El crimen organizado como instrumento de poder

Dr. Pedro Francisco Ramos Josa

Hace tiempo que las nociones tradicionales sobre crimen organizado han dejado de ser útiles a la hora de luchar contra esta lacra social. La imagen distorsionada por la ficción acerca de un grupo de delincuentes unidos por su origen étnico, un particular código de honor y siempre en lucha contra sus rivales y el sistema, se encuentra muy alejada de la realidad de un fenómeno que se ha convertido en una de las principales amenazas para nuestras democracias.

Las organizaciones criminales, lejos de encontrarse en los márgenes de nuestros sistemas, confinadas en la alegalidad, forman parte de nuestras sociedades de igual forma que cualquier otro elemento de la misma. No sólo proporcionan bienes y servicios demandados por determinados sectores sociales, sino que además se han convertido en productores y distribuidores de riqueza.

De igual modo, para comprender la naturaleza actual del crimen organizado hay que indicar que no sólo buscan maximizar sus beneficios de forma egoísta, sino que en no pocos casos acaban formando parte de las redes tejidas por determinados estados para debilitar a sus rivales geopolíticos.

La transnacionalización de la criminalidad, de la mano de la globalización, no sólo ha supuesto que las organizaciones criminales expandan sus actividades por todo el mundo y que la cooperación entre ellas sea más sencilla, también que participen activamente en la pugna por el dominio global. De esa forma, la criminalidad organizada ha acabado por convertirse en un instrumento más en la competición estratégica que caracteriza la escena mundial.

¿Cómo se instrumentaliza la criminalidad organizada?

Como recoge EUROPOL en su último informe *The changing DNA of serious and organised crime*, si bien la ganancia económica continua siendo la principal motivación de las organizaciones criminales, sus acciones son también instrumentalizas, ya sea directa o indirectamente, por aquellos actores externos que despliegan amenazas híbridas, contribuyendo así a sus objetivos políticos e irradiando inestabilidad geopolítica.

Lo que buscan los actores externos con la instrumentalización del crimen organizado es potenciar su capacidad de desestabilización en terceros estados, conscientes de la enorme capacidad lesiva de la que son capaces las organizaciones criminales. A través de actividades criminales tales como el sabotaje de infraestructuras críticas (ya sea a través de medios físicos o digitales), el robo de información, las campañas de

desinformación, los ciberataques, el tráfico de personas o el narcotráfico socavan la fortaleza de nuestras sociedades abiertas explotando sus vulnerabilidades.

El objetivo de esos actores externos no es otro que la desestabilización de nuestros sistemas democráticos, diezmando la cohesión social, la percepción de seguridad y el imperio de la ley en nuestras sociedades, sin olvidar el perjuicio que causan a nuestra estabilidad financiera y prosperidad económica. En ese caldo de cultivo de crisis y desafección inducidas es donde esos actores externos intentan explotar a su favor nuestras divisiones sociales mediante campañas de desinformación que manipulan a su favor la percepción pública.

De ese modo, la cooperación entre actores externos y criminalidad organizada les brinda a ambos la oportunidad de compartir recursos, experiencia y protección en sus actividades criminales. Así, determinados estados ofrecen gustosamente su territorio como espacio seguro desde el cual los criminales cometen sus delitos, lo que es una ventaja para ambos, pues el estado es capaz de negar la atribución del ataque mientras el criminal se mantiene seguro tras perpetrarlo a cambio de proporcionar su infraestructura y conocimientos al estado, en una especie de subcontratación conocida como *crime as a service*.

No sólo eso, la criminalidad organizada, de la mano de su transnacionalización y su capacidad para explotar las ventajas de las nuevas tecnologías, se ha convertido en una pieza clave para aquellos estados sobre los cuales pesan diversos tipos de sanciones internacionales, colocando sus cadenas de blanqueo de capitales al servicio de los gobiernos sancionados. De ese modo, las prohibiciones pueden ser burladas con mayor facilidad, lo que les permite no sólo mantener a flote sus economías, sino incluso mantener el pulso contra sus rivales.

Varios ejemplos de instrumentalización criminal

El primer ejemplo muestra esa colaboración financiera que tantas veces pasa desapercibida en las investigaciones. En diciembre de 2024, la Agencia Nacional del Crimen británica anunció la desarticulación de una red rusa de blanqueo de dinero gracias a una investigación internacional coordinada, con la participación del FBI estadounidense, la Dirección Central de la Policía Judicial francesa, la Garda irlandesa y autoridades de Emiratos Árabes Unidos. Los servicios proporcionados por la red de blanqueo eran utilizados simultáneamente por traficantes de droga como el clan de los Kinahan, delincuentes financieros huyendo de las sanciones occidentales, criminales como extorsionadores en línea y espías extranjeros en sus operaciones en el Reino Unido y en campañas de desinformación orquestadas por el Kremlin, principalmente a través de su cadena *Russia Today*.

La operación se saldó con la detención de 84 personas junto con el decomiso de 20 millones de libras, entre efectivo y criptomonedas, cuyo alcance global quedaba demostrado con su extensión a más de 30 países, desde Europa y Oriente Medio a Sudamérica.

El blanqueo se realizaba a través de dos empresas pantalla, Smart y TGR, que actuaban en tándem desde sus sedes en Londres, Moscú y Dubái. Las redes criminales entregaban a dichas empresas el efectivo a blanquear, luego ese dinero era movido e introducido en el sistema legal mediante un complejo entramado de empresas, sobre todo constructoras, para finalmente devolver el depósito a esas mismas organizaciones criminales en criptomonedas, lo que permitía a estas reinvertir en drogas o armas sin necesidad de mover físicamente el dinero entre fronteras. A su vez, una cantidad significativa de dichas criptomenadas eran el producto de fraudes online, cuyos autores buscaban a cambio dinero en efectivo. De ese modo todo el mundo quedaba satisfecho.

El sistema inventado por la organización actualizaba los principios de la *Hawala* a las herramientas del siglo XXI, lo que les permitía mezclar técnicas tradicionales con nuevos mecanismos de pago para sobrealimentar sus esfuerzos de blanqueo.

Por otra parte, la operación ha evidenciado el papel que la diáspora rusa juega en la política exterior del Kremlin, al instrumentalizar las actividades criminales que se dan en parte de la misma en beneficio del régimen putinista, tanto en su actividad encubierta como en su propio financiamiento.

El segundo de los ejemplos nos presenta una de las caras más peligrosas de la subcontratación de la criminalidad, el sicariato contra quienes son considerados enemigos del régimen. El 9 de noviembre de 2023, cuando Alejo Vidal-Quadras paseaba por el madrileño barrio de Salamanca, un hombre se bajó de una moto y le disparó en la cara antes de salir huyendo. Afortunadamente, el sicario falló en su tiro y su víctima se ha podido recuperar.

El político español, ex líder del Partido Popular en Cataluña, fundador de Vox y Europarlamentario por esa formación, se ha mostrado siempre muy beligerante hacia el régimen iraní, no dudando en usar las instituciones europeas para denunciar los crímenes de Teherán. En respuesta, Irán había anunciado sanciones contra sus críticos, especialmente el Grupo de Amigos de un Irán libre, a los que acusaba de apoyar a grupos terroristas, incitar al terrorismo y propagar la violencia y el odio. Entre los sancionados se encontraba Vidal-Quadras.

Las investigaciones condujeron inmediatamente a un asesino a sueldo, un ciudadano francés de origen tunecino que sería detenido meses después en el barrio de Harrlem, a las afueras de Amsterdam, cuando intentaba perpetrar otro asesinato. Tanto el

sicario como sus colaboradores serían miembros de la *Mocro Maffia*, la organización criminal afincada en Países Bajos y Bélgica, famosa por el control que ejerce sobre sus puertos, desde los que inunda a Europa con cocaína sudamericana, y por haber amenazado con secuestrar a la heredera a la corona holandesa y con asesinar a su antiguo presidente, Mark Rutte, actual Secretario General de la OTAN.

No era la primera vez que Irán se valía de organizaciones criminales para atentar contra lo que considera sus enemigos en suelo europeo, desde ataques a empresas judías a seguimientos de personas públicas y privadas. Pero lo que el intento de asesinato de Alejo Vidal-Quadras revela, más allá de la capacidad iraní en Europa, son los peligrosos lazos de unión entre organizaciones criminales dispuestas a vender sus servicios y determinados gobiernos extranjeros deseosos por contratarlos para así borrar las huellas de su autoría.

Ya no sólo se trata de desestabilizar a las sociedades occidentales, como la elección del momento del atentado sugiere en este caso, justo después de unas elecciones nacionales, sino de amedrentar en el exterior a quienes se oponen y denuncian las prácticas criminales de determinados regímenes, expandiendo la implacable represión interna más allá de sus fronteras.

El tercer ejemplo de instrumentalización criminal nos remite a cómo nuestra dependencia de las nuevas tecnologías puede ser aprovechada para provocar lo que se conoce como un “Pearl Harbor electrónico”. En abril de 2007, el Gobierno de Estonia aprobó la reubicación de la estatua del Soldado de Bronce del centro de la capital, Tallin, a un cementerio de las afueras; la reacción en Moscú no se hizo esperar, al considerar la decisión como una afrenta a su pasado soviético. Incluso se llegaron a producir importantes disturbios civiles en ambos países.

Inmediatamente después y durante el siguiente mes de mayo, Estonia fue el objetivo de un ciberataque coordinado. Durante un período de tres semanas, fueron atacados portales del gobierno y del parlamento, ministerios, medios de comunicación, proveedores de servicios de internet, los mayores bancos y pequeñas empresas, principalmente mediante ataques de Denegación de Servicio Distribuida (DDoS).

La gran mayoría del tráfico de red malicioso tenía origen en idioma ruso e indicios de motivación política. Aunque el gobierno ruso negó cualquier implicación en los ataques, estos estuvieron acompañados por una retórica política hostil por parte de funcionarios rusos, junto a medidas económicas poco amistosas y una negativa a cooperar con la investigación estonia, lo que probablemente alentó a los perpetradores a continuar con sus acciones.

Lo ocurrido en Estonia supuso toda una novedad debido a la capacidad de que los ataques fueran efectivos sin un riesgo significativo de atribución o represalia. Esto se

logró de una manera que no implicaba *hackeos* ni el uso de *malware* dirigido directamente al objetivo, sino que aprovechaba el envío masivo de tráfico de internet hacia los sitios atacados desde computadoras secuestradas (las llamadas computadoras "zombi") ubicadas en todo el mundo. Los ataques no pudieron haber sido llevados a cabo por individuos aislados, sino que se utilizaron herramientas organizadas y automáticas. Las estimaciones varían respecto a cuántas computadoras zombi (*botnet*) estuvieron involucradas, pero algunas estimaciones indican entre 1 y 2 millones.

Es más, la combinación del uso de lo que resultaron ser atacantes profesionales pertenecientes a una organización criminal conocida como la *Russian Business Network*, junto con usuarios principiantes de herramientas DDoS, permitió que estos últimos sirvieran de pantalla para proteger a los primeros del escrutinio mediático y de posibles acciones políticas.

En definitiva, este ciberataque demostró la capacidad de la Federación Rusa para imponer costos elevados y disruptivos a otro estado sin necesidad de recurrir a formas convencionales ni incurrir en una escalada militar o política. Enviando así un mensaje claro: unos pocos hackers pueden provocar daños asimétricos y debilitar la confianza de la población en sus estructuras militares y de seguridad.

La nueva realidad

Por tanto, la instrumentalización de la criminalidad por determinados estados para promover sus objetivos estratégicos comporta un claro perjuicio para la comunidad internacional en general, y para los países en los que actúan las organizaciones criminales en particular.

La respuesta en el actual escenario internacional, dominado por la competición estratégica entre grandes potencias, debe comenzar por sacar a la luz los vínculos de esos estados con la criminalidad organizada, revelar y denunciar su estrategia y a partir de ahí poner todos los medios para luchar contra la penetración criminal en nuestras sociedades.

No podemos continuar en nuestra ingenuidad, debemos asumir que algunos estados usan la propagación de actividades delictivas para socavar nuestras sociedades, de ahí que nuestras políticas criminales deban borrar la separación entre las esferas interior y exterior, ya que todo forma parte de un mismo espacio asaltado por amenazas multidominio, desde campañas de sabotaje y desinformación, a flujos de inmigración ilegal y la expansión de la corrupción institucional.

Los conflictos no sólo se libran en distantes campos de batalla, sino que en realidad se libran a diario en nuestras calles, ordenadores y dispositivos móviles, en una guerra de desgaste cuya primera víctima es quien desconoce serlo.