

Amenazas y desafíos a la política de seguridad del siglo XXI



Resumen de la conferencia magistral internacional presentando el libro "AMENAZAS Y DESAFÍOS A LA POLÍTICA DE SEGURIDAD DEL SIGLO XXI" ofrecida por su autor, Javier Gamero Kinosita, en la International Police Association (IPA) - Sección España, en la Sala de Jueces del Instituto de Formación Integral de Seguridad y Emergencias (IFISE) de la Comunidad de Madrid el 19 de septiembre de 2022.

Los factores de estrés del mañana

Dentro de los factores de estrés del mañana, que la civilización humana tendrá que confrontar en el siglo XXI, tenemos la demografía, las nuevas tecnologías, el cambio climático y la geopolítica.

En lo que concierne a la demografía, los expertos señalan, que al 2050 la población mundial crecerá de 7 a 9 mil millones de habitantes y se prevé, que al 2100 el número se incrementará de 10 a 11 mil millones de habitantes, ello tendrá desde luego una masiva repercusión en la vida sobre el planeta y sobretodo en el uso de los recursos.

Con respecto a las nuevas tecnologías, ellas son una bendición y una maldición a la vez, pues tengamos en cuenta que hoy en día la vida de los seres humanos, ya sea en el ámbito social, económico, cultural y político, discurre en el ciberespacio, será cada día más difícil para el estado poder controlar estas tecnologías, entrañando nuevos peligros para la seguridad, verbigracia tenemos la cibercriminalidad, el ciberterrorismo, las ciberguerras, etc.

En lo que concierne a la geopolítica, sabemos que las relaciones de poder son volátiles, hay constantes desplazamientos de poder a nivel global, incremento de poder de actores no estatales, siempre hay naciones que ascienden y descienden, verbigracia tenemos el descenso de Estados Unidos y el ascenso de nuevas potencias,

como el caso de China, que pretende ser el nuevo hegemon del mundo.

La sociedad de riesgo global del siglo XXI

Hoy vivimos en la denominada "sociedad de riesgo", una teoría del científico social alemán Ulrich Beck de la Universidad Ludwig Maximilian en Múnich, Alemania, quién sostiene que los riesgos son reflejos normales del progreso, ya no es posible eliminarlos, solo es posible reducirlos, Beck planteaba que ya no existe un puerto seguro, por que vivimos en una permanente inseguridad, ya que ellos son consustanciales e inherentes con el nuevo orden mundial, tenemos que coexistir con ellos, es el precio que tenemos que pagar por el triunfo de la modernización.

Dentro de estos riesgos globales identificamos al terrorismo internacional, los peligros nucleares y atómicos, el crimen internacional organizado, las pandemias, etc. El profesional de la seguridad del siglo XXI es un gerente de riesgos, aplica la justicia matemática del seguro, hoy se habla de zonas de alto riesgo y de bajo riesgo, actores de alto riesgo y de bajo riesgo, fenómenos de alto riesgo y de bajo riesgo.

Amenazas y desafíos globales y las guerras del futuro en el siglo XXI

Dentro de las amenazas emergentes en los espacios comunes globales de la presente centuria, el

Instituto Internacional de Estudios de Seguridad Global (INISEG) de Madrid ha identificado a las armas de destrucción masiva, los conflictos militares, los conflictos armados, el crimen organizado, el terrorismo, el espionaje y los ciberataques.

Dentro de los desafíos emergentes en los espacios comunes globales el Instituto Internacional de Estudios de Seguridad Global de Madrid ha identificado el cambio climático, la dependencia energética, la crisis económica, los desastres naturales, los flujos migratorio, las pandemias y la vulnerabilidad de los estados fallidos.

Dentro de las inminentes guerras del futuro se han identificado la Guerra Helada producto del cambio climático, la guerra por las materias primas, la guerra por las proteínas en el Atlántico Norte, la guerra por los tubérculos en el Mar del Norte, la guerra por la alimentación mundial, la guerra por el espacio interplanetario, la guerra por las nuevas tecnologías, la guerra por la tecnología de la información, la guerra producto de la migración y las pandemias, consideradas la maldición del conocimiento.

Complejidad e incertidumbre del entorno híbrido del siglo XXI

El siglo XXI nos ofrece un nuevo mundo híbrido, que se abre a nuestros ojos, presentándonos un escenario inédito, atestado de riesgos y amenazas poliédricas cambiantes, difíciles de evaluar y

predecir, que los expertos en políticas de defensa y seguridad, identifican como una zona gris impregnada de complejidad e incertidumbre, una zona ambigua que es cercana a la paz y a la vez, cercana a la guerra.

Hoy se habla de “guerras híbridas”, “amenazas híbridas”, “ataques híbridos”, “estrategias híbridas”, etc.

Este mundo híbrido esboza un abanico completo de distintos modos de hacer la guerra en los denominados espacios comunes globales, ya que combina acciones convencionales y no convencionales, acciones militares y no militares, acciones encubiertas y no encubiertas, recurriendo a organización y tácticas irregulares, actos terroristas, ciberataques aprovechando de las vulnerabilidades sistémicas y críticas de otros Estados, con el fin de desestabilizarlo, crear ambigüedad y obstaculizar en cierto modo, la toma de decisiones, buscando generar perturbaciones económicas y desgobierno.

En este nuevo contexto híbrido o entorno híbrido no hay más certezas, se dan permanentemente cambios de las reglas de juego, existe una complejidad para definir la relación causa-efecto, existiendo una interdependencia de varios actores internacionales, que están en la búsqueda incesante de las vulnerabilidades sistémicas y críticas de los otros para el interés propio.

Las estrategias híbridas exigen una combinación sincronizada de acciones que se focalizan en las vulnerabilidades de cada nación, las mismas que muchas veces rebasan los límites de la diploma-

cia y el derecho internacional, usando en muchas ocasiones la ley como arma. Ellas priorizan su accionar para calar gradualmente en la voluntad de la población. Esta sincronización de acciones opera simultáneamente en la esfera política, económica, social, militar, diplomática, civil, de la infraestructura y de la información. Sus efectos no son lineales. En consecuencia hoy se requieren operaciones multidominio para hacerles frente, vale decir actuar en el ámbito de tierra, aire, mar y el espacio virtual.

Ciberespacio y ciberseguridad: Cambio de paradigma de la seguridad mundial

La OTAN declaró en el 2016 el ciberespacio como nuevo dominio de naturaleza militar, en efecto, el ciberespacio es el nuevo teatro de operaciones, en donde se perpetran las ciber guerras y actúan los ciberterroristas y ciberdelincuentes para desestabilizar a nuestros países. Este proceso globalizador impregnado de las nuevas tecnologías, ha hecho del ciberespacio el principal factor de desarrollo político, social, económico y cultural, entre otros, generando condiciones cambiantes y nuevos retos para la seguridad y defensa de los estados, en consecuencia, es necesario desarrollar capacidades militares de ciberdefensa y ciberseguridad en los estados para contrarrestar las ciberamenazas.

El ciberespacio es el nuevo desafío para los cuerpos de seguridad, él ya no es un dominio emergente de índole exclusivamente militar. Los estados actúan en él para establecer su poder y marcar presencia, también actúan en él actores no estatales, lo que ha originado un marcado

incremento de operaciones cibernéticas. Hoy las técnicas y tácticas de las tecnologías de la información se aplican a las operaciones militares para las acciones propias de las ciber guerras y las operaciones de ciberdefensa, ya que nos encontramos en una guerra electrónica o guerra de la información.

En el año 2021 se calcula, que la cibercriminalidad ha ocasionado daños que ascienden a 6 trillones de dólares a nivel mundial. En ese año, en el Perú se produjeron 433 millones de ataques cibernéticos, los ciberdelincuentes aprovechan la hiperconectividad, se estima que el 50% de la humanidad está online, en consecuencia el ciberespacio es el escenario perfecto y de riesgo permanente para el crimen. Los ciberataques se perpetran contra el sector industrial, sector empresarial, sector público, sector bancario y los usuarios.

La sociedad de vigilancia: Un elemento esencial de la política criminal internacional

La sociedad de vigilancia constituye un cambio de paradigma en la política criminal, implica un giro preventivo, se ha virado de la lógica de una represión reactiva a la lógica de una prevención proactiva.

Hoy vivimos en una sociedad plagada de cámaras, video-cámaras, circuitos cerrados de televisión, número de pines y códigos, etc. Tenemos datos de geolocalización y GPS (Global Positioning System) para rastrear a la gente en lugares infectados con Covid - 19, cámaras de seguridad termográficas instaladas en aeropuertos y supermercados,



que pueden medir la temperatura a 120 personas por minuto, tecnologías para vigilancia de fronteras para el control de la inmigración con drones o aviones no tripulados de observación, sistemas de lectores de mentiras por inteligencia digital, sistemas de reconocimiento facial que permiten el reconocimiento de los microgestos e inclusive sistemas de identificación de la gente por los latidos de corazón a 200 metros de distancia, la vibra cardíaca es única en cada individuo, similar al iris o la huella digital.

Todo ello implica un sometimiento general de la población, a subordinarse a un control permanente, este beneplácito ciudadano se conoce en política criminal como “consenso de vigilancia”. Esta sociedad de vigilancia tiene un costo social, ya que conlleva a una pérdida de privacidad, erosión de la autonomía individual, las nuevas tecnologías son cada vez más sofisticadas e intrusivas. Es necesario un marco regulatorio más claro y restrictivo.

Ciberseguridad y democracia: Riesgos, fortalezas y desafíos

Hoy vivimos una revolución tecnológica exponencial, que tiene un efecto drástico en todas las esferas de la vida, que acarrea fortalezas, riesgos y desafíos, incluso en el ámbito de la política.

Hoy rige el imperio de los datos, se habla de una soberanía digital que difiere de la soberanía territorial. Existe una desintermediación, han desaparecido las ventanillas, la digitalización ha tomado posición de nuestra forma de vivir.

Dentro de las fortalezas, ella ha repotenciado la participación ciudadana, reivindicando la democracia directa y fomentando una democracia deliberativa, hoy los ciudadanos pueden expresarse y levantar su voz desconcentrándose de cierta manera el poder. Sin embargo ella acarrea ciertos riesgos, tales como las brechas digitales, hoy la diferencia es entre los conectados y no conectados, en el ámbito político puede generarse una serie de anomalías tales como la expansión del populismo, la misoginia, el odio y el racismo, pueden producirse manipulaciones electorales por el auge de las redes sociales, expansión de fake news, arremeter contra el derecho de libertad de expresión (espionaje, bloqueos, etc), control de la información priorizando intereses políticos y comerciales.

En consecuencia esta sociedad de vigilancia constituye un desafío para los gobiernos, la prensa y la sociedad civil. La ONU ha trazado una hoja de ruta para la cooperación digital orientada a generar una mayor sensibilización y educación al alcance de sus derechos. En Europa se habla ya de los derechos digitales, de ciudadanía digital y de alfabetización digital.

Incremento de la cibercriminalidad en la sociedad de vigilancia

La sociedad de vigilancia está atestada de ciberdelitos (racismo y violencia, piratería, lavado de dinero, fraude online, terrorismo, crimen contra la propiedad intelectual, abuso sexual, monedas virtuales, crimen organizado internacional, corrupción), ciberobjetivos (sistemas de salud/pacientes, infraestructuras críticas, servicios, hoteles, restaurantes, datos privados, gerencias de mercado, finanzas y estrategias, gobierno e instituciones públicas, PYMES, e industria) y ciberriesgos (información sensible, información clasificada, inversiones, datos de pacientes, secretos del yihadismo, control político y de familias, competencia, servicios y cadenas de suministro). Nuevos ámbitos de actuación del ciberdelincuente se centran en el teletrabajo, compras por internet, en el ámbito sanitario. Se requiere una smart police (censores policiales).

Nuevos paradigmas de los servicios de inteligencia

Hoy es imprescindible instituir una cultura de inteligencia para consolidar una auténtica cultura de defensa y de seguridad. La evolución de la inteligencia ha transitado por 3 fases históricas bien marcadas. La inteligencia entre los años 50 y 70, influenciada por la Guerra Fría estuvo marcada por la doctrina de seguridad nacional y basada en la cultura del secreto. La inteligencia en la década de los 90, influenciada por el fin de la Guerra Fría, estuvo marcada por la doctrina de la seguridad democrática rigiendo el paradigma del gobierno abierto. Por último la inteligencia en la era de la sociedad pos 11/09, en ella rige una cultura que involucra a la sociedad, se da una apertura de los servicios de inteligencia en las diferentes esferas, estableciendo interconexiones con el sector privado y la sociedad civil en su conjunto, ya que muchos de sus actores son operadores no estatales de servicios estratégicos en las distintas esferas de la actividad humana (energía, salud, agricultura, alimentación, etc.).

El entorno híbrido hoy en día es un continuo proceso de transformación, se advierte cambio de objetivos entre el 11-S y el 11-M. El binomio de la inteligencia humana-operaciones militares es fundamental, lo será aún más en las operaciones militares futuras, cuyo entorno operativo será complejo y poliédrico, ya que hay nuevos actores y nuevas amenazas, que conllevarán a las operaciones multidominio en los nuevos dominios no físicos. La inteligencia del futuro requiere de una tecnología avanzada, equipos multidisciplinarios que les permita actuar en el ciberespacio, en el entorno híbrido, en donde existe dificultad de identificar las autorías. Es necesario un análisis prospectivo, ya que el entorno del futuro es un objetivo que se mueve y que nos plantea un mun-

do nuevo. La ventaja informativa será clave para la seguridad, ya que el análisis de datos serán garantía del conocimiento.

De la inteligencia a la ciberinteligencia

De la inteligencia se debe virar a la ciberinteligencia, la inteligencia es la base de la ciberinteligencia. Esta ciberseguridad debe de reforzar las capacidades técnicas, garantizar la capacidad de resiliencia, impulsar la conciencia ciudadana y empresarial, incrementar la capacidad de investigación para contrarrestar la cibercriminalidad, impulsar la industria de ciberseguridad y del talento. Es necesario tener una cultura de ciberseguridad dentro de un Plan Integral de Seguridad Nacional. Los objetivos de la ciberinteligencia es tomar conocimiento de las amenazas del ciberespacio, sus actores, sus capacidades, sus vulnerabilidades y sus formas de acción. De igual forma identificar, eliminar y administrar las amenazas informáticas que coadyuvan a la toma de decisiones en la protección de los Activos Críticos Nacionales, que están en función a la satisfacción de las necesidades vitales (recursos e infraestructuras, sistemas de salud, sector financiero, seguridad, etc, flujos de información y redes energéticas, refinerías e hidroeléctricas, son las arterias que sostienen la vida y que permiten nuestra forma de vida actual y futura.

Situación actual de la seguridad ciudadana en América Latina

América Latina es la región más violenta en el mundo, contando con una tasa de 24 homicidios por cada 100,000 habitantes versus la tasa de 6 homicidios por cada 100,000 habitantes en el resto del planeta. Existe una bipolaridad en la concepción de seguridad en la región, por una lado, la demanda colectiva de una mano dura contra la delincuencia, mientras que por otro lado, persisten los altos índices de pobreza, que es generador de la violencia. No olvidemos que la criminalidad es el núcleo duro de la pobreza. De igual forma se percibe una narcotización de la política de seguridad de los países de la región, se ha priorizado la lucha contra el tráfico ilícito de drogas, que sin lugar a dudas, es uno de los desafíos fundamentales de la seguridad, pero se han dejado de lado las políticas de seguridad ciudadana y el combate contra los delitos menores, habiéndose incrementado la microcriminalidad urbana.

La región cuenta con una política de seguridad reactiva y padece de la ausencia de inteligencia preventiva, pues la policía se han centrado en perseguir los delitos, dejando de lado la prevención debido a la falta de una política criminal racional, coherente y moderna, producto de la fractura de consensos políticos, que han dado lugar al surgimiento de políticos advenedizos

oportunistas, que ofrecen respuestas populistas con fines electorales, originando que las políticas de prevención a largo plazo sean dejadas de lado por los decisores políticos.

De igual forma se constata por un lado un déficit en los cuerpos de seguridad y policía de la región, se identifican serias asimetrías, producto del centralismo político y administrativo de los gobiernos, existen serias asimetrías regionales, desigualdades internas entre las unidades policiales de la capital y las unidades policiales en las zonas rurales, estas asimetrías no solo son de carácter administrativo y presupuestario sino que se traduce en asimetrías en el acceso del conocimiento y la profesionalización, beneficiándose solo el personal que labora en la capital o en grandes ciudades, en desmedro del personal de las zonas alejadas. Lamentablemente hoy los decisores políticos cofunden los roles entre policías y militares, se ha producido una militarización de la policía en la región, es necesario distinguir la línea divisoria entre defensa y seguridad. La policía no debe de tener enemigos a quién combatir, sino ciudadanos a quién proteger.

El momento histórico actual constituye un gran reto para los cuerpos de policía, la pandemia ha tenido efectos permisivos en los cuerpos de seguridad y policía, ellos han estado en primera línea de control de la pandemia, tangenciando libertades en virtud de las cuarentenas, confinamientos y restricciones sociales generando una merma de la confianza de la sociedad, marchas, movilizaciones y protestas violentas, creando una polarización de la opinión pública.

Las crisis ofrecen a su vez oportunidades, estamos ante una inflexión histórica y tenemos la oportunidad de revolucionar la cultura policial en la región, las medidas coercitivas adicionales conferidas deben de considerarse solo como ultima ratio. Es más probable, que las personas cumplan después de un encuentro con la policía, si sienten que han sido tratadas justamente, han recibido una explicación y han tenido la oportunidad de dar su opinión. Un modelo de intervención policial debe basarse en 4 principios: compromiso, explicación, persuasión y apoyo y por último, cumplimiento de la ley. La crisis del Covid – 19 da el chance para reflexionar sobre el estatus de las fuerzas policiales en las democracias del siglo XXI.

Para superar esta crisis es necesario armonizar las políticas institucionales de los cuerpos de policía en la región con los estándares internacionales orientar su actuación respetando los derechos humanos, el principio de no discriminación y formas de policiamiento en sintonía plena con los valores democráticos.

Reflexión final

Vivimos en una sociedad mundial que reposa en un espacio transnacional, la sociedad global es multidimensional, policéntrica y contingente, hay nuevos actores globales.

La globalización ha acentuado el proceso de transnacionalización, no solo de los espacios geográficos, sino también de los acontecimientos, problemas y conflictos.

En lo que concierne a los desafíos ecológicos, visualizamos hoy en día, una acción antrópica agresiva y violenta sobre el medio natural, lo que genera problemas ambientales globales, producto de la supremacía del modelo de desarrollo neoliberal y la globalización, vivimos en una sociedad en beneficio del mercado, la monopolización del poder, la injusticia y la desigualdad social. Ello ha generado una visión apocalíptica que se traduce en la muerte de la humanidad, dando lugar al surgimiento del pensamiento verde, una filosofía moral ecologista, que pretende imponer fronteras sociales al ser humano respecto a su relación con la naturaleza.

En lo que concierne a los desafíos tecnológicos, la ciberseguridad es el más grande desafío de las próximas décadas, ella afectará a cada familia, cada empresa, cada organización y cada gobierno. Los ciberataques destruirán datos, paralizarán la producción de empresas, comercializarán con mercancías ilegales e influirán en las elecciones, debilitando los procesos electorales.

Los órganos de inteligencia deben contar con especialistas de sistemas, programadores de diversos lenguajes, analistas de información y especialistas en arquitectura de redes para hacer frente a los incidentes informáticos.

Ya la Academia Nacional de Ciencias de Estados Unidos de Norteamérica nos advertía en 1990, que "estamos en peligro, cada vez dependemos más de las computadoras, los terroristas del mañana podrán ser capaces de hacer más daño con un teclado que con una bomba".

En lo que concierne a la seguridad ciudadana, esta constituye un elemento esencial para la gobernabilidad en el estado de derecho moderno, la seguridad ciudadana es un concepto democratizador que fortalece los derechos humanos y la cultura de paz, ella no debe ser vista como un producto acabado, sino más bien como un proceso vivo y permanente en el que todos estamos involucrados.

La seguridad nos concierne a todos. Las nuevas políticas de seguridad del siglo XXI deben conjugar y armonizar lo público y lo privado, el estado y el mercado, la centralización y la descentralización, al ser humano y la naturaleza, al hombre y a la mujer, el corto plazo y el largo plazo, la prontitud y la estabilidad, el Norte y el Sur, el derecho nacional y el derecho internacional, y por último, las políticas de derecha y las políticas de izquierda (la igualdad y justicia y los incentivos de actuación). Afrontamos nuevos problemas, conceptos y desafíos. Se requiere una nueva arquitectura de seguridad.



Autor: Javier Gamero Kinoshita