EN RADAR: TENDENCIAS DE DEFENSA Y SEGURIDAD EN LA POSPANDEMIA

INFORME FINAL

KONRAD ADENAUER STIFTUNG

Suipacha 1175, Piso 3. C1008AAW
Ciudad de Buenos Aires
República Argentina
Tel: (54-11) 4326-2552

www.kas.de/argentina

info.buenosaires@kas.de

Diciembre 2021

I. INTRODUCCIÓN

Este informe es producto de los debates, las reflexiones y las conclusiones alcanzadas por expertos en defensa y seguridad de Argentina, Alemania, América Latina y el mundo en el ciclo de sesiones académicas virtuales organizado por la Fundación Konrad Adenauer y la Fundación Embajada Abierta durante el mes de noviembre de 2021 y titulado "En radar: tendencias de defensa y seguridad en la pospandemia".

Los vertiginosos cambios del siglo XXI aceleran las transformaciones del sistema internacional en múltiples tableros. Dos de ellos, profundamente entrelazados, son la defensa y la seguridad. Desde la consolidación de nuevos actores a las innovaciones tecnológicas, vemos cómo diferentes agendas locales, regionales y globales se ordenan en torno a nuevos desafíos políticos, económicos, militares, sociales y hasta éticos.

Si bien hay un protagonismo acentuado por parte de China y los Estados Unidos, estamos en un mundo que no tiene las características que protagonizaron antes las tensiones de la Guerra Fría. Un mundo que no es estático, sino que está en constante movimiento. Sin embargo, la interdependencia entre ambos Estados es fuerte e impacta en los proyectos y en los intereses del resto de los actores mundiales.

Esta situación, por ejemplo, ha llevado a los Estados miembros de la Unión Europea a avanzar en la elaboración de una estrategia de seguridad y de defensa autónoma debido al nuevo enfoque de la política exterior estadounidense y su intención de no involucrarse en proyectos que no entran en el ámbito de sus propios intereses nacionales.

La pandemia de COVID-19 y sus implicaciones más amplias han puesto de manifiesto la importancia de las transformaciones de todos los aspectos en la sociedad, y la tecnología ha desempeñado un papel fundamental al respecto, a la vez que ha alterado drásticamente la industria de la defensa.

Las potencias están tratando de acelerar drásticamente sus modelos de adquisición para conseguir que las tecnologías más prometedoras lleguen a su campo más rápidamente, como ilustra el caso de la puja por el 5G. Las nuevas amenazas cibernéticas, electromagnéticas y de guerra biológica aumentan la urgencia y cambian la naturaleza de la defensa y la seguridad.

Esto refuerza la necesidad de un cambio de mentalidad que deje atrás la seguridad tradicional y que ponga sobre la mesa la seguridad humana.

Agendas que se creía que no estaban vinculadas a la seguridad, como el comercio y el cambio climático, en los últimos años han demostrado de manera contundente la importancia de incorporar agendas más amplias a los cálculos de política pública por parte de los Estados.

Los Estados se enfrentarán a una mayor competencia en la prestación de servicios públicos que tradicionalmente han sido responsabilidad de los gobiernos y se enfrentarán a los nuevos actores no estatales, tanto a nivel nacional como internacional.

La ciberseguridad, las armas autónomas, la industria satelital y el crimen transnacional organizado son ejes centrales para comprender de forma

más acabada los conceptos principales de la defensa y la seguridad en el siglo XXI y el impacto de la pandemia en ellos. Todas estas temáticas se combinan para hacer sonar una alerta que no podemos postergar: el mundo post COVID-19 será más inseguro.

II.
CIBERSEGURIDAD

En esta primera mesa quedó en evidencia que quizás la mayor tendencia que requiere esfuerzos de mitigación es la centralidad de la información en el siglo XXI, situación que la pandemia profundizó debido al número insólito de personas que tienen ahora acceso a información casi ilimitada.

La potencia de procesamiento, el volumen y la variedad de datos y la conectividad seguirán creciendo exponencialmente e impulsarán el desarrollo de la inteligencia artificial, la computación cuántica y la capacidad de resolver problemas de creciente complejidad y dificultad.

En un ciberespacio cada vez más poblado, la información desempeña un rol fundamental para la comisión de ciberataques y la difusión de información falsa. En ese sentido, las redes sociales pueden provocar una "cámara de resonancia" que polarice a las poblaciones, erosione la confianza en las instituciones y cree incertidumbre y alimente una violencia social latente.

La ciberseguridad configura una problemática que nos obliga a poner el foco en la importancia trascendental de mejorar las medidas de seguridad, no solo en nuestras computadoras personales, sino, en especial, en los sistemas gubernamentales, ya que las amenazas digitales respecto a las infraestructuras críticas de los Estados son una realidad acuciante.

Todos hemos sido testigos de cómo en las primeras décadas del siglo XXI el aumento de incidentes relacionados con ataques cibernéticos y sus impactos cada vez más dañinos han crecido de forma exponencial. La debilidad de los Estados en materia de seguridad, en especial los de bajos recursos, es un elemento crítico.

La tecnología se ha transformado en un recurso de poder y esta no está solo en manos del Estado. El sector privado avanza más rápido que el público, básicamente porque tiene recursos técnicos y financieros más avanzados frente a urgencias más acuciantes del sector público. El ejemplo de Latinoamérica es elocuente. Varios Estados buscan incluir la ciberseguridad en sus agendas domésticas, pero cuando surge alguna crisis económica y/o social, se hace imposible el sostenimiento de políticas vinculadas a esta temática.

Por ese motivo, los países de renta media o países menos desarrollados deben apostar a la regionalización con un enfoque sistemático y planificado que articule lo regional y lo global. Para esto se debe avanzar en un relevamiento ordenado y sistemático de este nuevo "ambiente", ponderando capacidades y vulnerabilidades de las redes de comunicación al tiempo que se forman cuadros preparados en nuevas tecnologías. La interacción entre los distintos niveles de gobierno y la construcción de una diplomacia del ciberespacio son elementos esenciales ante estos nuevos escenarios.

El abordaje de las agendas de la seguridad y de la ciberseguridad también ha sido parte del debate. Las conclusiones alcanzadas demuestran que es fundamental el trabajo paralelo en ambas, pero de forma conjunta con la agenda de desarrollo. Así se planteó la necesidad de un esquema de ciberseguridad multidimensional donde se permita generar sistemas de estabilidad, pero que no comprometan el desarrollo, buscando como fin último

la preservación de la integridad nacional, la estabilidad política, económica y social.

La evolución del cibercrimen en la pandemia ha sido exponencial y ha operado de forma muy agresiva. Frente a un escenario donde la totalidad de la población mundial requirió del uso de la tecnología para mantener una cierta normalidad, surgieron amenazas que eran desconocidas para la mayoría de las personas y quedaron en evidencia, como nunca, la vulnerabilidad y la dependencia de los sistemas cibernéticos por parte de la humanidad en su conjunto.

Sin duda, uno de los aspectos en donde la postpandemia tendrá mayor impacto es en la digitalización y la ciberseguridad. Para afrontar esos nuevos desafíos, será fundamental explorar posibilidades de generar mayores estrategias de cooperación, mecanismos adecuados y apelar a estrategias multilaterales que den respuesta a estas amenazas de manera más eficiente que antes o durante la misma.

Se debe entender la ciberseguridad no solo como protección, sino también como herramienta de crecimiento. Sin seguridad no hay desarrollo y sin desarrollo no hay seguridad.

Esto implicará un arduo trabajo en todos los sectores de la sociedad, ya que esta problemática se encuentra todavía en un nicho de la agenda política. No es parte de las grandes políticas en general. La pandemia nos ha dado un ejemplo de qué sucede cuando no se toma conciencia de las amenazas. Si hubiera un virus informático como una pandemia, esa conciencia llegaría al instante.

III.
ARMAS AUTÓNOMAS

Sin duda, donde más brutalmente podemos ser testigos del rol de las nuevas tecnologías es en las armas autónomas, cuyo desarrollo tiene profundas implicaciones para el futuro de la defensa y la seguridad. El impacto a largo plazo de la inteligencia artificial (IA) en las relaciones internacionales no tiene precedentes en la historia.

Los sistemas de armas autónomos (AWS, por sus siglas en inglés, o LAWS) son aquellos en los que no es necesaria la intervención humana en la selección de objetivos y el posterior ataque.

Tras el fin de la segunda guerra mundial, pero con mayor énfasis tras el fin de la Guerra Fría, surge un nuevo paradigma que orienta las acciones militares hacia fines humanitarios. Esto derivó en la búsqueda de armamentos cada vez más precisos, con el fin de disminuir la cantidad de civiles y militares muertos en combate. Para los años 80 ya existían teóricamente, pero no fue sino hasta los 90 que los elementos tecnológicos para el desarrollo de las LAWS comenzaron a ser una realidad.

Ahora bien, en la actualidad el desarrollo de los LAWS en general y de la IA en particular, y su complejidad, van cada vez más rápido. El recientemente exitoso lanzamiento de misiles hipersónicos por parte de China y la

consecuente inversión y el desarrollo de los EEUU en sus propios sistemas para enfrentar a su contraparte china comienza a encender las alarmas sobre una posible nueva carrera armamentista.

Ahora bien, cuando se habla de LAWS, no se debe hablar de la diferenciación de lo que es o no un arma, sino de qué partes de un sistema de armas son las que hacen que el sistema sea letal. Un sistema de radar o un láser pueden ser esenciales para combatir con precisión un objetivo, pero ciertamente no son los que causan daño o matan. Sin embargo, la munición es la parte letal, que es la razón por la que ahora existe una prohibición de las bombas de racimo, por ejemplo. Con las LAWS es más difícil trazar esta línea, que es una de las razones por las que las negociaciones internacionales no logran avances significativos. No podemos simplemente prohibir los LAWS o permitirlos totalmente, porque hay partes de ese sistema que no son letales.

Los defensores de los LAWS sostienen que estos permiten asumir mejor los principios de distinción y de proporcionalidad. Con estos sistemas, argumentan, es más fácil distinguir e incorporar parámetros que permitan disminuir los daños colaterales; distinguir aquello que es una amenaza de aquello que no. A su vez, estos sistemas permitirían alcanzar una proporcionalidad en la respuesta ante una agresión y asegurar que no exceda a la agresión misma.

Esto explica, en parte, uno de los motivos del interés por parte de los Estados en desarrollar armas autónomas.

Ahora bien, el principal foco de debate en la actualidad sobre estas armas es su tipificación y su control por parte del derecho. La discusión cuando hablamos de LAWS no es sobre lo letales que son, sino sobre las implicancias éticas y legales de estas armas cuando un humano aprieta el gatillo o, en este caso, el botón.

Como sabemos, el derecho regula conductas humanas; no está concebido para otras conductas. Por eso, la forma en que podrá regularse, o no, este ámbito, depende del grado de autonomía de las armas. Así, si el sistema es enteramente autónomo se presenta el problema de determinar quién es el sujeto responsable último de la operación del sistema.

El tema principal es la responsabilidad. ¿Quién es el responsable de un uso indebido de armas? ¿Es el operador, el programador, el ejército? ¿Qué sucede cuando no funcionan como deben de funcionar? Las armas autónomas son precisas hasta que dejan de serlo. El posible acceso a estas tecnologías por actores no estatales, o incluso por organizaciones terroristas, es una amenaza real y que debe ser analizada por la comunidad internacional.

En la actualidad hay un amplio consenso respecto al rol de los humanos y su papel decisivo en la decisión de matar por medios militares o no. Sin embargo, aún no hay una respuesta definitiva sobre cómo se puede hacer operativo este principio de "control humano". Incluso dentro de una alianza como la que existe entre Alemania, Francia y España en relación con el Futuro Sistema Aéreo de Combate, no existe un acuerdo final sobre los requisitos de un sistema autónomo.

El principal foro en el que las partes interesadas debaten sobre los marcos para las armas convencionales es en el marco de la Convención sobre Prohibiciones o Restricciones del Empleo de Ciertas Armas Convencionales que Puedan Considerarse Excesivamente Nocivas o de Efectos Indiscriminados de las Naciones Unidas (CCW por sus siglas en inglés) y sus protocolos. La convención tiene como objetivo restringir o prohibir las armas que provocan un sufrimiento excesivo. Desde 2014 las LAWS han comenzado a estar en la agenda de la CCW y, desde 2017, el Grupo de Expertos Gubernamentales se dedica a este tema.

El Grupo de Expertos Gubernamentales tiene el mandato de desarrollar elementos para un marco normativo para un protocolo de la CCW sobre las LAWS que sea legalmente vinculante; algo que parecería ser poco probable en el corto plazo, dada a la falta de apoyo de potencias como los EEUU o Rusia.

El debate de las LAWS es muy complejo. Hace más de quince años que se lleva a cabo y los avances han sido limitados. Las crecientes amenazas y el acelerado desarrollo tecnológico, potenciado por actores privados, parece traer más incertidumbre que respuestas hacia el futuro y la regulación por parte de la comunidad internacional de estos sistemas parece estar aún lejos de alcanzarse.

IV.
INDUSTRIAL SATELITAL

Esta industria es cada vez más importante debido a la creciente centralidad de los sistemas satelitales en la vida humana. Ello se verifica con incontables ejemplos, en especial la creciente importancia del planeamiento del petróleo.

En los próximos años se verificará la importancia creciente de lo espacial en la vida humana y, al mismo tiempo, cómo la inutilización de estos sistemas puede traer perjuicios no solo para la economía y la actividad cotidiana, sino también para la soberanía y la seguridad nacional.

Estamos hablando, por ejemplo, de que potencias estén en condiciones de apagar satélites de otros; en el corto plazo veremos demostraciones de los países que tienen capacidad de hacer esto. India y China han hecho experimentos militares para que otros puedan adquirir sus satélites desactivados, con el fin de demostrar su capacidad de hacerlo.

Además, hay que tener presente la vinculación entre la guerra espacial y la cuestión cibernética. Esto nos alumbra un panorama en el que estamos rodeados indirectamente de sistemas espaciales.

Esta actividad involucra a actores privados, como por ejemplo Virgin, una empresa importante que tiene lanzamientos de plataforma aérea. Hoy en

el mundo hay cuatro empresas que están autorizadas a lanzar satélites al espacio; todas cuentan con una capacidad financiera muy importante, lo que les permite tener un desarrollo propio. Pero también involucra cooperación bilateral. Por ejemplo, la agencia espacial alemana (DLR) investiga en forma conjunta con Brasil combustibles espaciales, un área científica en expansión.

Cabe remarcar la importancia de la industria satelital dentro de la geopolítica de los espacios ultraterrestres. Estos se han convertido en un tablero de juego entre potencias y otros actores poderosos. A la disputa tradicional se suman nuevas, como la minería espacial (*space mining*).

Por supuesto, todavía existen limitaciones tecnológicas para que la industria sea viable. A pesar de ello, hay países que abren sus brazos a la venta de estos espacios ultraterrestres. En los próximos años esperamos ver cambios en los sistemas legales.

El Tratado Sobre los Principios que Deben Regir las Actividades de los Estados en la Exploración y Utilización del Espacio Ultraterrestre, Incluso la Luna y Otros Cuerpos Celestes de 1967 establece que ningún país puede declarar soberanía sobre un cuerpo celeste, pero no dice que no se puedan obtener recursos del espacio ultraterrestre. Este tratado deja abierta la posibilidad de la utilización de estos espacios para fines científicos. Se puede hacer un paralelismo con la Antártida desde el punto de vista jurídico, como así también con las potencias de China y EEUU desde el punto de vista geoestratégico.

Es muy difícil que una norma siga siendo aplicable en un contexto y que en otro sea igual de válida y efectiva. El contexto actual es diferente al de cuando se escribió el tratado del 67. En ese momento, en el contexto de la Guerra Fría, donde los únicos actores espaciales eran agencias nacionales

que se adaptaron a ese contexto. Ahora la tecnología va más allá, al igual que la capacidad de inversión. Los actores privados no existían por no tener tecnologías ni fondos para emprender las aventuras espaciales. El derecho internacional deberá evolucionar para hacer frente a estos nuevos desafíos.

Dentro de los cuerpos celestes tenemos asteroides que contienen condritas, de las que se obtienen agua, platino y otros metales. En el futuro de la industria espacial, es el agua lo que más importa. La minería espacial se hace posible incluso tan cerca como la Luna, donde se descubrió un isótopo de uranio que crea energía nuclear no contaminante, cuyo valor económico y ambiental es elevadísimo.

La explotación de estos recursos ha desencadenado reacciones encontradas y preocupación en la comunidad internacional. A tal respecto, la ciudadanía global espera que potencias espaciales como Rusia, EEUU y China cooperen en este ámbito. Sin embargo, estamos lejos de esto. Por ejemplo, bajo la administración Trump, Estados Unidos exacerbó esta situación con la orden ejecutiva de Fomento del Apoyo Internacional a la Recuperación y Utilización de los Recursos Espaciales que se firmó en abril 2020, que permite la explotación y extracción de recursos ultraterrestres, lo que abrió la puerta para su explotación comercial.

En esta misma línea encontramos los Acuerdos de Artemis, en octubre del 2020, que suponen un marco legal de explotación minera y de cuerpos celestes por parte de individuos con fines comerciales. Esta iniciativa fue firmada por Australia, Emiratos Árabes Unidos, Canadá, Italia, Reino Unido, Japón y Luxemburgo, y dejó a un lado a China y Rusia, lo que empujó a Moscú y Beijing a una cooperación estrecha.

Por otro lado, la Agenda 2030 contempla la diplomacia espacial para crear alianzas, siempre considerando que el fin último debe ser pacífico y aboga

por el fortalecimiento de la cooperación internacional teniendo en cuenta las necesidades de los países en desarrollo. Más allá de esto, predomina todavía un panorama hobbesiano, en el que los intereses estratégicos de las principales potencias espaciales se imponen. Un enorme desafío en esta carrera será la inclusión de otros países para que participen en esta nueva frontera de competencia internacional.

Respecto a los riesgos de seguridad dentro o en relación con el espacio exterior, hay un riesgo que a menudo pasa un poco inadvertido, a saber, la interdependencia entre el espacio y el ciberespacio.

En nuestras sociedades dependemos cada vez más del funcionamiento de la infraestructura de los satélites y de los activos basados en el espacio, ya sea para el posicionamiento temporal o para la navegación, ya sea para la observación de la Tierra y del tiempo o para los sistemas de defensa antimisiles. Por lo tanto, cada vez más, cualquier interrupción o pérdida de capacidad podría conducir a impactos potencialmente dañinos.

Para funcionar correctamente, los sistemas relativos al espacio dependen de las redes basadas en internet, y viceversa. Vemos un alto potencial para el aumento del compromiso de los sistemas basados en el espacio debido a varias vulnerabilidades.

Primero, existe un elevado número de puntos de entrada, ya que todos los segmentos pertenecientes a la infraestructura espacial pueden ser potencialmente atacados. En la actualidad sigue existiendo la creencia generalizada de que basta con proteger los límites exteriores o el sistema terrestre, mientras que la propia nave espacial suele tener una protección cibernética mínima o nula (también porque históricamente se pensaba que hackear un satélite no era posible).

Segundo, debido a las numerosas interfaces (de datos) entre el sector militar y el civil y, en particular, en el ámbito de las tecnologías de la información. El sector civil no tiene necesariamente dentro de sus prioridades la seguridad de sus sistemas.

Tercero, por el uso de hardware y software informático obsoleto, que a menudo no puede volver a actualizarse debido a que muchos de los satélites no tienen suficiente memoria o capacidad de procesamiento, a veces incluso para albergar el típico software antivirus.

Cuarto, por la imposibilidad práctica de realizar actualizaciones periódicas de software para subsanar vulnerabilidades conocidas, ya que muchos de los sistemas funcionaban 24/7, y resulta prohibitivo ejecutar actualizaciones de seguridad debido a la dañina interrupción del servicio que esto supondría.

Además, existen muy pocas normas de ciberseguridad para los sistemas espaciales y se observa un progreso muy lento en este ámbito. Y debido a que la nueva economía espacial está configurada con la necesidad de ahorrar costes, con tecnología lista para usar y software de código abierto, y con satélites cada vez más pequeños, la ciberseguridad del sistema en general a menudo se descuida o el propietario del satélite ni siquiera sabe cuán seguras son las partes individuales. Además, con la gran cantidad de satélites que hay actualmente en el espacio y los muchos satélites pequeños, es imposible que los humanos se den cuenta de cada comportamiento anormal en los movimientos de aquellos.

A diferencia de otros riesgos de seguridad en el espacio exterior o en los satélites, como la presencia de armas antisatélite de cualquier tipo, muchos de los riesgos de ciberseguridad pueden ejecutarse de forma relativamente fácil y rentable (en comparación con otros). En muchos casos, la tecnología

necesaria para atacar un satélite está disponible para el ciudadano común en el mercado.

Por lo tanto, los ciberataques a los sistemas basados en el espacio también pueden ser ejecutados potencialmente por actores no estatales. Además, los costes de la piratería informática están disminuyendo, mientras que los beneficios están aumentando.

Algunos riesgos, como la interferencia o la suplantación de la comunicación, son reversibles; otros podrían provocar el daño de un satélite y el consecuente desencadenamiento de otros riesgos de seguridad. El problema es que las ciber-vulnerabilidades minan la confianza en los sistemas estratégicos, al tiempo que aumentan la incertidumbre en la información y el análisis.

Esto también puede conducir a un deterioro de la confianza entre los actores, también porque la atribución de los ciberataques es muy complicada. Los ciberataques podrían desencadenar una nueva escalada en el ámbito del espacio exterior y, posiblemente, provocar la represalia de un ciberataque con otros medios.

Un gran tema de debate es el desafío de llevar esta cooperación más allá de coyunturas políticas, más allá de nuestros gobiernos de turno e incluso pensar regionalmente más allá de los intereses de cada Estado. Los países en desarrollo y desarrollados que apuestan por una vertiente científica tendrán más posibilidad de construir espacios de cooperación.

No puede perderse de vista que el ambiente espacial tiene un carácter geopolítico. De ahora en más, deberá formar parte de los balances de rivalidad geopolítica.

V.
CRIMEN TRANSNACIONAL ORGANIZADO

Tras los debates y las presentaciones avanzados en esta mesa, podemos afirmar que la creciente complejidad y la naturaleza global de los desafíos de la figura del crimen transnacional organizado (CTO) nos exigen una visión más integral y soluciones más sofisticadas para hacerle frente. El impacto económico y social de las redes criminales es cada vez mayor, y las nuevas corrientes de seguridad que intentan hacer frente a las cambiantes prácticas de las primeras no parecen estar teniendo el impacto esperado.

Por otro lado, los vínculos entre el crimen, el terrorismo y la insurgencia suponen un desafío adicional por su penetración en las estructuras estatales y empresariales. Estas dinámicas se vieron reforzadas por la globalización, primero, por la crisis de gobernanza global más tarde y por la pandemia en la actualidad.

Actualmente, el crimen organizado (CO) es un tema plenamente inserto en la agenda de la seguridad internacional contemporánea. Este fenómeno está considerado una amenaza no convencional (en tanto no está protagonizada por Estados ni canalizada por medios militares) de naturaleza transnacional.

La Convención de Palermo de las Naciones Unidas del año 2000 fue el primer instrumento internacional sobre la temática, ya que recién tras el fin de

la Guerra Fría el CTO fue objeto de atención en el campo de las relaciones internacionales.

Desde esos momentos hasta el presente, el fenómeno de la criminalidad organizada no ha cesado de crecer; uno de los indicadores de este aumento es el volumen de capitales que moviliza.

Latinoamérica ocupa un lugar relevante en el mapa del CTO global. Aunque prácticamente todas las manifestaciones de este tipo de crímenes (tráfico de armas, narcotráfico, contrabando de personas, trata de personas, tráfico de órganos, contrabando y falsificaciones) se observan en su geografía, destaca el narcotráfico, a partir de la conjunción de una serie de factores, entre ellos: la producción del 100% de la cocaína global, de importantes cantidades de cannabis y algo de heroína; la existencia de los dos mayores mercados nacionales de consumo de cocaína (EEUU y Brasil); y, últimamente, la creciente presencia de drogas sintéticas elaboradas localmente o importadas de Europa y Asia (en este caso, fentanilo).

Esto se da porque en Latinoamérica existen "facilitadores" para el CTO, como ser la corrupción, la impunidad y la debilidad estatal. Esta última se evidencia en la incapacidad del aparato público tanto para desempeñar ciertas tareas y proporcionar determinados servicios, que son cubiertos por los grupos criminales, como para controlar de manera efectiva la totalidad del territorio nacional.

A este respecto, podemos decir que el crimen es un espejo donde se refleja la fragilidad de los Estados y que, a su vez, configura una combinación de altos riesgos y de la incapacidad del Estado de absorberlos y mitigarlos. Esta fragilidad nos muestra que el CTO depende de actores híbridos: grupos encargados de la infiltración del Estado donde actúan en la legalidad y brindan

protección a los criminales. Por lo tanto, para combatir el crimen organizado es fundamental combatir la corrupción.

La criminalidad organizada tiene impacto en el mantenimiento del ciclo de violencia armada en la región. Latinoamérica es considerada una de las regiones más violentas del mundo, principalmente Centroamérica. Medido en homicidios cada cien mil habitantes, América más que duplica el promedio mundial, y tanto América Central como América del Sur cuadriplican ese promedio. La violencia se explica a partir de la puja entre organizaciones criminales por el control de rutas y mercados de consumo de drogas, como también por el enfrentamiento entre estos grupos y las fuerzas del Estado.

Uno de los principales problemas al cual nos enfrentamos para combatir el CTO es la falta de cooperación. Cada Estado quiere mantener su "soberanía" en materia de control y aplicación de penas, pero cuando nos enfrentamos con un flagelo que no tiene bandera, la mirada debe ser distinta. Los Estados deben cambiar su concepto de soberanía tradicional en pos de la coordinación para enfrentar estas amenazas. La asistencia técnica mediante capacitación, formación y conocimiento en los niveles de agencia es fundamental. Tratar una agenda compartida con objetivos comunes y con una voluntad común para enfrentar a estas organizaciones transnacionales es un elemento esencial.

Se requiere de una estrategia holística para enfrentar el CTO, que contemple programas o planes nacionales de mediano plazo que excedan los tiempos electorales y estén dotados de los recursos financieros, humanos y de equipamiento necesarios; que abarquen todas las áreas del Estado; que no se limiten al plano federal, para alcanzar también los niveles regional y local; que involucren la esfera privada; y que incluyan la cooperación internacional. No solo se debe tener estructuras policiales acordes, sino que tiene que haber un abordaje social para perseguir a las organizaciones.

Sin embargo, nada de eso tendrá una efectividad duradera si al mismo tiempo no se atacan la corrupción y la impunidad ni se resuelve la cuestión de la debilidad estatal.

VI.
CONCLUSIONES

El eje transversal a todos los temas de este ciclo fue el rol de la tecnología, que ha alterado drásticamente la industria de la seguridad y de la defensa.

Las voces de los expertos de diversos ámbitos y países nos han permitido debatir sobre todas estas temáticas que, combinadas, nos han hecho sonar una alerta que no podemos postergar: el mundo post COVID-19 será más inseguro. Con eso en mente, hoy más que nunca, resulta imperativo seguir apostando por espacios de intercambio que posicionen estas cuestiones frente al desafío de la estabilidad y el desarrollo en el marco de una inserción internacional inteligente.

En este sentido, creemos que esta iniciativa será la piedra basal para el desarrollo de futuras actividades y que ayudará a producir y difundir el conocimiento indispensable sobre las principales transformaciones que el COVID-19 generó en cada uno de los ejes abordados a lo largo de este ciclo. Debemos seguir apostando por el desarrollo de espacios de intercambio y diálogo que posicionen estas y otras cuestiones y que den debida cuenta de sus principales desafíos y oportunidades en el siglo XXI.