or its preparatory acts, implementing the typical tasks of the police investigator.

COMISARIO AUGUSTO CASTRO SARUBBI

Jefe de la división antiterrorismo
Policía de la ciudad de Buenos Aires
FBINAA Sesión 243
E-Mail: augustocastro@buenosaires.gob.ar

COLABORADORES DE ESTE NÚMERO

ARIEL RODRÍGUEZ MORENO
Designer and Editor

ANNY A. CUELLO
Consultancy

JULIO G. BERNAL CAVERO
Consultancy

MTRO. ALEJANDRO LARES V
Design Adviser

Autores:
ADRIAN VEGA
SOFÍA ARAYA BUSTAMANTE
BENJAMÍN LUNA-ALATORRE
DWAYNE S. CUMBERBATCH
JUAN RAÚL GUTIÉRREZ ZARAGOZA
FELIX ALEJANDRO MALDONADO JIMENEZ
AUGUSTO CASTRO SARUBBI

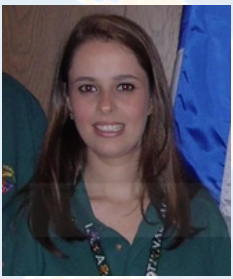
BOARD MEMBERS

ANNY A. CUELLO
President

ARIEL RODRÍGUEZ MORENO
Communications & Image

JULIO G. BERNAL CAVERO
Adviser

SHIRLEY TAPIA CONDORI
Continued Studies



FERNANDA HERBELLA MAIA
South America Coordinator

VICTOR JARA URRUTIA
Secretary/Treasurer

WENDELL HERNÁNDEZ LUCAS
Caribbean Region Representative

PAULA MORA MALTÉS
Youth Leadership Program