PROSEGUR RESEARCH

Innovación tecnológica criminal

PROSEGUR

Índice

Este documento es interactivo

01 La innovación criminal

¿Qué es la innovación criminal?

La creatividad y la imaginación son inherentes al ser humano, si bien sus aplicaciones sobre propósitos delictivos no han sido tradicionalmente estudiadas en el mundo de la criminología y la seguridad. De hecho, el informe de la Comisión de Investigación de los atentados del 11S determinó que la falta de imaginación, en parte impidió prevenir el ataque terrorista, cuya materialización podríamos definir sin lugar a dudas como radicalmente diferente, disruptiva e innovadora.

Parece importante, por tanto, conocer cómo innovan los criminales y explorar las fórmulas empleadas hasta la fecha. Pues bien, la innovación se define como "la adopción de nuevos patrones de comportamiento"[1]; por tanto, la innovación criminal sería aplicable cuando este comportamiento es delictivo[2]. Inspirados en Lubrano[3] (2021) podemos definir innovación criminal como **un proceso en el cual se reformulan componentes sustanciales de códigos y normas preexistentes, escritas o no, que caracterizan el modus operandi de organizaciones o individuos con fines o medios ilegales.**

Esto implica la consideración de la innovación como un proceso y como un producto. Pero creatividad no equivale a innovación: mientras que la creatividad se asocia a la generación de nuevas ideas o conceptos, la innovación implica la implementación de dichas ideas.

Atendiendo a las fórmulas de cambio, podemos identificar distintos tipos de innovación

La innovación incremental se sustentaría en la necesidad de superar obstáculos a la hora de cometer delitos, como la superación de las medidas de seguridad, o en la introducción de nuevos desarrollos que perfeccionan o mejoran el modelo original; por ejemplo, drones por parte de organizaciones criminales para distintos usos: comienzan empleándose como medio de vigilancia a las autoridades y posteriormente incluyen explosivos para ahuyentar a la policía.

La innovación radical supone un cambio fundamental, saliéndose de procesos y productos previos, como los ataques terroristas del 11S. Tiene una duración corta, al ser inmediatamente imitada, siendo de esta forma incentivo para la innovación incremental. La innovación radical es, por ello, un motor de la innovación incremental, que permite incorporar todas esas zonas grises existentes en la conceptualización de innovación, especialmente cuando hablamos de imitación, emulación o adaptación.

En su libro, *The innovator's dilemma* (El dilema del innovador), Christensen (1997) introduce el concepto de **innovación disruptiva:** aquella en que se suministran bienes y servicios que son menos costosos y más accesibles, y eventualmente reemplazan formatos previos. Supone un cambio total frente a la situación previa en productos, o mercados o sectores, como por ejemplo el uso de Inteligencia Artificial para la imitación de voz de directivos en extorsiones a empresas o el uso de impresoras 3D para generar llaves con rapidez.

---

[1] Tomado de **Crenshaw** (2010).
[2]Un concepto interesante es de la "creatividad malévola" **(malevolent creativity)** o el **"lado oscuro de la creatividad"**, como el esfuerzo creativo para lograr unos objetivos dañando a otros individuos o grupos.
[3]Aunque su **estudio** está más centrado en innovación en ataques terroristas, el marco proponemos es aplicable a cualquier actor criminal.

¿Qué es la innovación criminal?

Otra clasificación interesante es la de **Crenshaw (2010),** que diferencia entre innovación táctica, operacional y estratégica atendiendo al alcance del cambio implementado.

- Considera que la **innovación táctica** es la que se centra en adoptar nuevas tecnologías para abordar los objetivos tradicionales, mientras que tendría carácter estratégico cuando la finalidad es abordar nuevos objetivos. Por tanto, sería definida como cambios sustanciales en la ejecución de los delitos que redefinen patrones de comportamiento de una organización o individuo. Se centra en las armas y tecnologías utilizadas, objetivos, tiempo y localización de la acción y selección de los delitos y objetivos.

- La **innovación operacional,** llamada organizacional por Crenshaw, se refiere a cambios en las estructuras e instituciones de una organización. Se centra en actividades necesarias para mantener la operativa: estructura organizacional, reclutamiento, financiación, comunicación, etc. Innovaciones operacionales pueden ser el uso de criptomonedas, le encriptación, el recurso a aplicaciones móviles de comunicación o a la DarkWeb.

- Finalmente, es **innovación estratégica** aquella que afecta patrones fundamentales de los retos criminales hacia las autoridades políticas, lo que implica o bien nuevos objetivos o bien una nueva forma de desarrollar sus operaciones hacia ese objetivo.

No solo innovan las empresas

A menudo ponemos de relieve las mejores prácticas en términos de innovación implementadas por empresas y organismos públicos; lo cierto es que **los criminales también innovan**, y posiblemente lo hagan mejor.

Esto tiene su explicación: es más fácil diseñar e implementar novedades en un equipo al margen de la ley, que incumple sistemáticamente todo tipo de normas y que asume riesgos por encima de sus capacidades. Además de esta **flexibilidad**, quien está al otro lado de la ley tiene más **tiempo** para preparar sus iniciativas ilegales y en ocasiones, más **recursos** si se trata de un negocio ilegal altamente rentable.

En este contexto, innovar sin criterio legal ni ético permite a los criminales explotar **vulnerabilidades**[4] y diseñar **engaños** para confundir tanto a **humanos** a través de ingeniería social mediante ***phishing*** y tecnologías DeepFake[5] como a las propias **herramientas,** actuando de forma sigilosa mediante simulación de comportamientos humanos para evitar UEBA[6].

Pero la innovación criminal no es algo exclusivamente de la época actual, buen ejemplo de ello fue el **uso anticipado** del subfusil Thompson[7] por parte de la mafia antes que la policía estadounidense en la época de la Ley seca[8].

La innovación criminal es una constante

Incluso los momentos críticos para las sociedades no suponen un impedimento para los grupos criminales, que saber aprovechar las oportunidades para actualizar sus operativas, directrices y métodos de actuación. La COVID-19 es un buen ejemplo de ello: las restricciones de movilidad y en servicios de propiciaron la búsqueda de nuevas vías por parte de las organizaciones criminales para dar continuidad a sus activiades ilícitas. El uso de narcosubmarinos para transportar droga desde el continente americano hasta Europa es solo una muestra de ello[9], como veremos más adelante.

---

[4] Como ocurrió en diciembre de 2021 con log4j, una vulnerabilidad de día cero de alta gravedad.
[5] Que generan contenidos audiovisuales falsos gracias a la Inteligencia Artificial, hasta ahora prácticamente imposibles de diferenciar de los contenidos reales.
[6] UEBA, por sus siglas en inglés, User and Entity Behaviour Analytics, son herramientas de análisis del comportamiento del usuario; también se denomina Insider Risk Management.
[7] Un arma automática más cómoda, veloz y precisa a corta y media distancia que las demás armas del mercado a principios del siglo XX, bautizada como la Máquina de escribir de Chicago por su capacidad aproximada de 1000 disparos por minuto.
[8] En el ámbito armamentístico, el uso de material innovador por parte de organizaciones criminales antes que de ejércitos y policías está muy extendido, dado el proceso que deben respetar para que sus gobiernos aprueben nuevas armas; como hemos comentado previamente, no respetar las normas facilita este tipo de anticipaciones.
[9] Si bien estos aparatos existen desde la década de los 90, su utilización se ha visto incrementada en los últimos meses, llegando a interceptarse entre 30 y 40 cada año tan solo en Colombia.

02 Innovar desde el lado oscuro

¿Cómo se innova desde el lado oscuro?

Identificamos cuatro dimensiones desde las que podemos analizar las principales innovaciones criminales conocidas en la actualidad.

Aprovechando los avances tecnológicos

Si bien el progreso tecnológico ha conllevado avances importantes en la civilización, lo cierto es que también ha supuesto un sensible aumento de la superficie de ataques para los delincuentes[10].

La clave de su rentabilidad radica en poner el desarrollo tecnológico y su uso extendido al servicio de los criminales. Así, podemos afirmar que los cibercriminales están en constante innovación ***(Europol, 2021).***

Por ejemplo, desde los primeros ATM o cajeros automáticos de finales de los 60, se han incorporado exponencialmente a nuestro día a día, transformándose en uno de los principales focos de ataque a entidades financieras tanto mediante **fraudes** (suplantación del usuario) frecuentemente mediante skimming (clonado de tarjetas), **ataques lógicos** como el jackpotting[11] a través de malware[12], como **ataques físicos**, por ejemplo, colocando falsas bocas en el dispensador de efectivo. Estos ataques continúan incrementándose año tras año especialmente los troyanos en móviles, innovando por ejemplo con el uso de impresoras 3D para replicar llaves con rapidez al menos desde hace más de diez años, o el robo de tokens para eludir MFA (Múltiples Factores de Autenticación).

[10] Especialmente las tecnologías horizontales, más ampliamente difundidas en términos de curva de difusión. Esto ha ocurrido en gran parte gracias al IoT (Internet de las Cosas), la digitalización de empresas y el uso extendido de internet, que supone una importante oportunidad de enriquecimiento ilícito a través de todo tipo de ciberataques.
[11] Esta técnica permite lograr hasta 40 billetes cada 23 segundos.
[12] Especialmente troyanos en móviles (Europol, 2021).

Sin duda, el **Crime-as-a-Service**[13] como entorno de intercambio de servicios cibercriminales ha generado un auténtico ecosistema de innovación altamente rentable: del Malware-as-a-Service[14] ahora muy centrado en dispositivos móviles al Ransomware-as-a-Service[15] orientado a reducir el time-to-ransom para espionaje industrial y el robo de datos son muestra de ello[16]. Dentro de este **ecosistema de actividades criminales,** una forma que se ha descubierto rentable para estos grupos es la 'subcontratación' de servicios a otras organizaciones para llevar a cabo diferentes actividades, como la producción de cocaína en laboratorios latinoamericanos, con el objetivo de ser más ágiles y eficientes, así como poder ahorrarse tareas de producción y logística y aislar a los nodos centrales de las bandas organizadas.

Además, saben aprovechar la criptografía como fórmula de autoprotección[17], anonimizando su identidad cuando cometen ilegalidades en internet, por ejemplo, mediante la navegación en la **deepweb y la darkweb** o el lucrativo abuso de la privacidad ofrecida por los **criptoactivos** para blanqueo de capitales, estafas y cobros de extorsiones. En este sentido, el empleo **de drones para monitorización** de policías o vigilantes es conocido, como hicieron los miembros de la MS13 en Honduras en 2020, o **drones con explosivos** para ahuyentar a la policía como hizo el CCJNG en México este mismo año. En ocasiones los octocópteros han permitido al crimen organizado introducir contrabando (drogas, teléfonos e incluso cuchillas) en **prisiones de alta seguridad.**

Algo más sencillo y eficiente es el empleo de los **vehículos como armas** durante los últimos años, existe una importante vulnerabilidad de los actuales protocolos de seguridad ante la posibilidad de que se empleen vehículos oficiales como **ambulancias,** aprovechando el libre acceso que estos tienen a la práctica totalidad de los espacios restringidos, y la confianza que suscitan entre la población y los miembros de las fuerzas del orden, al formar parte de los servicios de emergencia[18].

También hemos visto el empleo de tecnología de **semiconductores para espionaje industrial** mediante ingeniería inversa para la obtención ilícita de todo tipo de información, especialmente con intención de infringir los derechos de propiedad intelectual.

---

[13] Por sus siglas CaaS, supone la existencia de una auténtica industria del cibercrimen.
[14] MaaS permite adquirir servicios de malware.
[15] RaaS ofrece programas ilegítimos de Ransomware para extorsionar a personas y empresas.
[16] Se encuentran en constante renovación, maximización de beneficios y minimización de riesgos, customizando al máximo los servicios ofrecidos: si se quiere atacar a una persona específica se diseña ad hoc con la tecnología más puntera.
[17] Tal y como indican los últimos informes de Europol. Así, las aplicaciones y dispositivos cifrados parecen haberse convertido en la principal forma de comunicación, debido a las garantías que ofrecen para no ser descubiertos.
[18] Lo cierto es que, desde 2001, se han identificado un total de 19 casos en los que una ***ambulancia ha sido empleada como VBIED*** en ataques terroristas: 14 en Oriente Medio y los 5 restantes en el Sudeste Asiático.

Potenciando los mercados del crimen organizado

La tecnología ofrece un amplio abanico de fórmulas de mejora del intercambio de bienes y servicios; algo que, lógicamente, el crimen organizado está sabiendo aprovechar en el mercado negro, cada vez más lucrativo.

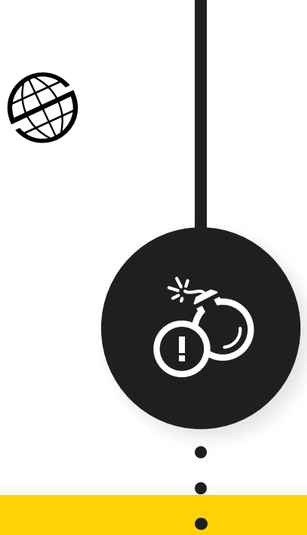
Las **mejoras en la producción,** como el refinado en las **técnicas de cultivo** que reducen la superficie de plantación de cocaína a la vez que se incrementa la producción, el uso de **laboratorios móviles,** de mayor tamaño y con mejores mecanismos de conversión, así como la producción, por parte de los grupos, de **sus propios precursores** como el permanganato potásico son muestras de las constantes aproximaciones de los grupos criminales a una optimización de sus procesos, recursos y servicios.

La sofisticación en la **autoprotección,** como el empleo de drones tanto para el traslado de droga en fronteras[19] o prisiones como el propio diseño de narcodrones y narcosubmarinos[20] para viajes transatlánticos. Para mejorar el tráfico también se transporta droga en **bloques de hormigón,** cocaína **líquida** o en **crema;** además, se vende en internet, especialmente en la darkweb y deepweb, a través de **criptomercados**[21].

Estas fórmulas permiten a las organizaciones criminales **incrementar la eficiencia y maximizar sus beneficios** a la vez que asumen menos riesgos al disminuir su visibilidad y la trazabilidad de sus actividades.

De estas innovaciones tecnológicas de autoprotección también se han beneficiado otros mercados ilegales[22] como el de armas, llegando a establecer talleres de **fabricación de armas mediante impresoras 3D.**

[19] Como entre EEUU y México en 2014.
[20] Como se identificó en España con cargamento procedente de Brasil en 2021.
[21] Plataformas que, por supuesto, se encuentran en pleno crecimiento, pues existe un gran desbalance entre el tiempo que se tarda en localizar y cerrar una plataforma de estas características y el que se tarda en crear una nueva, lo que sin duda es una ventaja para las bandas criminales.
[22] También, por ejemplo, de tráfico de seres humanos y de material de abuso sexual infantil.



Optimizando los ataques terroristas

La apuesta del terrorismo por la innovación a la hora de explorar nuevas formas de perpetrar atentados, como el uso de vehículos, VBIEDs e incluso fórmulas de coordinación con medios tecnológicos han roto con las tácticas del terrorismo clásico. La actividad terrorista tradicional en suelo occidental[23] principalmente implicaba, hasta la aparición de DAESH, la utilización de cargas explosivas (tanto activadas remotamente[24] como detonadas por operativos suicidas[25]). Destacan, por tanto, tres fórmulas innovadoras:

A

Empleo de vehículos convencionales como armas para atentar contra grandes grupos de civiles

Pese a que el empleo de vehículos convencionales como arma ya había sido puesto en práctica en algunas ocasiones anteriores a 2016[26], y aunque la posibilidad de estos ataques lleva décadas contemplada, por ejemplo, por ***informes*** recogidos por el Departamento de Justicia de los Estados Unidos, la innovación de DAESH a la hora de enfocar su ofensiva hacia este modus operandi, aprovechando su sencillez, su bajo coste, su alto impacto y su elevada dificultad de detección[27], ha propiciado que las fuerzas de seguridad se vieran sorprendidas por la magnitud y la imprevisibilidad de los ataques, y que se produjeran graves consecuencias sobre la población[28].

En esta misma línea innovadora, el asalto a Mosul por parte de DAESH, en 2014 (semanas antes de la proclamación del Califato), se basó en el empleo coordinado de varios **VBIEDs[29] suicidas,** equipados con blindajes ***rudimentarios,*** que fueron detonados contra las defensas de la ciudad en ***diferentes puntos de manera simultánea.*** Estos dispositivos provocaron un gran efecto sobre los defensores, que sobreestimaron las fuerzas y recursos de DAESH, y ordenaron la retirada, dejando la ciudad a merced de las fuerzas de DAESH y dando comienzo a 3 años de gobierno local del grupo[30].

---

[23] Con la expansión de la insurgencia en Siria e Irak -especialmente a partir del comienzo de la pérdida de control sobre el territorio, en 2015-, y basándose en las lecciones aprendidas en el campo de batalla, el grupo terrorista DAESH compensó sus limitaciones ofensivas y su pérdida de material bélico con la adopción de una postura innovadora que implicó, desde 2016, un cambio en el modus operandi del grupo y una modificación de las tácticas empleadas por sus seguidores tanto para atentar contra Europa y Estados Unidos, como para mantener su actividad insurgente en sus áreas de influencia.

[24] Como, por ejemplo, ocurrió con el primer atentado contra el World Trade Center, en 1993, o como es el caso de algunos de los explosivos detonados en el atentado perpetrado contra instalaciones turísticas de Bali (Indonesia) en 2002.

[25] Como en el caso de los atentados del 11-M de 2004 en Madrid, atribuidos a un comando suicida de Al-Qaeda.

[26] Por ejemplo, en los ataques llevados a cabo los días 21 y 23 de diciembre de 2014 en las localidades francesas de Dijon y Nantes, respectivamente, que se saldaron sin víctimas mortales.

[27] En el caso de otro tipo de atentados, como los perpetrados con armas de fuego o explosivos de fabricación casera, tanto las armas como los precursores de los explosivos pueden ser sometidos a seguimiento, dado que no se trata de elementos convencionales.

[28] Por ejemplo, los ataques de Niza (2016), Berlín (2016), Londres (Westminster, en marzo, y Puente de Londres, en junio de 2017), Estocolmo (2017), Levallois (2017), Barcelona (2017) y Murcia (2021) fueron perpetrados mediante el uso de vehículos.

[29] Vehículos equipados con artefactos explosivos improvisados.

[30] La experiencia derivada de la utilización de estos medios en el campo de batalla ha tratado de ser exportada sin éxito a Europa, al menos en los siguientes casos: i) Barcelona, 2017: según indican las investigaciones policiales posteriores al atentado de las Ramblas de Barcelona, la explosión de un chalé en la localidad de Alcanar, en las horas previas al atentado, se produjo mientras un comando yihadista fabricaba explosivos caseros con la intención de introducirlos en una furgoneta con la que, primero, arrollar civiles y, después, llevar a cabo una detonación en las inmediaciones de la Sagrada Familia. Ii) París, 2017: un yihadista embistió una furgoneta de la Gendarmería con un coche cargado de explosivos, pero no se produjo la deflagración prevista y la única víctima mortal fue el agresor.

B

Utilización de drones para la carga de explosivos y la comisión de atentados o ataques

Durante los últimos años, se ha registrado un **incremento en el uso de drones caseros modificados para cargar explosivos** improvisados, granadas de mano, granadas de 40mm y pequeños proyectiles de mortero por parte de varias **insurgencias activas** en las guerras de Siria, Ucrania, Libia, Irak o Yemen y presentes también en países como México o Colombia, entre otros.

El primer registro de **uso de drones domésticos** o caseros para la comisión de ataques data de 2014[31]. Desde entonces, se han registrado otros incidentes, como el ataque de un **enjambre de drones explosivos** caseros contra una base rusa en Siria, en enero de 2018; el **ataque** de los rebeldes hutíes[32] contra la plana mayor del ejército yemení, en enero de 2019; los **ataques con drones** durante enero de 2022, en el marco del conflicto entre el Cártel Jalisco Nueva Generación (CJNG) y los **Cárteles Unidos** (Familia Michoacana, los Caballeros Templarios y los Viagras), o las operaciones de **DAESH** en Siria e Irak.

Si bien la innovación en materia de drones lleva décadas en desarrollo, la adopción del concepto de la *"guerra de drones"* y su adaptación a los condicionantes de los grupos criminales e insurgentes supone un enfoque innovador que ha derivado en un enorme desafío a la seguridad. Esto se debe, en parte, a que la mayoría de los sistemas de defensa antiaéreos[33] están pensados para afrontar amenazas propias de un nivel de ingeniería militar muy avanzado (como es el caso de cohetes, misiles, aviones de combate o drones de última generación- y no son aptos, u óptimos, para la interceptación de **drones caseros de pequeñas dimensiones).** Además, en ocasiones el coste de derribo de cada dron es infinitamente superior al coste del propio aparato[34].

C

Innovación para mejorar la coordinación

Las acciones terroristas que tuvieron lugar en la ciudad de Bombay en noviembre de 2008 incorporaron un ***modus operandi innovador*** respecto a las modalidades utilizadas por grupos de carácter islámico radical como Al Qaeda y sus derivados en atentados previos.

La innovación radicó en la extrema coordinación en la concatenación de las ***acciones,*** su ***magnitud y la intensidad*** dificultaron las labores de las fuerzas de seguridad y garantizaron el impacto de las acciones previamente planeadas.

Los ataques, presuntamente planificados desde Canadá y Pakistán, incluyeron tiroteos en infraestructuras que contaban con una amplia afluencia de civiles, específicamente seleccionadas atendiendo a las dificultades que presentaba su control por parte de las autoridades, así como en establecimientos emblemáticos de la ciudad de Bombay. Asimismo, los terroristas emplearon GPS para su orientación y recurrieron a dispositivos BlackBerry y teléfonos satélite para asegurar la coordinación de sus acciones y garantizar la comisión del plan previamente estudiado de manera ***integral.***

---

[31] Cuando la guerrilla de Hezbolá (grupo militante chií con sede en el Líbano) logró llevar a cabo una acción terrorista exitosa contra un edificio de Al Qaeda en la frontera entre Líbano y Siria.
[32] Los hutíes emplean drones de mayor sofisticación, que no pueden considerarse caseros, entre ellos: Samad-1 (envergadura de 3,5 m, 500 Km de alcance, vigilancia), Samad-2 (UAV-X, envergadura de 4,5 m, 500 Km+ de alcance, vigilancia o carga explosiva) y Samad-3 (envergadura de 4,5 m, 1500 Km de alcance, carga explosiva).
[33] Como es el caso de los Phalanx C-RAM o los S-300/400.
[34] A modo de ejemplo, se señala que el coste de un misil Patriot (tierra-aire) oscila entre los 1 y 6 millones de dólares, mientras que un dron casero modificado puede oscilar entre los 100 y los 3.000 dólares. Pese a este bajo coste, un dron casero tiene potencial para causar cuantiosos daños materiales, pérdidas de vidas y un gran impacto psicológico. En esta línea, durante los últimos años han aparecido dispositivos láser capaces de detectar y destruir aparatos de hasta 0,002 m2 de superficie.

Hackeando la mente

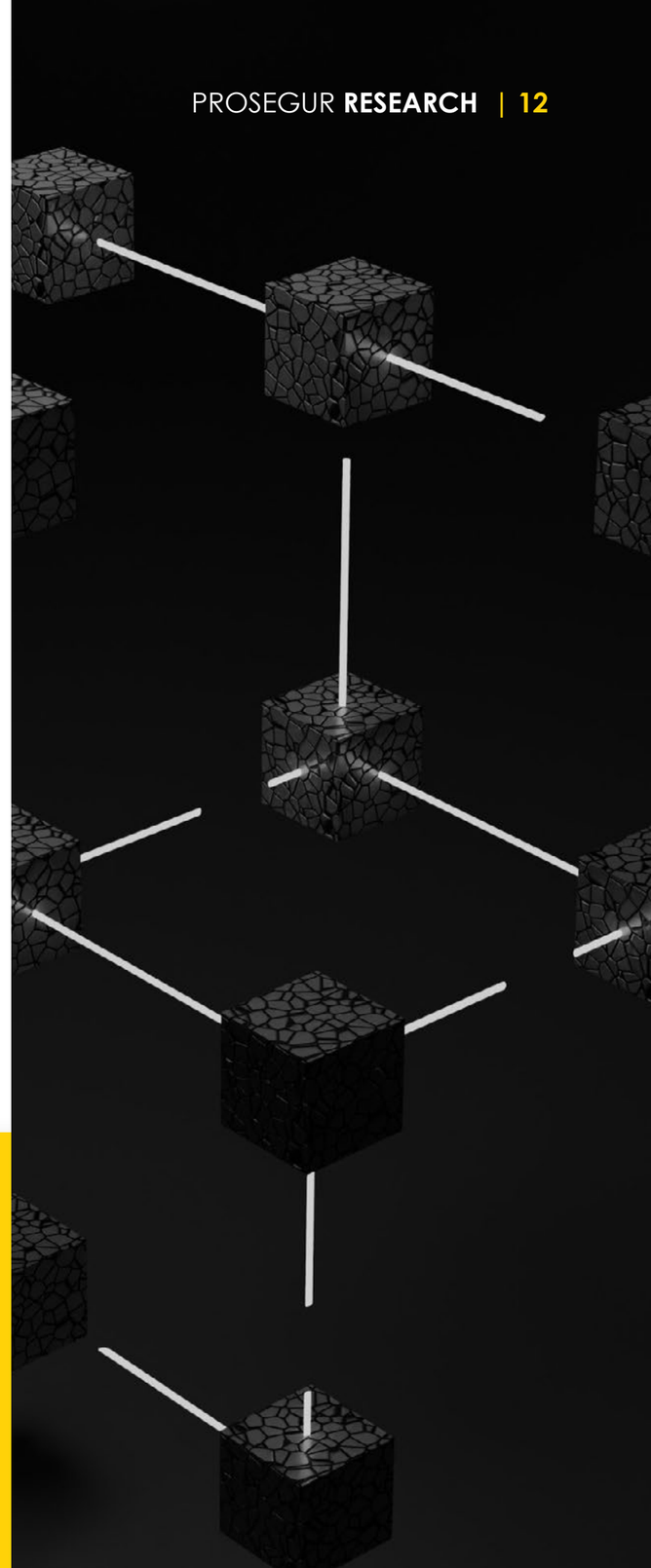
La ingeniera social, inovación que incrementa anualmente, es altamente rentable. Lo cierto es que los **errores humanos son el origen del 95%** de los fallos de seguridad en la actualidad, por lo que se trata de un vector de ataque de enorme valor.

Los engaños para cometer **estafas mediante phishing** incluyen métodos sofisticados como el uso de **chatbots** figurando ser usuarios reales o mediante **deepkafe,** llegando a generar **caras artificialmente** que resultan más confiables que las humanas.

Buen ejemplo de innovación criminal fue la **imitación la voz del CEO** de una empresa energética mediante Inteligencia Artificial[35] para extorsionar a un proveedor en 2019, técnica conocida como **vishing**[36].

Muchas innovaciones en estafas aprovechan la estacionalidad de campañas en las que las personas bajamos la guardia: en el plazo de declaración de la renta con un falso email de la Agencia Tributaria[37], al día de los enamorados fingiendo ser un usuario de una web de citas, así como todo tipo de modas[38].

También el uso de **redes sociales y los videojuegos** más populares del momento son potentes canales de reclutamiento para el **terrorismo** y el **crimen organizado,** bajo la promesa de vivir auténticas aventuras o para la **trata y explotación** de personas a través de sextorsión u ofreciendo falsamente un trabajo o una relación amorosa estable.



[35] Esta estafa se realiza a través de algoritmos que funcionan con RGAs (redes generativas antagónicas) que analizan las grabaciones de voz y permiten generar nuevas frases a partir de ellas.
[36] Un phishing con mensaje de voz.
[37] O similar en cada país.
[38] Como series televisivas populares cuyas temáticas atraen víctimas a ciberataques y estafas.

03 ¿Qué será lo siguiente?

Lo que está por venir

Posiblemente sepamos una pequeña parte de todas las innovaciones criminales actualmente en marcha, y ello nos limita identificar de forma ajustada las tendencias del lado oscuro.
No obstante, podemos apuntar algunas posibles líneas de innovación criminal con un gran potencial.

Veremos cada vez más alianzas entre organizaciones criminales, terroristas y **ciberdelincuentes,** que rentabilizarán los avances en términos de innovación compartiendo productos e ideas.

Continuarán creciendo los mercados del **"todo-como-servicio"** (Everything-as-a-Service) con importantes innovaciones criminales para ataques a la cadena de suministro, la nube, el IoT masivo (MIoT), en plena expansión.

El desarrollo expansivo de la Inteligencia Artificial y la robótica permitirán fabricar mejores armas y robots o soldados criminales, esto es, armas autónomas, incluso nanorobots criminales[39].

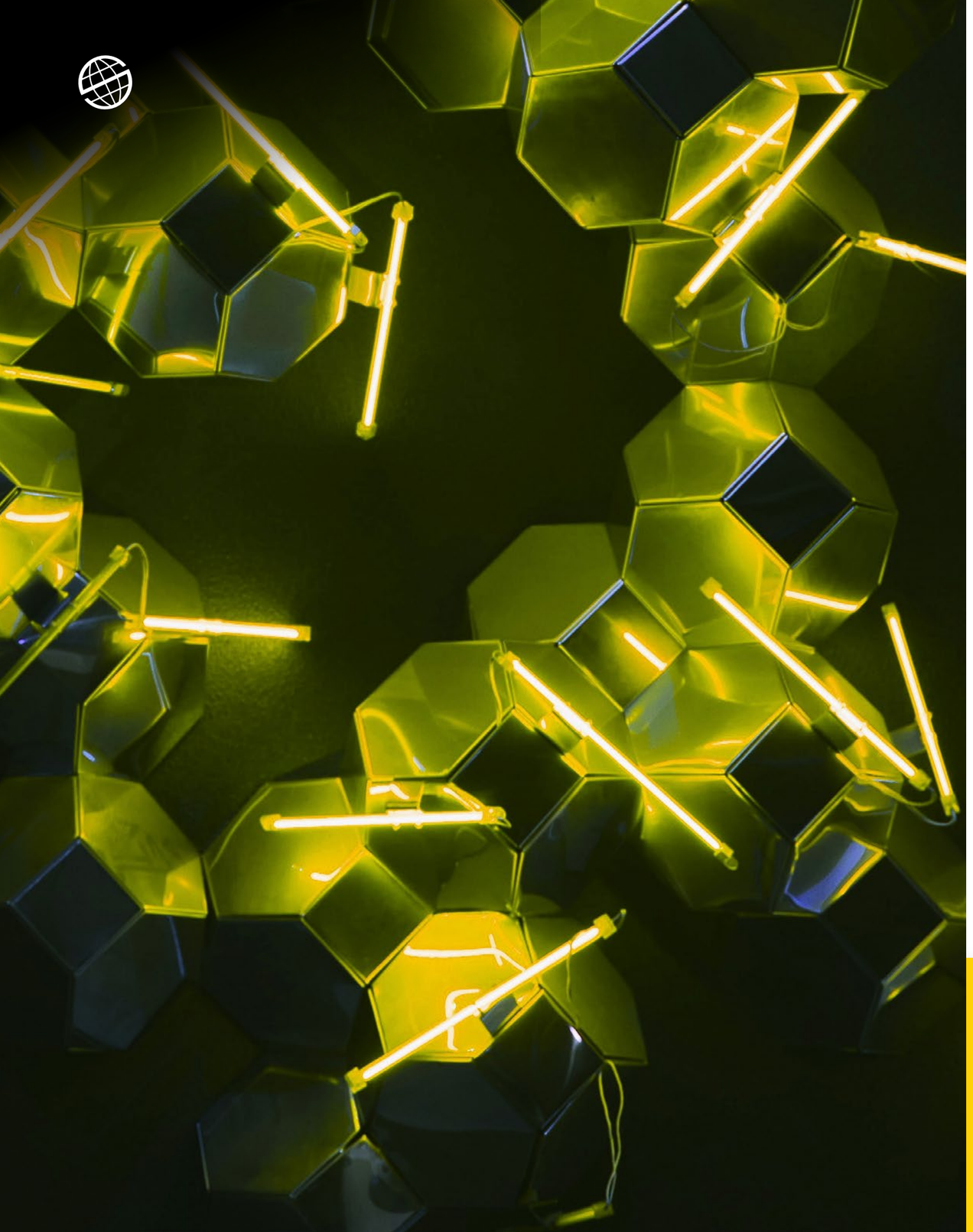
A su vez, este desarrollo tecnológico global supone un contexto complejo en el que se diseñan nuevos ciberataques contra personas que cada vez interactúan más en el entorno digital y empresas en pleno proceso de digitalización.

Entre los posibles usos de drones además de los ataques físicos consistentes en estrellar drones contra personas o propiedades, se encuentran los ataques lógicos[40] mediante puntos de acceso.

La detección de posibles vulnerabilidades en componentes open source, empleados por ejemplo en vehículos autónomos, pueden derivar en ciberataques que generen importantes daños físicos y contra la integridad de las personas.

---

[39] Máquinas muy pequeñas al servicio de organizaciones criminales o terroristas; siempre y cuando mejoren el precio, la accesibilidad y las necesidades de especialización de su tecnología.
[40] La configuración de una red Wi-Fi móvil falsa o un punto de acceso no autorizado con el fin de interceptar el tráfico de red de los smartphones en alcance para capturar información confidencial de los usuarios o tomar el control de sus dispositivos, ya sean móviles, ordenadores, coches, etc.



Tecnología 4D o Next Generation Bioprinting (NGB), que consigue objetos más flexibles, cuyas estructuras pueden transformarse de forma programada en respuesta a un estímulo, actualmente aplicado a la bioimpresión de tejidos vivos, pero con un potencial en producción de drogas.

Los avances en ámbitos como la computación cuántica o el eHealth permitirán un salto importante en términos de innovación criminal. Por ejemplo, en el primer caso, llegando a capacidades de procesamiento que desafíen las herramientas de protección mediante la criptografía empleadas hasta la fecha; en el segundo, las técnicas de edición genética[41], hasta ahora de uso conocido en salud, se puedan emplear para mejorar el diseño de drogas o incluso ataques de **bioterrorismo.**

El desarrollo del metaverso se postula como uno de los grandes vectores de ataque para los cibercriminales en el futuro de Internet[42]. El usuario podría experimentar una enorme diversidad de riesgos o ataques[43], como la suplantación de la identidad, el robo de información personal (datos biométricos, o de navegación, por ejemplo), la extorsión, la estafa o el acoso. Por todo ello, el metaverso, y en general, el entorno digital se ha convertido en un nuevo terreno de juego para la innovación criminal.

La innovación criminal, altamente ligada a la capacidad de aprovechar los desarrollos tecnológicos de manera original, continuará orientándose hacia inversiones de alta rentabilidad y bajo riesgo. En este sentido, las tendencias vendrán marcadas por la accesibilidad de las tecnologías que, si bien suponen un avance positivo para la humanidad, también aportan creativas oportunidades de negocio para los criminales.

---

[41] Concretamente, la técnica CRISPR que cambia una secuencia de genes específicos.
[42] A modo de universo virtual inmersivo, el metaverso se cimenta sobre la base de la socialización virtual, con el objetivo de interactuar con otros usuarios, representados mediante avatares.
[43] Una hipotética economía basada en los NFTs (non-fungible tokens), que se fundamenta en la tecnología blockchain, podría dar lugar a ataques como los ransomware u otro tipo de delitos relacionados con el blanqueo de capitales, especialmente cuando la protección de datos y la propiedad intelectual no estarían claramente definidas.

PROSEGUR

Garantizamos la seguridad de las personas,
las empresas y la sociedad en su conjunto.

research@prosegur.com