La tecnología (y la virtud de su uso) en la lucha contra el tráfico ilícito

Raquel Jorge Ricart

Un empleado de Irkutsky Forestry lanza un quadcopter como parte de un monitoreo forestal constante y remoto del área en busca de madereros ilegales en la aldea de Khomutovo, Rusia, 2021 (Alexei Kushnirenko via Getty Images).

¿Cómo podemos utilizar la tecnología de una manera oportuna, proporcionada y segura a la hora de combatir amenazas transnacionales como el tráfico ilegal de personas, animales, fauna, drogas o armas?

La tecnología es un activo cuyos beneficios o efectos negativos dependen del uso que se haga de ella. Se suele hablar de cómo la tecnología lleva a sistemas de vigilancia en algunas ciudades, de la falta de un análisis completo y medido sobre los efectos de las *cámaras de eco* algorítmicas en la polarización política y la creación de discursos de odio en las redes sociales, y tantos otros impactos. Este debate es necesario, tal y como indica Naciones Unidas al señalar que “la tecnología se ha convertido en una piedra angular de la criminalidad” también. Pero, al mismo tiempo, en un acto de tecno-responsabilidad (que no de mover la balanza necesariamente hacia un lado u otro como única vía), es importante plantear que la tecnología también produce otros efectos positivos.

En concreto, el mundo de la seguridad transnacional —el de los tráficos ilícitos, como son la caza furtiva de animales, la tala ilegal, el tráfico de drogas y de armas, y el de personas o especies— es un espacio cada vez más mediado por las tecnologías. Bien para seguir haciéndolo clandestino (como es el caso de parches de ciberseguridad en la *dark* y la *deep web* por parte de ciberdelincuentes para seguir vendiendo drogas y armas y no ser interceptados), bien para aprovechar lo digital para acceder a mayor información personal de las personas o no

garantizar ciertos derechos fundamentales (como sería el caso de la falta de consentimiento informado en la recopilación de datos biométricos de personas refugiadas o en tránsito), entre otros. Pero también la tecnología media para ayudar a combatir estos riesgos y actos ilícitos en otros casos.

Destilando varios casos prácticos

Veamos un ejemplo. La Iniciativa Humanitaria de la Universidad de Harvard (HHI) tiene un programa únicamente dedicado al uso de tecnologías e innovación digital para dar mayor respuesta a las crisis humanitarias o emergencias sobre el terreno, como es el caso del análisis de datos mediante satélite de flujos de "migrantes climáticos" en el Cuerno del África para garantizar que no vayan por zonas peligrosas o sean capturados por grupos criminales.

No es algo únicamente dedicado a la investigación académica. Se trabaja mano a mano con fundaciones o empresas que implementan sobre el terreno esos diseños. Este mismo programa tiene una línea dedicada a la detección y documentación de atrocidades humanas en masa mediante metodologías que integran el análisis satelital de imágenes, y apoya a la mejora de aplicaciones reales. Es el caso del Proyecto Sentinel, una ONG canadiense que ayuda a comunidades amenazadas y en riesgo de ser víctimas de crímenes internacionales a ser protegidas cooperando directamente con ellas para recopilar datos sobre el terreno —por ejemplo, qué tipo de accidentes geográficos existen en su región para prevenir el acceso de ciertos grupos criminales o maliciosos. El Proyecto Sentinel utiliza las tecnologías para

documentar crímenes y mitigar la violencia en cuanto se detecta mediante planes de evacuación y emergencia.

Pero no todo son satélites. La inteligencia artificial también se puede utilizar para combatir tráficos ilícitos. El proyecto de Microsoft *"AI for Earth"*, que trabaja por utilizar la nube y la IA para ayudar a resolver problemas medioambientales, tiene una línea dedicada a prevenir la caza furtiva de elefantes mediante *machine learning*, frenar el comercio ilegal de marfil y conservar el hábitat natural. En esta iniciativa, *Elephant Listening Project*, en la que colabora Microsoft y la Universidad de Cornell se utilizan algoritmos avanzados para distinguir los sonidos de los elefantes, estimar la población, monitorizar sus movimientos e identificarlos individualmente. Este tipo de proyectos al mismo tiempo abre cuestiones sobre cómo garantizar que su buen uso se alinee con el respeto a los derechos fundamentales y humanos, si se protegen los datos recopilados y si el manejo de la IA es proporcionado al objetivo que se espera.

En el ámbito del tráfico ilícito de armas y drogas, el trabajo está realizándose mayoritariamente desde el nivel de los organismos internacionales, como es la INTERPOL, y no tanto a nivel academia-fundación o academia-empresa-fundación como en los casos anteriores. Este modelo se debe a que el tráfico ilícito de armas y drogas es un asunto que en todos los casos ocurre entre dos países o más y, por tanto, requiere una coordinación tanto de planificación de estrategia y prevención, de comunicación, como de respuesta policial inmediata que sea constante y permanente.

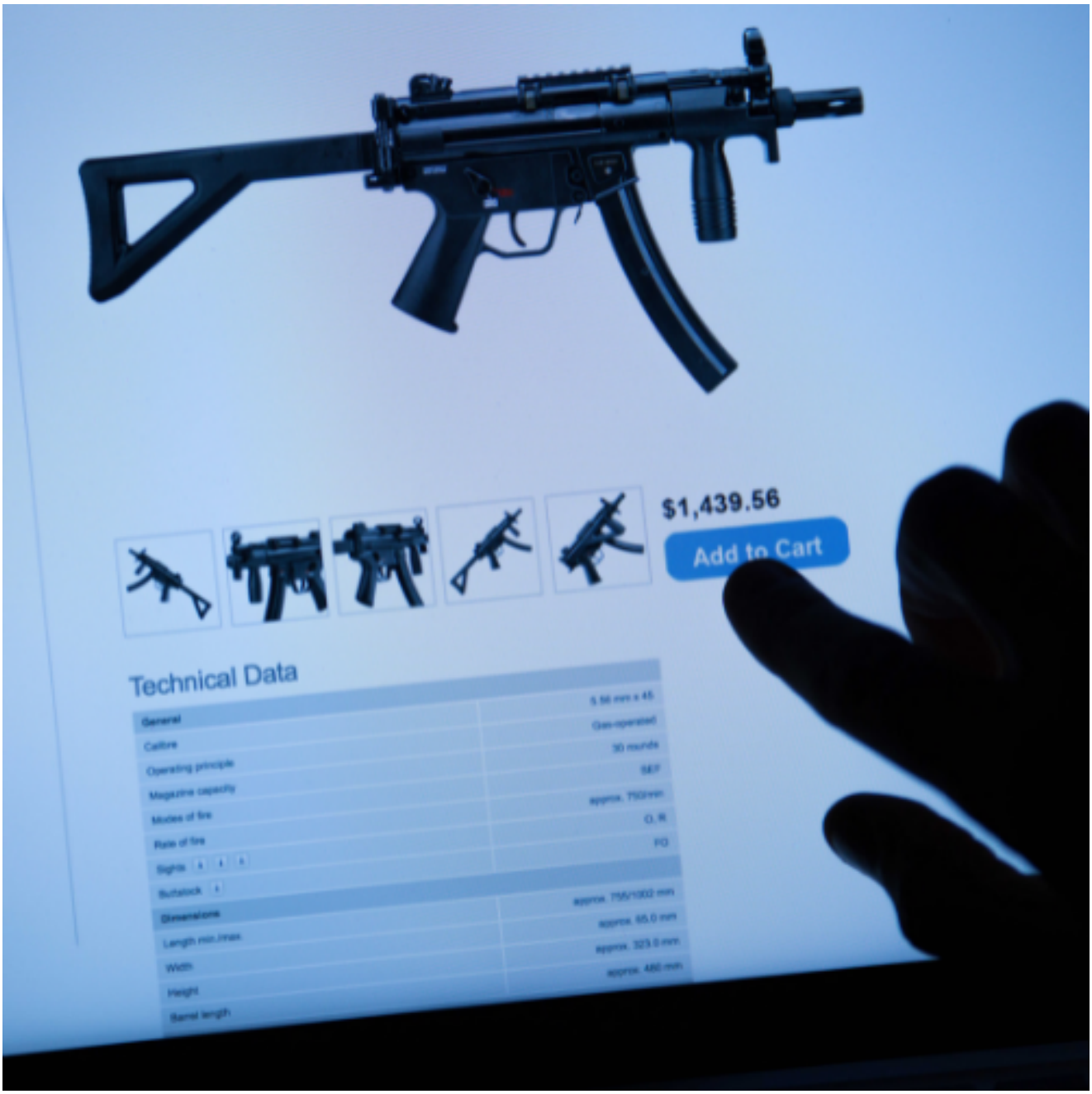
Un informe de RAND Corporation mostraba que el tráfico ilícito de armas, explosivos y munición en la *dark web* es creciente, ya que este espacio facilita la circulación y venta de equipos más allá del mercado negro presencial o físico, puesto que los ciberdelincuentes son cada vez más precisos y sofisticados a la hora de poner parches cibernéticos que les permitan ser invisibles al rastreo digital de la policía. A esto se une que el anonimato de los individuos en la *dark web* complica el trabajo de seguridad digital de la policía, sin tampoco olvidar el creciente uso de criptomonedas alternativas (como Altcoin) que complican la trazabilidad para el sistema financiero tradicional.

Para ello, la Interpol centraliza los Grupos de Trabajo, las comunicaciones entre países e intercambios de datos, y sus equipos de análisis en su Centro de Cibercrimen ubicado en Singapur. A través de este centro, la Interpol provee de talleres de formación y capacitación técnica a Estados y agencias de seguridad en temas como herramientas forenses digitales; ayuda a países con menor madurez de ciberseguridad a defenderse ante ciberataques o a hacer seguimiento de amenazas ilícitas como el tráfico de armas o drogas mediante la *dark web*

; o desarrolla herramientas para seguir las transacciones de criptomonedas mediante blockchain a través de la *Darkweb Monitor*. En este caso, no hay información completa sobre el impacto de este trabajo —pues es un asunto sensible y que muchas veces pertenece a los servicios de inteligencia—, pero hay informes anuales de seguimiento.

Retos y necesidades

Lo cierto es que estos son unos ejemplos entre tantos otros que se están dando para combatir los riesgos ilícitos en varios frentes de la seguridad transnacional mediante el uso de tecnologías. Sin embargo, la relevancia de este tema no es tanto el ejemplo en sí, como los desafíos que plantea.



Una de las primeras cuestiones que debe abordarse cuando se utilizan las tecnologías para luchar contra el tráfico ilícito de personas, animales, fauna, drogas, armas u otros, es el modelo de gobernanza. Es decir, quién está gestionando estos proyectos. Esto puede verse de varias formas: la academia o un *think tank* con libertad de cátedra para investigar aquello que considere más oportuno mediante financiación de una empresa privada que no exige un entregable específico; un modelo horizontal en el que una empresa privada y un centro de investigación trabajan conjuntamente para un objetivo específico previamente delimitado; una empresa privada que aporta el producto y lo ofrece directamente a un gobierno o entidad pública para su implementación; o un organismo internacional —como sería el caso de la

Interpol, o la UNODC u Oficina de Drogas y Crimen de Naciones Unidas— y que funciona como plataforma o *hub* de encuentro, coordinación y comunicación para países tanto avanzados como no en la madurez tecnológica.

No hay un modelo único, oportuno ni efectivo. Todos los modelos tienen ventajas y desventajas: mientras que unos aportan rapidez para implementar un sistema y dar respuesta inmediata a crisis, otros puede que sean más lentos, pero tienen otro factor importante: la generación de medidas de confianza entre países que son desiguales en lo tecnológico, pero que se necesitan mutuamente para combatir estas amenazas.

Sin embargo, analizar quién gobierna qué tipo de proyectos es importante para una segunda pregunta: qué mecanismos de protección se han establecido para garantizar el uso proporcionado, adecuado y positivo de los datos recopilados —en el caso de la IA y de las imágenes satelitales— y qué mecanismos de defensa y respuesta se han complementado para asegurar que esta información no pueda ser interceptada por otros —como ocurre con las bases de datos de las ONG, que tienen un elevado grado de vulnerabilidad a ciberataques.

En este asunto, un reto mayor es que no existen todavía normas internacionales vinculantes de gestión de datos que puedan dar respuesta al fenómeno de las tecnologías que recopilan datos de diversos países y fuentes para hacer frente a amenazas transnacionales, es decir, entre países. El Comité Internacional de la Cruz Roja trata de dar respuesta a este tema mediante su *Manual de Protección de Datos en la Acción Humanitaria*, aunque no es de carácter vinculante. También la Cruz Roja hace concursos para descubrir innovaciones en tecnologías humanitarias e incluye en sus requisitos que se garantice el uso adecuado de datos. Sin embargo, los intentos por garantizar esta protección son todavía *ad hoc* y dependen del actor que lo desea hacer por cuenta propia.

A este tema se une el grado de participación de las ONG pequeñas y medianas en comparación a las grandes. Amnistía Internacional ya tiene su sección *AmnestyTech*, se han creado organizaciones no gubernamentales internacionales con un presupuesto elevado, como *AccessNow* o *Centre for Democracy & Technology*, quienes trabajan con ONG pequeñas sobre el terreno para recopilar datos. Sin embargo, todavía queda un largo trabajo para involucrar a organizaciones de esta base territorial, no como colaboradoras o receptoras, sino como agentes propiamente activos e independientes a la hora de usar tecnologías propias para responder a sus propios retos. Aquí entra el problema de la falta de presupuesto, de capital humano y de concienciación sobre el *Doing no digital harm* (no hacer daño digital). Esto va hilado con que en los últimos años se habla cada vez más del *AI4SocialGood* (IA para el Bien Social), o de tecnologías con un impacto social positivo. Sin embargo, deberíamos plantearnos

realmente a qué nos referimos con “bien social”, para quién va dirigido y con qué medios esto se consigue (y el constante y necesario dilema entre los medios y los fines).

En conclusión, el uso de las tecnologías para combatir las amenazas transnacionales como el tráfico ilícito de personas, animales, fauna, drogas o armas, entre otros, aparece como una oportunidad y como un reto. Es en este binomio donde justamente reside la virtud de su uso, para que sea oportuno, proporcionado y medido a las necesidades reales.

Con el apoyo de:

Fecha de creación
4 noviembre, 2021